1629 K Street, NW, Suite 300 – Washington, DC 20006
www.cirq.org

QUALITY MANUAL

Table of Contents

The content of this Quality Manual applies to and is proprietary to CIRQ. However, this manual is available for inspection by customers and other interested parties, on request.

Document control

This is a Controlled Document maintained on the CIRQ Intranet site

Change Record

Revision #	Revision Date	Revised by	Description of Change
2.16			
2.15			
2.14	Feb 2023	J. Wood	Update to include requirements for ISO 27001:2022 and remove all text re: ISO 27001:2013
2.13	May 2022	J. Wood	Update to include requirements for ISO 27701 audit and certification services
2.12	Jan 2022	J. Wood	Update org chart and doc control # for ISO/IEC 27001:2022 audit report (per ANAB RFI)
2.11	Aug 2021	J. Wood	Update ISMS Application and justification of audit time text to reflect ISO/IEC 27006:2015 2020 Amendment to clause B.2.1
2.10	Apr 2021	J. Wood	Add ANAB ISO 17021-1:2015 accreditation mark and statement for ISO/IEC 27001:2022 certification program. Remove all PECB text.
2.9	Dec 2020	J. Wood	ANAB findings & system wide improvements
2.8	Oct 2020	J. Wood	Removal of CLC ISO/IEC 27001:2022 Audit Program Checklist to FC 2005 Audit Program Log (MASTER) to capture all client 3yr cycle data
2.7	March 2020	J. Wood	Revisions made to incorporate ISO 17021-1:2015 requirements for ISO/IEC 27001:2022 certification program
2.6	Jan 2020	J. Wood	Add ANAB ISO 17065 accreditation mark and statement for ISO 20252:2019 certification program.
2.5	Dec 2019	J. Wood	S9 Australian Audit Procedures, update of ISO 17065:2012 to align with ANSI Review; 2019 CIRQ & Insights Association Outsourced Services Agreement implemented for additional ISO 17065:2012 compliance
2.4	Sept 2019	J. Wood	Update: New CIRQ ISO 20252 Certification Mark(s)
2.3	February 2019	C. Kneidl/J. Wood	Revisions made to incorporate release of ISO 20252:2019.
2.2	May 2018	J. Wood/C. Kneidl	Revisions made to ensure compliance with ISO 17065, and that description of the 20252/26362 Core Procedures in Quality Manual match the C1-C11 detailed procedures document following review of same. Also added appropriate changes regarding the inclusion of auditing and certification services related to ISO27001.
2.1	2018	J. Wood	Update: - Introduction of Insights Association relationship from 2017 merger of MRA & CASRO - Managing Director's role & responsibilities - Revised Organizational Chart - Confidentiality/no-conflict policies

			Advisory Committee to CIRQ Board of Directors
2.0	12-22-14	J. Maloney	Update 20252 references to include 20252:2012, • Section 1: Introduction • Update Managing Director's role • Update Operations Administrator's Update of Global Prospective
1.9	7-8-14	J. Maloney	Replaced Guide 65 with ISO/IEC 17065:2012
1.8	2-27-14	J. Maloney	-Increased the # of supporting procedures to 8 -Change Operations Director to Managing Director -Update Organization chart -Update according to changes in procedures
1.7	3-30-12	J. Maloney	Add CASRO President to read and write privileges on the CIRQ Intranet
1.6	3-21-12	J. Maloney	Remove requirement for document information to be on the header (footer only)
1.5	12-19-11	J. Maloney	Update CIRQ Seals
1.4	11-18-11	J. Maloney	-pg. 14 update steps in application process -pg. 23 update feedback form procedure CIRQ shall not delegate the authority for granting, maintaining, extending, suspending or withdrawing certification to an outside person or authority CIRQ shall not delegate the authority for granting, maintaining, extending, suspending or withdrawing certification to an outside person or authority
1.3	9-29-11	J. Maloney	-Corrected Internal Audit Document Numbers -Added "CIRQ shall not delegate the authority for granting, maintaining, extending, suspending or withdrawing certification to an outside person or authority "to Organization Responsibilities and Authority section -Defined Management Committee
1.2	04-28-11	C. Kneidl, J. Ward, J. Maloney	Complete review during self-audit in April 2011 to incorporate all recent changes such as: Application changed to RFQ, etc.
1.1	08-31-10	C. Kneidl	Revised to align with various procedures that have been written
0	04-09-2010	C. Kneidl	Initial release

Certification Institute for Research Quality (CIRQ)
QUALITY SYSTEM MANUAL

I. Introduction

Launched in 2017, the Insights Association was formed through the merger of two organizations with long, respected histories of servicing the market research and analytics industry: CASRO (founded in 1975) and MRA (founded in 1957). The result is a new, larger and more connected association with a unified, coordinated and higher profile voice, aligned in mission and message, and ultimately more effective at advancing the industry and profession in which we all share an abiding passion.

The Insights Association strives to effectively represent, advance, and grow the research profession and industry. Specifically, the organization:

- Provides government advocacy through legislative, regulatory and judicial means
- Cares for and improves the industry's image in the eyes of the media and public
- Markets the business case for industry products and services to buyers and users
- Sets and enforces professional standards
- Establishes and reinforces best practices
- Helps members grow their businesses, their departments, and themselves as research professionals

CASRO was dedicated to helping the survey research industry (both member and non-member companies) grow and improve their businesses. With over 300 member companies in the U.S. and abroad, CASRO has represented the "voice and values" of survey research and survey research businesses in the U.S. since 1975.

In 2018, the Insights Association undertook an update and published the new Insights Association Code of Standards and Ethics for Market Research and Data Analytics, and members are required to adhere to this internationally cited set of standards.

Adherence to these standards:

- Enhances the image of survey research,
- Protects the rights and privacy of the public, and
- Protects the confidentiality of clients and the work done on their behalf.

The importance of the Insights Association Code extends beyond Insights Association members. It is a major reference document for international research businesses and for the global research community. Further, Insights Association advocates our industry's self-regulation, champions legitimate research companies, and marginalizes disreputable research operations that threaten to tarnish the industry's reputation and alienate respondents.

Insights Association's extensive services to members (and non-members) provide information and guidance on research and research business issues and trends. It also holds unique position among all North American research associations as an active representative on numerous global initiatives and as the U.S. liaison with several leading international associations.

In this latter role, Insights Association (previously CASRO) provides singular leadership as the official U.S. delegate to the Technical Committee (TC) of the International Standards Organization (ISO) in the development and maintenance of quality standards for the global survey research industry.

Through their membership on this Technical Committee, these two prior standards were released as indicated below:

- ISO 20252, initially released in 2006 and revised in 2012
- ISO 26362 for access panels, released in early 2009.

And in February 2019 the new ISO 20252:2019 standard, which combines the two prior standards, was released.

Insights Association's involvement with maintaining these global standards has helped ensure that its members' and the U.S. research industry's research and business processes are recognized and supported internationally. Insights Association endorses these new standards as a means to provide a firm foundation of quality for managing any research project and recommends them as a key component of a three-part quality program:

- Pillar 1: The Insights Association Code of Standards and Ethics for Survey Research
- Pillar 2: The on-going development and enhancement of best practices guidelines in the sciences and methodologies of market and opinion research
- Pillar 3: The ISO research standard that provide the infrastructure needed for quality processes related to research project management

Insights Association believes that certification to the above-mentioned ISO standard will provide tangible benefits to research companies, to the clients of research companies, and to the public.

In 2010 there were no accredited certification bodies for ISO 20252 or ISO 26362 in North America, nor were there any North American standards organization interested in becoming an accreditation body specifically to address the research standards. As a result, CASRO formed a wholly owned, non-profit subsidiary called the CASRO Institute for Research Quality (CIRQ) to provide auditing and certification services to research firms (members and non-members) headquartered in North America, and subsequently in the global arena, desiring to be certified to ISO 20252:2012 and/or ISO 26362. With the January 1, 2017, merger between CASRO and the MRA to form the Insights Association, the name of CIRQ has been officially changed to the Certification Institute for Research Quality, enabling the continued use of the CIRQ acronym.

CIRQ, and its parent organization, the Insights Association may share services as appropriate for the administration and management of CIRQ, and those can include marketing (e.g., print, digital), press releases & communications, graphic design, information technology (IT) services and financial administration support (*ISO 17065: 2012, 6.2.2.3, 6.2.2.4 Outsourced services*). The current CIRQ IA Outsourced Services Agreement covers this type of relationship, as needed.

When external services are used for CIRQ business, CIRQ's Managing Director has the discretion to research and secure vendors to provide required services. External vendors provide contract and scope of work document to CIRQ, which is kept within the CIRQ Intranet, CIRQ Records, Outsourced Services folder. An annual Outsourced Services Log can be requested from CIRQ at any time and is updated as appropriate when *ad hoc* services are used for CIRQ business.

CIRQ shares the USPS mailing address and limited back-office functions with Insights Association, located at 1629 K Street, NW, Suite 300, Washington, DC, 20006. The back-office functions are limited to receipt of CIRQ invoice payments and some financial administration.

The Insights Association is uniquely positioned to carry on the work initially undertaken by CASRO to continue growth and development of this certification body and provide a credible and

authoritative ISO 20252:2019 certification program for several reasons:

(1) It is the only US-designated representative to the ISO research standards development committee (ISO TC 225), and therefore has superior knowledge of the content, interpretation, and application of these standards to the US research industry.

(2) Through its international members, its image of integrity, and its involvement in global research associations, Insights Association has earned a respected position in the global research community.

(3) It has long been committed to self-regulation and the establishment of verifiable credentials that support continued self-regulation.

4) We believe Insights Association to be the leading and most respected voice for U.S. research businesses and the executive leaders of those businesses.

An Accredited Certification Body

In Spring 2019, The CIRQ Board of Directors voted their approval of the recommendation by the CIRQ Managing Director to undergo formal compliance to ISO/IEC 17065:2012 *Conformity assessment — Requirements for bodies certifying products, processes and services* through accreditation by the American National Standards Institute (ANSI) National Accreditation Body (ANAB).

In the fall of 2019, The CIRQ Board of Directors again voted their approval of the recommendation by the CIRQ Managing Director to undergo formal compliance to ISO/IEC 17021-1:2015 *Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements* through accreditation by the American National Standards Institute (ANSI) National Accreditation Body (ANAB).

CIRQ's certification program for ISO 20252:2019 *Market, opinion and social research, including insights and data analytics — Vocabulary and service requirements* was formally accredited by ANAB to ISO/IEC 17065:2012 in January 2020.

CIRQ's certification program for ISO/IEC 27001:2013 *Information technology — Security techniques — Information security management systems — Requirements* was formally accredited by the American National Standards Institute (ANSI) National Accreditation Body (ANAB) to ISO/IEC 17021-1:2015 in April 2021.

In August 2022, CIRQ added of another standard to meet demand of market research and data analytics organization with the pursuit of ISO/IEC 27701:2019, the Privacy Information Management System security extension to ISO/IEC 27001:2022. ISO/IEC 27701:2019 is the privacy information management system standard, and for companies outside of the EU (i.e., US, Canada, Asia, etc.), is a solution that maps to the General Data Protection Regulation (GDPR).

CIRQ was formally approved to transition to ISO/IEC 27001:2022 in April 2023 by ANAB, following a transition plan gap analysis that allows CIRQ to offer updated audit and certification services. CIRQ has established its transition arrangement for ISO/IEC 27001:2022 considering the requirements of the IAF MD 26:2023 document and all transition requirements as established by CIRQ's accreditation body, ANAB.

ISO/IEC 27001:2022 Transition information – Communication through the Transition Process	Throughout this Quality Manual, highlight boxes have been added to communicate transition requirements for **current** ISO/IEC 27001:2013 certified clients. Notes for **new** clients coming into ISO 27001:2022 from the outset are also included. This is to ensure audit programme roles and understanding CIRQ and client responsibilities throughout the transition timeline.

This Quality Manual introduces the requirements for ISO 17065:2015, ISO/IEC 17021-1:2015 and ISO/IEC 27006:2015 to support CIRQ's continual improvement to be a fully accredited certification body for its ISO 20252:2019, ISO/IEC 27001:2017 & the transition from ISO/IEC 27001:2013 to ISO/IEC 27001:2022 and ISO 27701:2019 certification programs.

It is noted here that qualifying for the ISO/IEC 27701 security extension is wholly contingent upon a client's certification to ISO/IEC 27001:2013 / ISO/IEC 27001:2022, either as an addition to an existing certification or as formally stated in an Initial Certification Audit Program (Stage 1/Stage 2) in combination with ISO/IEC 27001:2013 / ISO/IEC 27001:2022. This is discussed in the ISMS Core Process IS1 section below, detailing Submission & Review of the Management System Application for Certification.

Note:

1. Throughout this manual the use of the term "shall" denotes mandatory requirements. The use of the term "should" indicate provisions which would normally be regarded as mandatory with any variations in only exceptional circumstances. The use of the term "may" indicate a possible way (i.e., an example) in which compliance with a requirement might be met.

References:

- ISO/IEC 17065:2012 *Conformity assessment — Requirements for bodies certifying products, processes and services*
- ISO 20252:2019 *Market, opinion and social research, including insights and data analytics — Vocabulary and service requirements*
- ISO/IEC 17021-1:2015 *Conformity assessment — Requirements for bodies providing audit and certification of ISMSs — Part 1: Requirements*
- ISO/IEC 27001:2022 *Information technology — Security techniques — Information security ISMSs — Requirements (Note: ISO/IEC 27001:2013 will remain as a reference during the transition period to ISO/IEC 27001:2022)*
- ISO/IEC 27006:2015 *Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems*
- ISO/IEC 27701:2019 *Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines*
- CIRQ Operating Agreement
- IRS Group Exemption for CIRQ
- Insights Association Code of Standards and Ethics for Market Research and Data Analytics
- CIRQ IA Outsources Services Agreement 2022 for ISO 17065:2012 Compliance

II. Definitions

ISO/IEC 17065:2012, Clause 3
ISO/IEC 17021-1:2015, Clause 3
IAF MD 1:2018, Clause 2
IAF MD 2:2017, Clause 1

For the purposes of this document, the terms and definitions given in ISO/IEC 17065:2012 and ISO/IEC 17021-1:2015 the following shall apply:

1. Area of Concern - Departure from a particular system requirement, or failure to consistently implement a requirement, that is not likely to lead to a collapse of the ISMS. Areas of Concern should typically be resolved within 4 months. If not addressed these could lead to a system deficiency resulting in non-conformance. **Areas of Concern will normally be reviewed at the next surveillance audit**.
2. Audit time - time needed to plan and accomplish a complete and effective audit of the client organization's *research process* or *information security* management system
3. Auditor - person who conducts an audit
4. Certification audit - audit carried out by an auditing organization independent of the client and the parties that rely on certification, for the purpose of certifying the client's ISMS
5. Checklists – controlled documents used to ensure all required steps for a particular activity have been completed; completed checklists become records that shall be maintained.
6. Company – A research company seeking or holding certification to ISO 20252:2019. Certified companies are the customers or clients of CIRQ. The words "customer" and "client" may be used interchangeably to represent a certified company.
7. Competence – ability to apply knowledge and skills to achieve intended results
8. Compliance – The assurance that specified requirements of a standard are met.
9. Corrective Action – Action taken to prevent a recurrence of a non-conformance. This requires an analysis to be undertaken to find out the cause of the non-conformance.
10. Documents – controlled documents used to provide consistent information at various times throughout the auditing and certification process.
11. Duration of ISMS certification audits - part of audit time spent conducting audit activities from the opening meeting to the closing meeting, inclusive of conducting the opening meeting; performing document review while conducting the audit; communicating during the audit; assigning roles and responsibilities of guides and observers; collecting and verifying information; generating audit findings; preparing audit conclusions; conducting the closing meeting
12. Forms – controlled documents that support the quality and consistent completion of a required step within a procedure; completed forms become records that shall be maintained.
13. Guide - person appointed by the client to assist the audit team. In many cases, this can be the ISMS consultant hired by the client.
14. Guidelines – controlled documents used to provide direction (or guidelines) for a particular activity; these do not become records in and of themselves.
15. ICT – Information and communication technology used as an approved alternative to in-person auditing. ICT includes all web-conferencing platforms (e.g., Zoom, Teams, etc.).
16. Impartiality - presence of objectivity. Objectivity means that conflicts of interest do not exist or are resolved so as not to adversely influence subsequent activities of the certification body. Other terms that are useful in conveying the element of impartiality include "independence", "freedom from conflict of interests", "freedom from bias".
17. ISMS consultancy – A consultancy firm or individual who leads the participation in establishing, implementing or maintaining an ISMS under contract with their client

18. Major nonconformity – nonconformity that affects the capability of the ISMS to achieve the intended results. Nonconformities could be classified as major in the following circumstances:
    a. if there is a significant doubt that effective process control is in place, or that products or services will meet specified requirements
    b. a number of minor nonconformities associated with the same requirement or issue could demonstrate a systemic failure and thus constitute a major nonconformity
    c. ISO/IEC 27001:2022 and ISO/IEC 27001:2022+ISO 27701: NCs shall be accompanied by the client's Root Cause Analysis
19. Minor nonconformity - nonconformity that does not affect the capability of the ISMS to achieve the intended results
20. Multi-Site Organization - An organization covered by a single management system comprising an identified central function (not necessarily the headquarters of the organization) at which certain processes/activities are planned and controlled, and a number of sites (permanent, temporary or virtual) at which such processes/activities are fully or partially carried out.
21. Non-conformance - A total absence of the criteria for compliance with the nominated standard; or a situation that raises significant doubt as to the effectiveness of the ISMS to achieve its intended outputs.
    a. ISO 20252: NCs must be resolved and closed within 2-4 months and may require a follow-up audit prior to the next surveillance audit.
22. Observer – person who accompanies the audit team but does not audit
23. Observation – A positive or negative statement of fact that relates to the operations observed during the course of the audit.
24. Opportunity for Improvement – An opportunity that, if considered by the client, may provide a potential improvement to the ISMS
25. Permanent Site: Site (physical or virtual) where a client organization performs work or from which a service is provided on a continuing basis.
26. Product: The use of this word includes tangible products, as well as processes or services delivered to clients.
27. Projects - A definable piece of work carried out for a client (or group of clients) including all work carried out ad hoc, or a "wave" of tracking or continuous work.
28. Technical Area - area characterized by commonalities of processes relevant to a specific type of ISMS and its intended results
29. Technical expert - person who provides specific knowledge or expertise to the audit team
30. Templates – controlled documents that provide a large majority of the text in a required communication between CIRQ and a client or applicant; these templates are customized to the individual company or situation and become retained records when completed.
31. Transfer of Certification - The recognition of an existing and valid management system certification, granted by one accredited certification body, (hereinafter referred to as the "issuing certification body"), by another accredited
    certification body, (hereinafter referred to as the "accepting certification body") for the purpose of issuing its own certification.
32. Transition audit – Auditing to a revised or updated version to an ISO standard. As of 2023, ISO 27001:2013 has been updated and the new requirements are reflected in ISO/IEC 27001:2022. Clients certified to the 2013 version of the standard will be required to transition to the 2022 version of the standard to achieve certification upon fulfillment of all CIRQ requirements.
33. Virtual Site – Virtual location where a client organization performs work or provides services using an on-line environment allowing persons from different physical locations to execute processes

34. Workbooks – controlled documents set-up as Excel workbooks to ensure the quality and consistent completion of a series of required steps within various procedures; completed workbooks become records that shall be maintained.

III. Principles

ISO/IEC 17021-1:2015, Clause 4

The overall aim of certification is to give confidence to all parties that an ISMS fulfills specified requirements. The value of certification is the degree of public confidence and trust that is established by an impartial and competent assessment by a third-party. Parties that have an interest in certification include, but are not limited to:

a) the clients of the certification bodies
b) the customers of the organizations whose RPMS, ISMS and PIMS are certified
c) governmental authorities
d) non-governmental organizations
e) consumers and other members of the public.

CIRQ's principles for inspiring confidence include impartiality, competence, responsibility, openness, confidentiality, responsiveness to complaints, and a risk-based approach.

IV. Scope of Certification Body

ISO/IEC 17065:2012 – Clause 4.4
ISO/IEC 17021-1:2015 – Clause 1

CIRQ has been established to provide auditing and certification services to Insights Association members, as well as other non-member survey research service providers, that wish to be certified to ISO 20252:2019, ISO/IEC 27001:2022, and ISO/IEC 27001:2022+ISO/IEC 27701:2019.

CIRQ offers its services globally. CIRQ certification services will not be restricted to, nor are these services conditional upon, the number of certifications issued.

The scope of this Quality Manual, and the Quality System (QS) it describes, is to address the policies and procedures needed to meet the requirements of:

1. Scheme document: *Accreditation requirements for organizations providing certification services to ISO 20252: 2019 Market, opinion and social research including insights and data analytics within the territorial jurisdictions of Australia, UK, and USA*. (Triumvirate MOU of The Research Society, The Market Research Society, and Insights Association respectively.)
2. ISO/IEC 17065:2012 *Standard for Conformity Assessment Requirements for bodies certifying products, processes, and services*.
3. ISO/IEC 17021-1:2015 *Conformity Assessment Requirements for bodies providing audit and certification of ISMSs.*
4. ISO/IEC 27006:2015 *Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems*
5. ISO/IEC 27006-2:2021 - *Requirements for bodies providing audit and certification of information security management systems — Part 2: Privacy information management systems*

This Quality System addresses the way in which business is conducted by CIRQ in providing auditing and certification services to Insights Association members and non-members, relative to ISO 20252:2019, ISO/IEC 27001:2022, and ISO/IEC 27701:2019. The policies and procedures of CIRQ are administered consistently, impartially, rigorously, and in a non-discriminatory way at all times.

References:

- Scheme Document: *Accreditation requirements for organisations providing certification services to ISO 20252: 2019 Market, opinion and social research including insights and data analytics within the territorial jurisdictions of Australia, UK, and USA*. (June, 2020)
- ISO/IEC 17065:2012
- ISO/IEC 17021-1:2015
- ISO/IEC 27006:2015
  ISO/IEC 27006-2:2021
- CIRQ Intranet

V. Quality & Impartiality Policies

ISO/IEC 17065:2012, Clause 5.2
ISO/IEC 17021-1:2015, Clause 5.2
ISO/IEC 27006:2015, Clause 5.2.1 IS 5.2
The quality policy of the Certification Institute for Research Quality (CIRQ) is……

CIRQ is committed to providing timely, thorough, and impartial assessment of their customers' research process management system and/or information security management system in order to make a determination regarding certification to ISO 20252:2019, ISO/IEC 27001:2013 / ISO/IEC 27001:2022, and ISO/IEC 27701:2019.

This quality policy is shared with all CIRQ staff and posted on CIRQ's website. The management of CIRQ ensures that the quality policy is communicated and understood within the organization through appropriate training, personal reinforcement, and implementation of quality objectives.

This quality policy and the Quality System are reviewed regularly to ensure that they:

- are appropriate and suitable for the organization
- include a commitment to comply with requirements and to continually improve the effectiveness of the quality system; and
- provide a framework for establishing and reviewing quality objectives.

CIRQ's impartiality policy is:
CIRQ is committed to impartiality in ISMS certification activities. CIRQ's Quality Policy is a publicly available statement stating that it understands the importance of impartiality in carrying out its ISMS certification activities as it manages conflict of interest and ensures the objectivity of its ISMS certification activities.

CIRQ's Board of Directors, personnel, external auditors and technical advisors are committed to ensure that all ISMS Certification activities are undertaken in an impartial and unbiased manner.

CIRQ complies with the requirements of ISO/IEC 17021-1:2015 and ensures impartiality for all its personnel related to all certification activities.

CIRQ has established processes to identify, analyze, evaluate, treat, monitor, and document risks related to conflict of interests arising from provision of certification including any conflicts arising from its relationships on an ongoing basis. In case of threats to impartiality, CIRQ documents and demonstrates elimination or minimization of such threats and documents residual risk. In cases of residual risk, each instance is then reviewed to determine if it is within the level of acceptable risk. The demonstration covers all potential threats that are identified whether they arise from within the certification body or from activities of other people, bodies or organizations. Whenever a relationship poses an unacceptable threat to impartiality then certification will not be provided.

To ensure the above, CIRQ has established an Impartiality Committee of interested parties that include clients, representatives of industry associations, and customer organizations.

To demonstrate effective Implementation of this Impartiality policy:

- CIRQ will not certify another certification body for their efforts of RPMS, ISMS or PIMS unless they are officially transferring their RPMS, ISMS or PIMS to CIRQ.
- CIRQ will not provide Management Consultancy services for realization, continuity and sustenance of certification.
- CIRQ will not conduct internal audits of its certified clients.
- CIRQ will not provide its services either marketed or offered as linked with organization providing management consultancy.
- CIRQ will not outsource audits to any RPMS, ISMS or PIMS consultancy organization nor allow any auditor, who was responsible for providing RPMS, ISMS or PIMS consultancy towards the client to be involved in audits.
- CIRQ will not state or imply that certification would be simpler, easier, faster or less expensive.
- CIRQ will take action to respond to any threats to its impartiality arising from the actions of other persons, bodies, or organizations.
- CIRQ personnel, both external and internal, or committees, who could influence certification activities will not allow any commercial, financial, or other pressures to compromise impartiality are required to sign and submit a No Conflict Statement (FC5001)
    - *It is the policy of CIRQ to disqualify any auditor from the responsibility of performing assessments or certification activity for any company in which the auditor has a current, prior or future interest. To the best of my knowledge, I will not accept assignments in which I have (1) a vested interest in the assigned client, (2) been employed by the client in some capacity within the past three years, currently, or will agree to be employed by the client in some capacity in the next year (3) provided consulting services to the client within the past two years or will provide consulting to the client in the next year, or (4) provided specific and tailored training services to the client within the past two years. If prior to or during the course of an assignment I identify a situation in which I believe the impartiality of the audit can be/has been compromised, I will notify the CIRQ*

Managing Director immediately.

- CIRQ requires revealing and recording of any situation of conflict of interest from its personnel for taking appropriate steps.

VI. Quality Objectives

CIRQ's quality objectives are to:

- Provide a valuable service to members and non-members that will help them strengthen the quality of the survey research services they provide.
- Provide a valuable service to members and non-members that will help them strengthen the quality of their information security management system and mitigate data breaches.
- Be the foremost respected certification body in North America for certification of research service providers to the ISO 20252:2019, ISO/IEC 27001:2022, and ISO/IEC 27701:2019 standards.
- Establish strong links with other certification bodies and relevant organizations with coverage outside of North America.

VII. Confidentiality and Conflict of Interest

ISO/IEC 17065:2012, Clause 4.5, 6.1.1.3
ISO/IEC 17021-1:2015, Clause 8.4
ISO/IEC 27006:2015, Clause 8.4.1 IS 8.4

Confidentiality

Protecting confidential CIRQ and customer information is critical to the integrity and reputation of CIRQ as a credible and authoritative certification body for ISO 20252:2019, ISO/IEC 27001:2022, and ISO/IEC 27701:2019 standards and to maintaining CIRQ's legal and corporate establishment.

It should be noted that since CIRQ is a wholly owned, non-profit subsidiary of Insights Association, a U.S. trade association, much of its administrative and financial operations are public record for individuals who may want to better understand the non-profit status. All information and documentation obtained from or provided by companies during the auditing and certification process, shall be treated as confidential by CIRQ and may not be disclosed to any third party (including the Insights Association) without the company's written consent. Information about an Organization which is already known to be available in the public arena may be disclosed without this written consent.

CIRQ maintains a password protected and limited use Intranet cloud solution for all templates, forms, documents and client audit information. Only the Managing Director has super-administrative permissions, and auditors are assigned specific client folders during the audit planning cycle to which they are assigned. Information is secure and handled on a confidential basis at all times.

Unless authorized by the applicant in writing, details of applications for certification are also treated as confidential until the conclusion of the certification process. Information about a particular certified client or individual shall not be disclosed to a third party without the written consent of the certified client or individual concerned. Upon certification, companies achieving certification and their Statement of Applicability will be posted on the CIRQ website. Where a Company is unsuccessful in its application for certification, this information is not made available by CIRQ.

Where the law requires information about an applicant or certified company to be disclosed to a third party, CIRQ shall inform the customer of the information provided, as permitted by the law, or, where the law requires such information, without such consent.

All CIRQ staff (defined as employees, independent contractors, board members, or consultants) shall maintain the confidentiality of the information referenced above. Confidentiality of such information is addressed in the agreements signed by independent contractors and technical advisors, plus it is addressed in the CIRQ Organization Handbook. Within CIRQ, confidential information should be discussed only with those who, according to their position description, have a role to play.

Note for ISO/IEC 27001:2022, or ISO/IEC 27001:2022+ISO 27701 Audits: Before the certification audit, the CIRQ shall ask the client to report if any ISMS/PIMS related information (such as ISMS/PIMS records or information about design and effectiveness of controls) cannot be made available for review by the audit team because it contains confidential or sensitive information. CIRQ shall determine whether the ISMS/PIMS can be adequately audited in the absence of such information. If the CIRQ concludes that it is not possible to adequately audit the ISMS/PIMS without reviewing the identified confidential or sensitive information, it shall advise the client that the certification audit cannot take place until appropriate access arrangements are granted.

Conflict of Interest

CIRQ staff and contractors are prohibited from engaging in any conduct, activity, practice, or act which conflicts with, or appears to conflict with, the interests of CIRQ, including any conduct which is directly or indirectly unethical, dishonest, disloyal, disruptive, competitive or damaging to CIRQ's interests. CIRQ personnel shall not accept any money or other gifts or favors of more than nominal value from such an enterprise, particularly in situations where certification judgment may be influenced.

Definitions

Auditor: An independent contractor who assesses and documents compliance with a standard

Auditing Conflicts: Situations where an auditor audits a company for which they are currently employed or consulting, or for which they have been employed or done consulting in the past 3 years

Consultant: Anyone who provides assistance, advice, know how, or guidance in exchange for a payment currently or within the last 3 years

Consulting Ban List: A list of companies where auditors agree to not conduct audits for in the next 3 years

Consulting Conflict: When an auditor has done consulting for a competitive company of the client, and the client objects to the auditor being assigned to audit their company.

Self-Declaration of No Conflicts: A declaration from an auditor and/or client prior to each potential audit that they are not aware of any conflicts that exist between the client and auditor.

Personnel are expected to regulate their business conduct and business knowledge so as to avoid loss (either monetary or informational) to CIRQ that might arise from their influence on CIRQ decisions or their knowledge of CIRQ business and plans. Personnel are expected to:

- Foster professional conduct that reflects positively on CIRQ, its stakeholders, and the market, opinion and social research industry.
- Protect the organization from financial loss.
- There must be no unreported business relationship with any enterprise that supplies, benefits from, or competes with CIRQ.

CIRQ auditors declare any interest in or connection with an applicant company, certified company, or other company involved in or subject to the certification process, before taking on any assigned work, or before the situation arises. Such interests or connections apply to past, present and future involvement with the company. Declarations will be in writing, and as follows:

No Conflict Statement (FC5001)
It is the policy of CIRQ to disqualify any auditor from the responsibility of performing assessments or certification activity for any company in which the auditor has a current, prior or future interest. To the best of my knowledge, I will not accept assignments in which I have (1) a vested interest in the assigned client, (2) been employed by the client in some capacity within the past three years, currently, or will agree to be employed by the client in some capacity in the next year (3) provided consulting services to the client within the past two years or will provide consulting to the client in the next year, or (4) provided specific and tailored training services to the client within the past two years. If prior to or during the course of an assignment I identify a situation in which I believe the impartiality of the audit can be/has been compromised, I will notify the CIRQ Managing Director immediately.

Such declarations and the outcomes shall be documented and retained on the CIRQ Intranet in the client folders. Any person in doubt about whether a potential conflict of interest exists shall immediately place the facts before the Managing Director for his/her determination. And should the Managing Director be in doubt about whether a personal potential conflict of interest exists, he/she shall immediately place the facts before the CIRQ Board for their determination.

References:
- CIRQ Organization Handbook
- Annual Agreements signed by Independent Contractors (TS7001)
- Auditor Declaration of No Conflict (FC 5001)

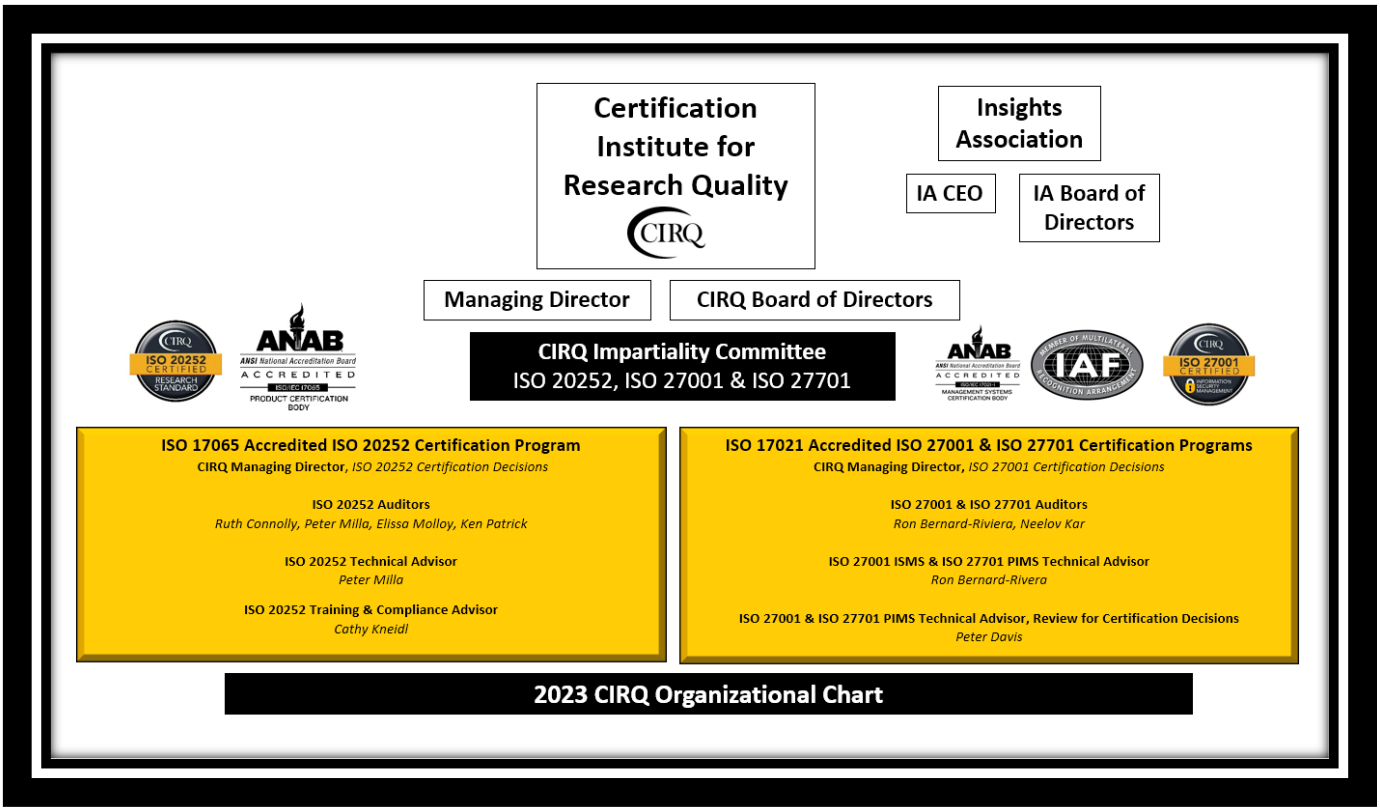
VIII. Organization Responsibilities and Authority

ISO/IEC 17065:2012 – Clauses 4.1.1, 4.3, 4.4, 5.1, 6
ISO/IEC 27006 – Clauses 5.2, 6; 7.1.1 IS 7.1.1-7.1.2 IS 7.1.2

CIRQ is set up as a wholly owned, non-profit subsidiary of Insights Association in order to facilitate impartiality and foster confidence in the auditing it conducts and the decisions it makes regarding certification to ISO 20252:2019, ISO/IEC 27001:2013, ISO/IEC 27001:2022 and ISO/IEC 27701:2019 standards. CIRQ's services are not dependent upon or a pre-requisite of membership in the Insights Association, as CIRQ does not discriminate, impede, or obstruct a client engagement, other than those policies and procedures outlined in this Quality Manual.

Documentation of CIRQ's legal status and liability insurance are maintained at CIRQ offices. Financial records for the Insights Association and CIRQ are maintained separately for both organizations, and securely maintained at the offices shared by the Insights Association and CIRQ. The organizational chart below reflects the general structure of CIRQ.

Image 1. 2023 CIRQ Organizational Chart for ISO 20252, ISO/IEC 27001:2022 & ISO 27701 Certification Programs



The CIRQ Managing Director (MD) and the CIRQ Board of Directors are committed to the development, implementation and continual improvement of its QS. This commitment is demonstrated by:

- Ensuring that a Quality System is established, implemented, and maintained in accordance with ISO/IEC 17065:2012, ISO/IEC 17021-1:2015, and the *Accreditation requirements for organisations providing certification services to ISO 20252: 2019 Market, opinion and social research including insights and data analytics within the territorial jurisdictions of Australia, UK, and USA*.
- Establishing the CIRQ Impartiality Committee
- Ensuring that the policies and procedures of CIRQ are impartially administered
- Establishing the CIRQ Quality Policy and Quality Objectives
- Conducting periodic internal audits and Management Reviews to monitor the performance and effectiveness of the Quality System
- Ensuring auditors/experts familiar with processes and requirements are provided access to up-to-date documented procedures and instructions through CIRQ's Management System pyramid on the CIRQ Intranet.
- Communicating the importance of CIRQ's role in the market research, consumer insights, data analytics, and social opinion research industry to CIRQ staff and customers
- CIRQ's promotion of its auditing and certification services to survey research companies, that represent potential customers.

CIRQ management ensures that Quality System responsibilities and authorities are defined and communicated within the organization, and among its Auditors and advisors. The following rules apply:

- A Managing Director who is a current Insights Association full time employee
- CIRQ trained Auditors including Independent Contractors
- A Training and Audit Advisor, who serves on a part-time basis, as an Independent Contractor
- A Technical Advisor for ISO 20252:2019, who serves on a part-time basis, as an Independent Contractor
- Technical Advisors for ISO/IEC 27001:2022 ISMS and certification review
- A Board of Directors is currently made up of industry volunteers who serve on a part-time basis and in an honorary capacity. At present, this Board consists of:
    - Managing Director of CIRQ
    - Insights Association CEO
    - CIRQ Board Chairperson
    - 4 additional CIRQ Board members (volunteers)

The CIRQ Board chair and the other 4 members represent various disciplines within the survey research industry. Overtime, as CIRQ grows, the Board may be increased by adding individuals representing the following:

- The individual responsible for the quality system in a CIRQ customer company certified to ISO 20252:2019
- The individual responsible for the information security ISMS in a CIRQ customer company certified to ISO/IEC 27001:2022
- A representative from another national association, if any, that establishes collaborative relationships with CIRQ
- An Insights Association Board member
- An Insights Association member, but non-Board member
- The Insights Association's General Counsel

The Insights Association CEO shall have interim financial responsibility for CIRQ. The Managing Director will report to the Insights Association CEO. A Training and Audit Advisor and a Technical Advisor will be consulted on a case-by-case basis for needs appropriate to ISO 20252:2019. CIRQ has

also appointed competent and knowledge technical advisors for the ISO/IEC 27001:2013 / ISO/IEC 27001:2022 program. Auditors will report directly to the Managing Director. As the base of customers grows additional positions may be created.

CIRQ shall solely retain the authority for granting, maintaining, extending, suspending or withdrawing certification for ISO 20252:2019, ISO/IEC 27001:2013 / ISO/IEC 27001:2022 and ISO 27701:2019.

All CIRQ staff will work in accordance with the existing CIRQ Organization Handbook, maintained on the CIRQ Intranet in Level 1 Corporate. During orientation training, CIRQ management, staff and Auditors are trained on their specific Quality System responsibilities outlined below. Responsibilities of CIRQ staff will be carried out in accordance with CIRQ's policies and procedures.

Board of Directors:

ISO/IEC 17065:2012 – Clause 5.2
ISO/IEC 17021-1:2015 – Clause 5.2

To ensure impartiality and independence of CIRQ from the Insights Association, a CIRQ Board of Director Chairperson will be appointed by the Insights Association CEO. The CIRQ Chair will then nominate additional CIRQ Board members. This Board comprises individuals with appropriate experience and expertise drawn from a cross section of disciplines and should represent parties concerned in the development of policies and principles regarding the functioning of CIRQ. There may be a need to supplement this Board from time to time due to growth, resignations, workload etc.

Prospective members may be identified by the Managing Director of CIRQ, the Insights Association CEO, or other Board members. Current members of the CIRQ Board or technical experts with appropriate expertise shall evaluate the nominee's competence, before a recommendation is made or accepted.

Management Reviews

ISO 17065:2012, Clause 8.5.2, 8.5.3
ISO 17021-1:2015, Clauses 10.2.5.2- 10.2.5.3

The CIRQ Board of Directors meeting 3-4 times per year for a combination of conference calls, web-conferences (video) and in-person meetings to discuss the CIRQ quality management system. The Board, with input from the CIRQ Managing Director and the CEO of the Insights Association, review management inputs:

a) results of internal and external audits
b) feedback from clients and interested parties
c) feedback from the CIRQ Impartiality Committee
d) the status of corrective actions
e) the status of actions to address risks
f) follow-up actions from previous management reviews
g) the fulfilment of objectives
h) changes that could affect the management system
i) appeals and complaints

The management review also addresses outputs that include decisions and actions related to the following:

a) improvement of the effectiveness of the management system and its processes
b) improvement of the certification body related to the fulfilment of ISO/IEC 17065
c) improvement of the certification body related to the fulfillment of ISO/IEC 17021 & ISO/IEC 27006
c) resource needs.

All review inputs and outputs are reviewed at least once per year and can increase as the need is identified. An agenda guideline document is prepared and accompanies the presentation (e.g., PowerPoint) that is prepared for each meeting. These management review records are kept on the CIRQ Intranet, CIRQ Records in the Management Review and CIRQ Board Meetings for the folder appropriate to the year.

Responsibilities include**:**

- Ensure the independence and impartiality of CIRQ by providing support to the Managing Director or taking independent action, as needed
- Provide input regarding:
    - policies and principles of CIRQ related to impartiality of CIRQ's certification services
    - any tendency of CIRQ to allow commercial or other considerations to prevent consistent, impartial certification services
    - matters affecting impartiality and confidence in certification
- Approve appointment of, and continue liaison with, CIRQ's management team
- As requested by Managing Director, assist with complaint/appeal issues and risk management issues
- Ensure adherence to the policies/procedures in the CIRQ Organization Handbook, which incorporates relevant sections of the Insights Association Board of Directors Book, including the Code of Conduct and the Code of Standards and Ethics for Survey Research
- Maintain the confidentiality of all information created or acquired during the course of offering its certification services, unless it is publicly available or when agreed between the client and CIRQ

References:

- CIRQ GLS4001 1.2 Guidelines for Board & Mgmt. Review Meetings

Managing Director

ISO/IEC 17065:2012, Clause 6
ISO/IEC 17021-1:2015, Clause 7.1, Annex A, D

This role has overall responsibility for operational matters as detailed in the Core Procedure documents and the Support Procedures (Level 2). Additional responsibilities include:

- Maintain the general operational matters of the CIRQ Quality System in such a way to create confidence in and credibility with its auditing and certification services on a global basis
- Oversee and manage ANAB accreditation requirements for both certification programs and revise/edit CIRQ Quality manual as needed/required to maintain accreditation status
- Ensure & facilitate impartiality in CIRQ operations from outside influence in order to foster confidence in the auditing it conducts and the decisions it makes regarding certification to ISO 20252:2019, ISO/IEC 27001:2013 / ISO/IEC 27001:2022 and ISO 27701:2019.
- Make certification decisions for ISO 20252:2019, ISO/IEC 27001:2013 / ISO/IEC 27001:2022 and ISO 27701:2019; the managing director refrains from the evaluation (audit) process.
- Ensure auditors/experts familiar with CIRQ processes and requirements are provided access to up-to-date documented procedures and instructions through CIRQ's Management System pyramid on the CIRQ Intranet.
- Hire all CIRQ staff, including Auditors, and ensure all staff complete appropriate training
- Oversee activities of all staff and conduct annual review of their performance, except for Board Members who do not receive annual performance reviews
- Review and approve all audit materials and refer to the CIRQ Board for input including

making final determination on certification matters
- Regularly review customer satisfaction results and take action as needed
- Serve as liaison with external parties on matters relating to the quality system
- Create and support promotion of ISO 20252:2019, ISO/IEC 27001:2013 / ISO/IEC 27001:2022 and ISO 27701:2019 certification to Insights Association members and non-members and other entities as opportunities arise
- Develop and support new client audit and certification activities
- Develop and manage relationships with global entities interested in or supporting certification for their regions
- Deliver periodic reports to CIRQ Board on the performance of the Quality System's effectiveness and as a basis for determining improvement of the Quality System
- Develop and report financial projections with Insights Association CEO
- Represent CIRQ at industry events
- Develop new CIRQ offerings
- Day-to-day financial responsibilities (invoicing, vendor expenses, etc.)
- Develop cost quotations according to CIRQ procedures
- Track audit workflow including auditor responsibilities
- Serve as the super-administrator for the CIRQ Intranet site
- Lead the refining of the CIRQ procedures
    - C1-C11 for ISO 20252:2019
    - IS1-IS10 for ISO/IEC 27001:2022
    - supporting procedures (S series documents)
- Revise old forms and develop new ones to better address CIRQ's needs
- Manage internal audit program
- Manage the Complaint, Appeal and Dispute procedure, as well as the Risk Management Procedure
- Field phone and email inquiries related to CIRQ
- Participate in marketing creation and associated efforts for CIRQ
- Update CIRQ website

Qualifications, Competencies and Knowledge requirements:

- Competent in the interpretation of ISO/IEC 17065:2012, ISO/IEC 17021-1:2015, ISO/IEC, ISO 19011:2018, ISO 27006:2015, ISO/IEC 27006-2:2021, ISO 20252:2019, ISO/IEC 27001:2013 / ISO/IEC 27001:2022 and ISO/IEC 27701:2019.
- Knowledge of scheme document: *Accreditation requirements for organizations providing certification services to ISO 20252: 2019 Market, opinion and social research including insights and data analytics within the territorial jurisdictions of Australia, UK, and USA.*
- Knowledge of and understanding of the CIRQ operational procedures and those Insights Association procedures which may impact on CIRQ management activities
- Market, opinion and social research industry knowledge and/or experience
- General computer skills
- Report writing skills
- Communication and consultation skills

ISO 20252:2019 Certification Program
Training and Compliance Advisor – As needed

- Support the impartiality in CIRQ operations from outside influence in order to foster confidence in the auditing it conducts and the decisions it makes regarding certification to ISO 20252:2019.
- Support promotion of ISO 20252:2019 certification to Insights Association members and non-members
- Create and deliver training programs for interested companies.
- Council auditors on practices as needed.
- Sign a confidentiality, non-compete, and non-solicitation agreement

Qualifications, Competencies and Knowledge requirements:

- Competent in the interpretation of ISO 20252:2019
- Competent in the auditing procedures and documentation process as established by CIRQ
- Market, opinion and social research industry knowledge and/or experience
- General computer skills
- Report writing skills
- Communication and consultation skills

Technical Advisor for ISO 20252 – As needed

This role has overall responsibility for technical matters as detailed in the C1 through C11 Procedure document (Level 2). Additional responsibilities include:

- Technology and technical oversight and direction regarding the operations of CIRQ
- Oversight and guidance regarding the technology, as well as the technical aspects, related to ISO 20252:2019 certification
- Support facilitation of impartiality in CIRQ operations from outside influence in order to foster confidence in the auditing it conducts and the decisions it makes regarding certification to ISO 20252:2019.
- Support promotion of ISO 20252:2019 certification to Insights Association members and non-members
- Deliver periodic reports to CIRQ Board of Directors on issues related to technology and the performance of the Quality System's effectiveness in relation to technology and technical matters
- Sign a confidentiality, non-compete, and non-solicitation agreement

Qualifications, Competencies and Knowledge requirements:

- Competent in the interpretation of ISO 20252:2019
- Market, opinion and social research industry knowledge and/or experience
- Strong information technology and technical knowledge and experience pertinent to those technologies and approaches used, and projected to be used in the market, opinion and social research industry. Recent research experience in this area is preferred.
- Report writing skills
- Communication and consultation skills

ISO 20252:2019 Auditors:

A pool of Auditors has been established and is maintained by CIRQ from which certification auditing teams (or individuals) are appointed. The Auditors appointed shall be independent and free of any conflict of interest in performing their function. This role has overall responsibility for audit

management functions as detailed in the C1 through C11 Procedures document (Level 2) for ISO 20252 and/or IS1 - IS10Procedures document (Level 2) for ISO/IEC 27001:2022.

Responsibilities for auditors are listed with ISO 20252 qualifications first, followed by ISO/IEC 27001:2022 auditors.

Additional responsibilities include:

- As part of the Auditor pool, and following assignment of audit functions to the Auditors, Auditors shall keep the Managing Director informed of all activities related to the audit, including changes that may occur throughout the process. Communications shall be undertaken in a timely manner.
- Use of the audit and other support tools provided by CIRQ
- Limit all reporting to the Managing Director, to ensure the interests of all parties are preserved
- Sign a confidentiality, non-compete, and non-solicitation agreement, when first hired as an auditor
- Confirm that they have no conflict of interest related to the assigned client prior to each audit
- Support the facilitation of impartiality in CIRQ operations from outside influence in order to foster confidence in the auditing it conducts and the decisions it makes regarding certification.
- Maintain the confidentiality of all information created or acquired during the course of offering its certification services, unless it is publicly available or when agreed between the client and CIRQ

Qualifications, Competencies and Knowledge requirements:

- Competent in the interpretation of ISO 20252:2019 and/or ISO/IEC 27001:2022
- Trained auditor according to the training standards prescribed by CIRQ
- Market, opinion and social research industry knowledge and/or experience
- General computer skills
- Report writing skills
- Communication and consultation skills

ISO/IEC 27001:2022 Certification Program: Including requirements for ISO/IEC 27701:2019

ISO/IEC 27001:2022 & ISO/IEC 27701:2019 Personnel Knowledge, Competence and Training

ISO/IEC 17021-1:2015, Clauses 7.1.2, 7.1.3, 7.2, Annex A, B, C
ISO/IEC 27006:2015, Clause 7.1.2, 7.2.1.1, 7.2.4

Preface: As of January 2023, ANAB outlined the transition requirements for accredited certification bodies to undertake the transition to the updated requirements reflected in ISO/IEC 27001:2022. Following requirements established in IAF MD 26:2023, this version of the Quality Manual details the transition process for clients who hold ISO/IEC 27001:2013 certification. Details of the process can be found in the Core Requirements IS1 – IS10 noted further in this manual. References will be made throughout to the 2013 and 2022 version of the standard, as certified clients have until October 2025 to transition; prospective clients will be able to certify to the 2013 version of the standard until March 2024. After that time, CIRQ will only certify clients to the 2022 version of the standard.

ISO 27001:2022 Client transition communications	CIRQ commenced communications to its clients regarding this transition and all requirements, beginning in December 2022, and will do so through ongoing general transition communications over the next 3 years. Specific client audit program communications will occur as certified clients submit their intended timeline to transition, and it is expected that all current clients will transition before July 2025 with the majority transitioning throughout 2024.

If a certified client fails to transition prior to the end of the transition period – October 2025 – their certification will be withdrawn. All certifications based on ISO/IEC 27001:2013 shall expire or be withdrawn at the end of the transition period. Clients will be required to undergo a full Stage 1 / Stage 2 ISO/IEC 27001:2022 initial certification audit, and their certification cycle dates will be reestablished upon a successful outcome.

CIRQ has a series of processes for selecting, training, formally authorizing auditors and for selecting and familiarizing technical experts used in the certification activity. The initial competence evaluation of an auditor shall include the ability to apply required knowledge and skills during audits, as determined by a competent evaluator observing the auditor conducting an audit.

The steps below give an overview to the auditor selection process for Clients (e.g., auditees), which is detailed in the Core Process Definitions for ISMS or ISMS/PIMS Certification beginning on page 38 The sections that follow go into detail on the CIRQ process and procedures for determining audit and technical advisor personnel knowledge, competency, behaviors, and training.

1. CIRQ Managing Director reviews the application sent by the auditee.
2. CIRQ Technical Advisor reviews the audit scope and Statement of Applicability
3. CIRQ reviews the recommendations made for "Skill set required for this auditee"
4. CIRQ Managing Director reviews the auditor pool and availability of the auditors
5. CIRQ invites pre-qualified auditors
6. If pre-qualified auditor is not available, then search from the pool of approved auditors
7. Auditor criteria matches and a resume is sent to the auditee
    a. Note: if the assigned Lead Auditor is new to CIRQ, the audit will be observed/witnessed by either/both the CIRQ Managing Director/Technical Advisor when other competency characteristics have been satisfied (see below)
8. Auditee formally accepts the auditor
9. CIRQ assigns auditor to the auditee and introduces both parties
10. CIRQ requests NDA and conflict of interest from the auditor
11. The CIRQ reviews the NDA and conflict of interest document
12. The CIRQ formally assigns the auditor
13. The audit selection process completes when both parties are formally notified, and Application & Audit Program Log are updated

CIRQ's ISO/IEC 27001:2022/ISO 27701:2019 personnel and auditors are required to meet the following criteria for verifying their background experience, specific training or briefing that ensures at least:

a) knowledge of information security
b) technical knowledge of the activity to be audited
c) knowledge of management systems
d) knowledge of the principles of auditing
e) knowledge of ISMS monitoring, measurement, analysis, and evaluation.

NOTE: Further information on the principles of auditing can be found in ISO 19011 and in the Insights Association on-demand auditor training program. Please contact CIRQ's Managing Director for more information, participant fee structure, and access to this program.

CIRQ is a customer-focused certification body, and as such, knowledge, experience, and competency skills are coupled with personal behavior and demeanor when considering the assignment of a client onsite or remote audit. These behaviors include the ability to be professional, ethical, open-minded, diplomatic, collaborative, observant, perceptive, versatile, tenacious, decisive, self-reliant, morally courageous, organized & efficient.

In addition, the following performance indicators, training, and documentation are required to meet the increased requirements to advise and audit for ISO/IEC 27001:2022:

- Knowledge (see table A.1 below)
- Competency
- Professional Experience
- Client Feedback
- Interviews
- Witness Audits
- Examinations & Evaluations

Knowledge:
Overall, it is CIRQ policy that auditors (independent contractors) for ISO/IEC 27001:2013 / ISO/IEC 27001:2022 and ISO/IEC 27701:2019 are responsible for knowledge of all requirements contained in ISO/IEC 27001:2013 / ISO/IEC 27001:2022 ISO/IEC 27701:2019, providing proof of their lead auditor knowledge, skills, and training, and for maintaining their education and competency strengths to serve as lead auditor.

Additionally, all members of the audit team shall have knowledge of: all controls contained in ISO/IEC 27002 and their implementation, categorized as: information security policies; organization of information security; human resource security; asset management; access control, including authorization; cryptography; physical and environmental security; operations security, including IT-services; communications security, including network security management and information transfer; system acquisition, development and maintenance; supplier relationships, including outsourced services; information security incident management; information security aspects of business continuity management, including redundancies; compliance, including information security reviews.

Table A.1 below provides an overview of CIRQ personnel knowledge – Managing Director, Technical Advisor, Lead Auditor – as it relates to their role within the certification process.

Table A.1 Knowledge for ISMS & PIMS Auditing and Certification

Knowledge and skills	Certification functions		
	CIRQ Managing Director: Conducting the application review to determine audit team competence required, to select the audit team members, and to determine the audit time	***CIRQ Technical Advisor for certification decisions:*** Reviewing audit reports and making certification decisions	***CIRQ Lead auditor:*** Auditing and leading the audit team
Knowledge of business management practices			x
Knowledge of audit principles, practices, and techniques	x	x	x
Knowledge of ISO/IEC 27001:2022	x	x	x
Knowledge of ISO/IEC 27002:2022	x	x	x
Knowledge of ISO 27701:2019	x	x	x
Knowledge of CIRQ processes	x	x	x
Knowledge of client's business sector	x	x	x
Knowledge of client products, processes, and organization	x		x
Language skills appropriate to all levels within the client organization	x		x
Note-taking and report-writing skills	x		x
Presentation skills	x		x
Interviewing skills			x
Audit Management skills			x
NOTE: Risk and complexity are other considerations when deciding the level of expertise needed for any of these functions.			

Competency:
CIRQ will also evaluate the numerous sources listed below to determine ongoing competency, as well as considerations to grow the auditor pool. ISO/IEC 27001:2013 / ISO/IEC 27001:2022 and ISO/IEC 27701:2019 Auditors and Technical Advisors are required to have a Competency Form in their personnel folder on the CIRQ Intranet, which will be reviewed before the assignment of each new client audit engagement.

New candidates for independent contractor auditors must demonstrate knowledge and competency prior to any audit assignment within CIRQ and must submit an CIRQ Auditor Competence Form which documents:

- Resume or CV: professional education or training to an equivalent level of university education; at least four years full time practical workplace experience in information technology, of which at least two years are in a role or function relating to information security
- Lead Auditor & Industry Certifications: successful completion of at least five days of training, the scope of which covers ISMS audits and audit management, resulting in a Lead Auditor Certificate from an approved issuing authority
- Audit Log: experience in the entire process of assessing information security prior to assuming responsibility for performing as an auditor. This experience should have been gained by participation in a minimum of four ISMS certification audits, including re-certification and surveillance audits, for a total of at least 20 days of which at most 5 days may come from surveillance audits. The participation shall include review of documentation and risk assessment, implementation assessment and audit reporting, and relevant and current experience
- Training: keeps current knowledge and skills in information security and auditing up to date through continual professional development provided by CIRQ throughout the year.

Resumes/CVs

CIRQ will keep the resume/CV within the personnel folders of all current ISO/IEC 27001:2013 / ISO/IEC 27001:2022 and ISO/IEC 27701:2019 auditors as a record of knowledge, showing work experience, audit experience, education and training. Other records, including past performance appraisals and certificates of completion for subject matter expert training, can also serve when added to the primary resume or CV document. These documents will also be utilized during the audit planning process, for formal client approval of the selected auditor.

Client Feedback

Upon completion of the assigned audit, a CIRQ Client Feedback form is sent clients requesting general questions about auditor performance, knowledge and competency through the entire audit planning process. These are stored in the client folders on the CIRQ intranet and taken into account during the annual assessment period, typically distributed in January, evaluating the previous year's performance.

Interviews

CIRQ's managing director, and technical advisor, will undertake interviews of new auditors as the CIRQ business grows. These interviews would likely be via phone, unless in person can be arranged with little or no additional effort. Interviews will set the baseline for auditor roles within CIRQ, brief role descriptions, followed by more formalized documentation (e.g., CIRQ Handbook, CIRQ Quality Manual) for review.

Witness Audits & Onsite Evaluation of New Auditors

CIRQ will strive to undertake at least one Witness Audit per calendar year of the ISO/IEC 27001:2013 / ISO/IEC 27001:2022 and ISO/IEC 27701:2019 audit staff. This can be done either in person at a client audit site, or via remote audit using web conferencing software (ICT), both with prior planning and approval by client for Observers during the audit. The Client is permitted to request the participation of observers during an audit, as appropriate to the facilitation of the audit schedule and scope (e.g., project managers, annex owners, quality, and compliance representatives, etc.). CIRQ may also request the Client to make provisions, where applicable, to accommodate the presence of observers (e.g., accreditation assessors or trainee auditors). Witness audits will be executed with the same level of confidentiality as is expected in the in-person audit environment.

For the evaluation of new auditors, either CIRQ's Managing Director or assigned Technical Advisor will observe the candidate auditor in person or remotely via ICT. A Witness Audit Report will be drafted by

the assigned observer to determine initial competence which includes the ability of the auditor to apply required knowledge and skills during audits. Once competence is determined by a competent evaluator observing the auditor conducting an audit, the new auditor will be assigned to lead CIRQ ISMS audits.

Examinations & Evaluations
CIRQ maintains an ISO/IEC 27001:2022 and ISO/IEC 27701:2019 Auditor Evaluation, Qualification Examination, and Selection process for the initial competence review, and ongoing monitoring of competence and performance of all personnel involved in the management and performance of audits and other certification activities, applying the determined competence criteria. The initial review process for personnel includes evaluation by the Managing Director, Technical Advisor, and CIRQ Board Chair.

- Initial Competence Evaluation: Before a formal hiring decision is made, CIRQ will assign a Sample Audit. Using a completed CIRQ ISMS Application form (fictitious company) and the CIRQ Audit Report template, the Auditor will fill it out for a Non-Conformance finding that there had been no management review meeting performed in the previous year. This will be reviewed and approved by the assigned CIRQ Technical Advisor and CIRQ Managing Director. *A witness audit of a prospective auditor by the CIRQ Managing Director will be accepted during an initial competence evaluation, and a report will be generated with observations from the CIRQ MD. The report will be filed within the personnel folder for the new auditor as part of the personnel file.

The completed CIRQ Comprehensive Auditor Competence Form will be approved and signed by CIRQ's Managing Director and filed in the Auditor's personnel file stored on the CIRQ Intranet.

CIRQ documents and monitors the process for ongoing auditor competence through the formal Annual Auditor Assessment, performed annually in January reflecting on the previous year. CIRQ's Managing Director will schedule annual performance meetings in January, reflecting on the previous year. It is the goal to complete the process by Jan 31 annually. The assessment form is composed of 4 sections:

- Section 1: During the interview, the MD will discuss the listed questions and capture input. The draft performance review will be sent via email for the auditor's responses.
- Section 2: CIRQ will input all of Section 2. The auditor is open to comment on the 3 evaluation categories.
- Section 3: Any disputes or conflicts that arise from the interview and responses will be documented on the form in Section 3.
- Section 4: If there are no comments for Section 3, the MD and CIRQ auditor will sign and date the form and it will be filed in the audit's personnel folder on the CIRQ Intranet.

Currently, all CIRQ personnel involved in the ISO/IEC 27001:2013 / ISO/IEC 27001:2022 and ISO/IEC 27701:2019 program have sought their Lead Auditor/Technical Advisor training from external providers. CIRQ maintains all evidence of training, certifications, resumes/CVs and other related support documentation for management system personnel (e.g., ISO/IEC 27001:2022, ISO/IEC 27701:2019) are maintained within the CIRQ Audit Program Log and in the CIRQ Personnel files stored on the CIRQ Intranet.

ISO/IEC 27001:2013 / ISO/IEC 27001:2022 Technical Advisors for Certification Decisions

ISO/IEC 17021-1, 7.1, 7.2, Annex A, Annex D
ISO/IEC 27006:2013 7.2.1 IS 7.2

CIRQ has processes for selecting, training, formally authorizing auditors and for selecting and familiarizing technical experts used in the certification activity. The initial competence evaluation of an auditor shall include the ability to apply required knowledge and skills during audits, as determined by a competent evaluator observing the auditor conducting an audit. Technical Advisors for Certification Decisions shall also have knowledge of management systems in general, audit processes and procedures and audit principles, practices, and techniques.

Additional responsibilities include:

- Oversight and guidance regarding the technology, as well as the technical aspects, related to ISO/IEC 27001:2013 / ISO/IEC 27001:2022 and ISO/IEC 27701:2019 certification decisions
- Support facilitation of impartiality in CIRQ operations from outside influence in order to foster confidence in the auditing it conducts and the decisions it makes regarding certification to ISO/IEC 27001:2013 / ISO/IEC 27001:2022 and ISO/IEC 27701:2019.
- Serve as technical review for initial and recertification ISO/IEC 27001:2013 / ISO/IEC 27001:2022 and ISO/IEC 27701:2019 certification decisions in support of final certification decision performed by Managing Director
- Support promotion of ISO/IEC 27001:2013 / ISO/IEC 27001:2022 and ISO/IEC 27701:2019 certification to Insights Association members and non-members
- Deliver periodic internal audit reports to CIRQ Managing Director and Board of Directors on issues related to technology and the performance of the Quality System's effectiveness in relation to its ISO/IEC 27001:2013 / ISO/IEC 27001:2022 and ISO/IEC 27701:2019 certification programs
- Sign a confidentiality, non-compete, and non-solicitation agreement

Qualifications, Competencies and Knowledge requirements:

- Competent in the interpretation of ISO/IEC 17021-1:2015, ISO 27006, ISO/IEC 27001:2022 and ISO/IEC 27701:2019.
- ISMS specific documentation structures, hierarchy and interrelationships; information security management related tools, methods, techniques and their application; information security risk assessment and risk management; processes applicable to ISMS and PIMS
- Strong information technology and technical knowledge and experience pertinent to those technologies and approaches used, and projected to be used in the market, opinion and social research industry. Recent research experience in this area is preferred.
- Report writing skills
- Communication and consultation skills

ISO/IEC 27001:2013 / ISO/IEC 27001:2022 and ISO/IEC 27701:2019 Lead Auditors

ISO/IEC 17021-1, 7.1, 7.2, Annex A, Annex D
ISO/IEC 27006:2013 7.2.1 IS 7.2

CIRQ selects auditors to conduct ISMS audits that shall possess the following criteria to ensure that each auditor meets the following requirements:

- Professional education or training to an equivalent level of university education
- At least four years full time practical workplace experience in information technology, of which at least two years are in a role or function relating to information security
- Trained successfully by completing at least five days, the scope of which covers ISMS audits and audit management

- Experienced in the entire process of assessing information security prior to assuming responsibility for performing as an auditor. This experience should have been gained by participation in a minimum of four ISMS certification audits, including re-certification and surveillance audits, for a total of at least 20 days of which at most 5 days may come from surveillance audits. The participation shall include review of documentation and risk assessment, implementation assessment and audit reporting
- Relevant and current experience
- Current knowledge and skills in information security and auditing up to date through continual professional development
- Knowledge of certification body's processes
- Knowledge of client's business sector, including client products, processes and organization
- Language skills appropriate to all levels within the client organization

CIRQ Personnel

Names, qualifications, and experience of CIRQ Management, Auditors or Advisors are available by referencing files established and maintained on the CIRQ Intranet site (see CIRQ Records/Personnel Records folder).

References:

- CIRQ Core Procedures, C1-C11 – ISO 20252:2019 (Level 2)
- CIRQ Core Procedures, IS1-IS10 – ISO/IEC 27001:2022 (Level 2)
- CIRQ Support Procedures, S1-S11 (Level 2)
- CIRQ Auditor Training Manual-Version April 2018, August 2018 Training Materials, Feb/March 2019 Training Materials, 2020-2021 Training
- FC 2005 1.0 ISO/IEC 27001:2022 Audit Program Log 2022
- TS 7006 1.1 Comprehensive Auditor Competence Form
- CIRQ Operating Agreement
- IRS Group Exemption for CIRQ
- Independent Contractor Confidentiality, Non-compete, and Non-solicitation Agreement (TS7001)
- Non-Disclosure/Declaration of No Conflict (FC5001)

IX. Quality System Structure

ISO/IEC 17065:2012, Clause 8.1
ISO/IEC 17021-1:2015, Clauses 8, 10.2 Option A

CIRQ has established, documented and maintains a Quality System which is regularly reviewed to identify ways in which its effectiveness can be improved in accordance with the requirements of ISO/IEC 17065:2012 and ISO 17021-1:2015.

CIRQ utilizes an Intranet cloud solution for all quality system, personnel and operational documents. The CIRQ Managing Director has super-administrative rights to assign specific client folders to auditors during the audit planning process to which they are assigned. Permissions for the system are password protected to guard the confidentiality of the client folders contained within.

Documentation for this system exists at several levels that start with a very broad and general perspective at Level 1 and become more detailed and specific at subsequent levels. These levels are described below.

Level 1 Documents consist primarily of the Quality Policy, the Quality Objectives and this Quality Manual, along with several other documents that are controlled and only change on a very infrequent

basis such as the Schedule of Fees. The Quality Manual contains the Quality Policy and the Quality Objectives and also references other policies and the processes constituting the Quality System, which have been established to conform to the requirements of ISO/IEC 17065:2012 and ISO/IEC 17021-1:2015.

The Quality Manual also contains references to QS procedures (Level 2 Documents), which further detail the processes defined later in this document.

Level 2 Documents include detailed procedures required by ISO/IEC 17065:2012 and ISO/IEC 17021-1:2015. They define steps taken to ensure the quality of services offered by CIRQ, show who is responsible for implementing the procedure, and indicate timelines for key steps of various procedures. Related forms, checklists, templates, etc., reference materials, and required records are referenced in the procedures. This level covers both Core and Support procedures.

Level 3 Documents are the standard Forms, Checklists, Templates, and Workbooks, required when implementing particular tasks of a procedure where the absence of such documents may adversely affect quality.

Level 4 Documents are the Records created as a result of the Quality System to provide objective evidence of compliance to requirements and of the effective operation of the QS. Level 4 documents include all records required by ISO/IEC 17065:2012 and ISO/IEC 17021-1:2015.

Advisory Notes: Advisory Notes are issued on an as required basis to clients, auditors and other CIRQ staff. The intention of the Advisory Note is to standardize understanding and approach by clients, CIRQ auditors, and other CIRQ staff; or when there are changes to the ISO 20252:2019, ISO/IEC 27001:2022 and ISO/IEC 27701:2019 standards.

CIRQ has identified 11 Core Procedures for ISO 20252:2019, 10 ISMS/PIMS Core Procedures for ISO/IEC 27001:2022 and ISO/IEC 27701:2019, and 11 Support processes needed for its QS to provide consistent auditing and certification services to its customers. These Core & Support processes address the requirements of *Clauses 7.11, 7.12, 8.3, 8.6, and 4.1.3, 6.1, 7.2, 7.2, 7.4, 7.4.6, 7.6, 7.9, 7.10, 7.13,* of *ISO/IEC 17065:2012 and Clauses 9.6.5, 9.9, 10.2.4, 10.2.6, 7, 9.2.2, 9.1.1-9.1.2, 9.1.3, 6, 9.5, 9.6, 9.7, 9.8 and Annex A of ISO IEC 17021:2015:1*.

All are outlined in the next section of this manual.

References:

- S6 Documentation Procedure
- CIRQ Intranet Site

X. Operations

ISO/IEC 17065:2012, Clause 7
ISO/IEC 17021-1:2015, Clause 7

The certification schemes covered in this manual comply with ISO 17065:2012 and ISO/IEC 17021-1:2015 and ISO 27006 respectively and is in accordance with the *Accreditation requirements for organizations providing certification services to ISO 20252: 2019 Market, opinion and social research including insights and data analytics within the territorial jurisdictions of Australia, UK, and USA* (June 2020) for certification bodies certifying to ISO 20252:2019. It shall apply to all companies seeking certification, and these companies shall meet the requirements of ISO 20252:2019 and/or ISO/IEC 27001:2022 and ISO 27701:2019. These companies will also comply with the appropriate code of standards for the industry associations in which they hold membership and comply with appropriate laws/regulations based on their geographic coverage.

Following is a high level outline describing the process of certification beginning with the initial request from a prospective client to the issue of the Certificate of Compliance, and through the 3 year cycle of Surveillance Audits and the Re-Certification Audit. Also included in the following outline is a description of the Support Processes needed for CIRQ's quality system. Refer to the C1-C11 Procedures-ISO 20252 document and the S1-S11 Procedures documents (Level 2) for a more detailed explanation of CIRQ's certification process and support procedures.

See also the Core IS 1 - IS 9 Procedures – ISO/IEC 27001:2022 document (Level 2) for a detailed explanation of the certification process as it relates to this standard, and requirements specific to ISO/IEC 27701:2019.

The Managing Director has overall responsibility for the Core procedures, supported by auditors on specific steps, and for the Support Procedures.

References:

- Scheme document: *Accreditation requirements for organizations providing certification services to ISO 20252: 2019 Market, opinion and social research including insights and data analytics within the territorial jurisdictions of Australia, UK, and USA. (June, 2020)*

A. Core (C) Process Definitions for ISO 20252

C1. Application for Certification

ISO/IEC 17065:2012, Clauses 4.1.2, 7.2 and 7.3

Companies seeking to be certified to ISO 20252:2019 shall have implemented a Quality System including documentation meeting the requirements of this standard; and shall be able to demonstrate approximately 3 months compliance against the standard immediately preceding the date of the Pre-Assessment, in order to show the sustainability of their system. The company then contacts CIRQ to make arrangements for required audits and certification. CIRQ shall require companies interested in becoming certified to electronically submit an RFQ and Authorization to Proceed, as well as the application fee to begin the process.

CIRQ shall review the RFQ and Authorization to Proceed to confirm the submitted Statement of Applicability and any requested exemptions to particular Annexes. CIRQ shall then define the objective and criteria for the audit, obtaining Client agreement on same. CIRQ's Managing Director (MD) has primary responsibility for this process.

Required Records:

- Completed RFQ (FC1001 2.1 Request for Quotation)
- Authorization to Proceed (FC1003 1.7 Authorization to Proceed)

References:

- Detailed procedures for the Application process in the C1-C11 Procedure document (Level 2)
- Audit & Certification Fees DC1001
- Audit Journey DC1002

C2. Self-Assessment

In order to assist in determining if the company is ready for ISO certification and has the required documentation in place with sufficient evidence to support it, the applicant company will be asked to complete a self-assessment which aligns with all requirements of the specific standard to which they wish to be certified. This Self-Assessment once completed and returned to CIRQ, along with the applicant's Quality Manual, will help determine readiness for audit, the Audit Schedule, and will be used by the Auditor to complete the Pre-Assessment.

When the Self-Assessment is returned along with the Quality Manual, the auditor (assessor) for the Pre-Assessment is assigned by the Managing Director, and the MD confirms that there is no conflict of interest present. The completed Self-Assessment and Quality Manual are made available to the Auditor via the CIRQ Intranet site, along with any other required documents that were submitted with the Self-Assessment.

When the Self-Assessment form is sent to the applicant, the applicant company will also be sent the invoice for the Pre-Assessment which shall be paid prior to beginning the Pre-Assessment.

Required Records:

- Completed Self-Assessment (WBC 3003 1.6 Self & Pre-Assessment Report Workbook ISO 20252:2019)
- Applicant's Quality Manual
- Declaration of No Conflict (FC5001)
- Standard Certification Agreement (TC4001 2.1 CIRQ Standard Certification Agreement 2019)

References:

- Detailed procedures for the Self-Assessment in the C1-C11 Procedure document (Level 2)

C3. Pre-Assessment

The Pre-Assessment will begin when payment for this stage is received. The objective is again to help determine that the applicant's Quality System appears to meet a large majority of the requirements of ISO 20252:2019, and that their system has been in place for approximately 3 months prior to the on-site Certification Audit. The Pre-Assessment process takes place off-site and involves a review of the Self-Assessment and the company's Quality Manual by the assigned auditor. A Pre-Assessment report is prepared by the auditor. Through this Pre-assessment CIRQ requires a company to indicate compliance with the Core Framework of the ISO 20252:2019 Standard (Clause 4), as well as with the various Annexes to which the client company attests—in order to move on to the Certification Audit. Any areas of shortfall regarding compliance are pointed out in the Pre-Assessment Report.

This report is sent to CIRQ management for review and approval, and then sent to the applicant company within 2 weeks following CIRQ's receipt of the Self-Assessment. Any discrepancies pointed out in the Pre-Assessment Report need to be addressed, corrected and confirmed as corrected prior to the on-site audit.

Required Records:

- Pre-Assessment Report (WBC 3003 1.6 Self & Pre-Assessment Report Workbook ISO 20252:2019)
- CLC 7001 1.4 Audit Program Checklist

References:

- Detailed procedures for the Pre-Assessment in the Core 1-11 Procedure document (Level 2)
- Auditor Training Materials, August 2018 and Feb/March 2019
- ISO 20252:2019 Standard

C4. Planning for Audits

ISO/IEC 17065:2012, Clause 7.4.1

Preparation for the Certification Audit begins when the Pre-Assessment is complete, and any discrepancies identified at this time have been corrected by the Client.

At this stage, and in most cases, the Lead Auditor should be the same person as the one who conducted the Pre-Assessment. If additional auditors are needed for the actual audit, the Managing Director assigns the auditor(s), and confers with the audit team about audit logistics and locations. The Managing Director also confirms that there is no conflict of interest on the part of the additional auditors. Where practical, CIRQ will strive to retain the same Lead Auditor for a 3-year cycle of audits. This Lead Auditor may be changed at the Re-Certification Audit to provide a fresh perspective on the customer's Quality System.

The Audit Schedule is prepared and sent to the client for their signature, along with the Certification Agreement and an invoice for 50% of the Certification Audit fee. When these two signed documents are received back from the Client and payment of the 50% of audit fees are received, CIRQ can proceed with the on-site audit.

Required Records:

- Audit Schedule (FC4001)
- Declaration of No Conflict (FC5001)

References:

- Detailed procedures for Audit Planning in the Core 1-11 Procedure document (Level 2)
- Auditor Training Manual Version April 2018 and Training Materials dated August 2018 and February - April 2019
- Auditor Workbook (WBC4003 1.7)
- Applicant's RFQ (FC1001 2.1 Request for Quotation)
- Completed Self and Pre-Assessment Report (WBC 3003 1.6 Self & Pre-Assessment Report Workbook ISO 20252:2019)

C5. Execution of Audits (Certification, Surveillance, and Re-Certification)

ISO/IEC 17065:2012, Clauses 5.1.4, 7.4, 7.5, 7.9

The Certification Audit shall take place at the Company's headquarters location and based on the Audit Schedule, at a sampling of other non-headquarter locations. In selecting these other locations, both the size of the location (i.e., # of staff) and where the attested Annexes are produced should be considered. Processes and activities carried out by the Company, related to the Statement of Applicability for ISO 20252:2019, and that most significantly affect the quality of the company's product or service shall be included in the Certification Audit.

Where processes and activities relate to projects, a sufficient number of projects, or sampled sections of projects, shall be audited to enable a decision to be made relating to compliance or non-compliance to the audit criteria of any particular Annex. If there is no project available to audit for a specific Annex for two years in a row, the Statement of Applicability must be revised.

The records reviewed in the audit should also cover both current and closed projects. Companies shall have approximately 3 months of project records including completed projects in order to undergo a Certification Audit. There shall be adequate documentation to demonstrate the sustainability of the

company's quality system.

The first Surveillance Audit, after certification, shall be carried out within a period not greater than twelve (12) months after the date of certification and thereafter at intervals of not more than twelve (12) months. Surveillance audits shall be conducted at least once a calendar year, except in recertification years.

Each Surveillance Audit shall cover:

- A review of the Statement of Applicability to confirm it still appropriately describes the services offered by the company to their clients
- A review of the most critical activities and processes related to clause 4, the Core Framework, as well as one or more projects representing each Annex to which the company attested.
- A review of procedures connected with any Area of Concern or Non-Conformance noted in the previous audit
- Any changes made to the Company's processes and procedures since the last audit
- Any additional requirements that now need to be met based on revisions to the standard

Over a period of not more than three (3) years, the Surveillance Audits shall cover **all** activities and processes carried out by the Company which are covered by the Statement of Applicability, as well as **all** locations of the Company. Again, if there is no project available to audit for a specific Annex for two years in a row, the Statement of Applicability must be revised.

After a period of not more than three (3) years from the date of certification, a Re-Certification Audit shall be carried out and shall cover **a majority of all** activities and processes carried out by the Company which are covered by the Statement of Applicability for ISO 20252:2019, and which significantly affect the quality of the product or service offered by the company; plus a review of the findings of all Surveillance Audits carried out since certification, or the last re-certification. Over the course of this three (3) year cycle all of the Company's locations (other than the headquarters location) shall be audited at least once. The headquarters location shall be part of every audit over the 3-year cycle.

An Audit Report will be prepared following each audit, as described in the C6 process described below.

Required Records:

- Completed Auditor Workbook (WBC4003 1.7)
- CLC 7001 1.4 Audit Program Checklist

References:

- Auditor Workbook (WBC4003 1.7)
- Completed Self and Pre-Assessment Report (WBC 3003 1.6 Self & Pre-Assessment Report Workbook ISO 20252:2019)
- Auditor Training Manual Version April 2018 and Training Materials from August 2018 and February - April 2019
- ISO 20252:2019 Standard

C6. Preparation of Audit Reports

ISO/IEC 17065:2012, Clauses 7.4.6, 7.4.9, 7.5

Upon completion of each audit, the assigned Auditor (or the Lead Auditor) shall prepare a report to indicate conformance (or Non-conformance) with all requirements of the ISO standard.

This report will identify any Non-Conformance or Area of Concern that must be addressed within a specified time limit, and whether additional auditing will be required before certification can be granted

or renewed. A Non-conformance must be addressed within 4 months of the audit report; an Area of Concern must be addressed by the next scheduled annual audit. Within the Audit Report, the client is directed to utilize the Section A: Status of Non-Conformance to document the Non-conformance and its remediation. The report may also include opportunities for improvement and observations about the company's quality system.

This report will be uploaded to the CIRQ Intranet for the MD's review, and following CIRQ's review and approval, it will be sent to the customer along with notification regarding certification status. The Auditor Workbook should be uploaded to the CIRQ Intranet at the same time as the Draft report.

Required Records:

- Audit Report (WBC6001 Audit Report Workbook 1.6)
- CLC 7001 1.4 Audit Program Checklist

References:

- Auditor Workbook (WBC4003 1.7)
- Audit Report Workbook (WBC6001 Audit Report Workbook 1.6)
- Auditor Training Manual Version April 2018 and Training Materials from August 2018 and February - April 2019

C7. Certification Process

ISO/IEC 17021-1:2015, Clauses 8, 9.5, 9.6
ISO 17065:2012, Clauses 4.1.3, 7.6, 7.7, 7.8, 7.11

a). Granting, Maintaining, Extending, Renewing and Reducing Certification

When the assigned Auditor (or Lead Auditor) is satisfied that the Company's QS documentation and implementation meet the requirements of the ISO Standard, a recommendation shall be made regarding certification in the report they submit to CIRQ. Any Non-Conformances identified during the audit shall be resolved before certification is granted, maintained or renewed. CIRQ's Managing Director determines an initial or recertification certification audit report is pending review and approval. If there are no additional questions or concerns during the review, approval is granted and documented on the report. If there are questions/concerns, the Managing Director conferences with the Lead Auditor, as appropriate, to discuss and clarify questions. The Lead Auditor will reference the Annex A: Reference Controls Objectives section of the audit report for real-time notes and findings documented from the audit for clarification and satisfaction that issues have been resolved.

On approval of the report, the CIRQ Managing Director will send the official report and a certificate will be issued (following the Initial audit and each subsequent Re-Certification audit) and the CIRQ Certification Register on CIRQ's website will be updated with the Company's name and Statement of Applicability details. The issue of a Certificate of Compliance in no way suggests or implies that any certified activity, process, product or service of the Company is approved by CIRQ or Insights Association. The Company must establish and maintain procedures for notifying their clients of any goods or services provided or produced outside the certification Statement of Applicability registered with CIRQ.

Certification to the specified ISO standard is valid for three years subject to ongoing Surveillance Audits, which usually occur at twelve-month intervals. CIRQ will advise certified companies of any change in their Audit schedule. A Re-Certification Audit of the Company's Quality System will be undertaken prior to the expiration of certification. A successful Re-Certification Audit will result in renewal of the Company's Certificate of Compliance for a further three years. However, where the Surveillance Audits or Re-Certification Audit cannot be

conducted in the timeframe mentioned above, CIRQ will grant a reasonable extension, in most cases not more than 60 days, until the Surveillance or Re-Certification Audit can be scheduled and new certificates issued for the Re-Certification Audit.

The certified company has the right to reduce or expand its Statement of Applicability, at any time. Any requests to do so must be made in writing to CIRQ.

b). Issuing the Certificate of Compliance certification document(s).
Issued by CIRQ's Managing Director after all requirements are satisfied as listed in section a) above, the certificate document will be prepared and identify the following:

- the name and geographical location of each certified client (or the geographical location of the headquarters and any sites within the scope of a multi-site certification).
- the effective date of granting, expanding, or reducing the scope of certification, or renewing certification which shall not be before the date of the relevant certification decision.

NOTE The certification body can keep the original certification date on the certificate when a certificate lapses for a period of time provided that:
— the current certification cycle starts, and expiry date are clearly indicated.
— the last certification cycle expiry date be indicated along with the date of recertification audit.

- The expiry date or recertification due date consistent with the recertification cycle
- The CIRQ issued certificate unique identification code
- Certification to ISO/IEC 27001:2022 language: "…And operates an Information Security Management System in compliance with ISO/IEC 27001:2022."
- the scope of certification with respect to the type of activities, products, and services as applicable at each site without being misleading or ambiguous. In most cases, the scope statement for the ISMS is related only to ISO/IEC 27001:2022 certification
- CIRQ's name, address, and certification of the specific standard. In the case of CIRQ's accreditation through the ANSI National Accreditation Board, an accreditation symbol will be included with the provision it is not misleading or ambiguous and leads the client to imply, promote or communicate, that its management system is accredited.
- any other information required by the standard and/or other normative document used for certification.

In the event of issuing any revised certification documents, CIRQ will communicate the implementation of the revised documents and issue the revision from any prior obsolete documents shall include the direction to destroy old documents and the revision of CIRQ's online Registry of Certified Clients.

c). Suspension or Withdrawal of Certification
CIRQ reserves the right to suspend or withdraw the Certificate of Compliance at any time. The Certificate may be suspended should the Company:

a. fail to complete corrective actions within the agreed time.
b. misuse the Certification Mark(s).
c. fail to comply with the financial requirements of the Agreement entered into with CIRQ; or
d. brings CIRQ into disrepute in any way.

CIRQ will assist the Company in taking appropriate remedial steps following suspension of the Certificate of Compliance, but should Company fail to do so within a reasonable time frame the Certificate of Compliance will be withdrawn.

Where withdrawal of Certification occurs, CIRQ will update its Register and website to make

note of the withdrawal, request the return of the Certificate, and request that the Company discontinue the use of the Certification Mark(s) in any way. Certificates and marks of compliance remain the property of CIRQ.

Required Records:

- CLC 7001 1.4 Audit Program Checklist
- Certification Register on CIRQ Internet site
- Certificate of Compliance
    - TC7001 1.3 CIRQ Certificate of Compliance 20252:2019
    - TC7002 1.0 CIRQ Certificate of Compliance ISO/IEC 27001:2022
- Letter explaining Certification, Denial of Certification, Suspension of Certification, or Withdrawal of Certification

References:

- Certificate of Compliance
    - TC7001 1.3 CIRQ Certificate of Compliance 20252:2019
    - TC7002 1.0 CIRQ Certificate of Compliance ISO/IEC 27001:2022
- Certification Mark(s) and CIRQ logo
- S1 Terms of Use for CIRQ Certification Mark(s)

C8. Soliciting Customer Feedback

The Managing Director will contact each customer within 2 weeks following delivery of the Audit report to solicit their feedback, via email. This communication shall follow a prescribed outline of discussion points, shall be documented, and a record of the communication shall be maintained in the customer's file. Follow up calls will be made where deemed necessary. The Managing Director shall share this feedback with the auditor(s) as appropriate.

Required Records:

- Completed Customer Feedback Form (FC8001)

C9. First Surveillance Audit

ISO/IEC 17065:2012, Clause 7.9

This audit shall take place 12 months following the Initial Certification Audit. Planning for it will begin approximately 3-4 months in advance of the 12 month mark. More detail about the process related to this audit can be found in the C1-C11 procedures of Level 2 of the CIRQ Quality System.

Required Records:

- See steps C4-C8 above

References:

- See steps C4-C8 above
- Results of Initial Certification Audit

Second Surveillance Audit

ISO/IEC 17065:2012, Clause 7.9

This audit shall take place 12 months following the First Surveillance Audit. Planning for it will begin approximately 3-4 months in advance of the 12 month mark. More detail about the process related to this audit can be found in the C1-C11 procedures of Level 2 of the CIRQ Quality System.

Required Records:

- See steps C4-C8 above

References:
- See steps C4-C8 above
- Results of Initial Certification Audit
- Results of 1st Surveillance Audit

C10. Re-Certification Audit

ISO/IEC 17065:2012, Clause 7.9

This audit shall take place 12 months following the Second Surveillance Audit. Planning for it will begin approximately 3-4 months in advance of the 12 month mark. More detail about the process related to this audit can be found in the C1-C11 procedures of Level 2 of the CIRQ Quality System.

Required Records:
- See steps C4-C8 above

References:
- See steps C4-C8 above
- Results of Initial Certification Audit
- Results of 1st Surveillance Audit
- Results of 2nd Surveillance Audit

C11. Certification Body Transfer

Clients wishing to transfer their certification to CIRQ shall complete the Authorization to Proceed for Certification Body Transfer (FC1004) form and return it with the indicated fee. CIRQ then requests the company's quality manual, key processes and recent audit reports for review. Client is notified that any outstanding non-conformances must be resolved prior to certification body transfer.

For all transfers, except Australian companies, a review of the Quality Manual, procedures and previous audit report is performed by an assigned Auditor, and client is billed for ½ audit day.

For an Australian Transfer: Transfer Fee is Charged, Australian auditor reviews the same documents per the Australian Audit Certification Procedure.

Required Records:
- Authorization to Proceed for Certification Body Transfer (FC1004)
- Client's Quality Manual and key processes
- Client's recent audit reports

Core Processes for ISMS or ISMS/PIMS Certification

CIRQ has implemented a series of core processes that should take place over the lifecycle of all audit activities. *ISO/IEC 17021-1:2015 Annex E and ISO 27006:2015* provides guidance for the core process progression listed in IS1 – IS9.

Preface: As of January 2023, ANAB outlined the transition requirements for accredited certification bodies to undertake the transition to the updated requirements reflected in ISO/IEC 27001:2022. Following requirements established in IAF MD 26:2023, this version of the Quality Manual details the transition process for clients who hold ISO/IEC 27001:2013 certification. Details of the process can be found in the Core Requirements IS1 – IS10 noted further in this manual. References will be made

throughout to the 2013 and 2022 version of the standard, as certified clients have until October 2025 to transition; prospective clients will be able to certify to the 2013 version of the standard until March 2024. After that time, CIRQ will only certify clients to the 2022 version of the standard.

ISO 27001:2022 Client transition communications	CIRQ commenced communications to its clients regarding this transition and all requirements, beginning in December 2022, and will do so through ongoing general transition communications over the next 3 years. Specific client audit program communications will occur as certified clients submit their intended timeline to transition, and it is expected that all current clients will transition before July 2025 with the majority transitioning throughout 2024.

If a certified client fails to transition prior to the end of the transition period – October 2025 – their certification will be withdrawn. All certifications based on ISO/IEC 27001:2013 shall expire or be withdrawn at the end of the transition period. Clients will be required to undergo a full Stage 1 / Stage 2 ISO/IEC 27001:2022 initial certification audit, and their certification cycle dates will be reestablished upon a successful outcome.

Core Process IS1. Submission & Review of Application for Certification

ISO 17021-1:2015, Clauses 9.1.1-9.1.2
ISO 27006:2015, Clauses IS 9.1.1., IS 9.1.3
IAF MD 4:2018, Issue 2, Clause 2

CIRQ requires prospective ISO/IEC 27001:2013 / ISO/IEC 27001:2022 and ISO/IEC 27001:2022 + ISO/IEC 27701:2019* certification clients to have a documented and implemented ISMS for at least six months which conforms to the standard. The client is also required to have completed one internal audit and full management review to be considered eligible to audit.

*Note: The ISO/IEC 27701:2019 certification is a security extension to ISO/IEC 27001:2013 / ISO/IEC 27001:2022 and **cannot** be obtained without previous or concurrent ISO/IEC 27001 initial audit, added to an ISO/IEC 27001:2013 / ISO/IEC 27001:2022 surveillance or recertification audit. ISO/IEC 27701:2019 is the privacy information management system standard, and for companies outside of the EU (i.e., US, Canada, Asia, etc.), is a solution that maps to the General Data Protection Regulation (GDPR). Compliance with ISO/IEC 27701:2019 is based on adherence to these requirements and with the requirements in ISO/IEC 27001:2013 / ISO/IEC 27001:2022.

CIRQ shall exchange information between itself and the certification client. Companies interested in becoming certified can electronically submit a CIRQ Management System Application. Based on the returned Application and after review of application by the Managing Director, details of client application including full staff count, effective personnel, hours of operation (including shift work), and organization products and services as appropriate within audit scope and Statement of Applicability are confirmed. Managing Director acknowledges receipt and scopes out audit program ISO/IEC 27006 Annex B to determine complexity and days.

CIRQ shall ensure that the client's information security risk assessment and risk treatment properly reflect its activities and extends to the boundaries of its activities as defined in the scope of certification. Certification bodies shall confirm that this is reflected in the client's scope of

their ISMS and Statement of Applicability. The certification body shall verify that there is at least one Statement of Applicability per scope of certification.

The MD prepares an Internal Cost Quotation Worksheet and an Estimated Cost Quotation (external document), converted to a .pdf file for the client's consideration (approval/decline). The Estimated Cost Quotation will outline the application fee, audit time, and all associated costs for a Stage 1 & Stage 2 initial audit and be communicated to the client.

Note: Direct auditor expenses are not included in the Estimated Cost Quotation but can be drafted/estimated upon client request.

If CIRQ approves the Application Form, and the client accepts the cost estimate, an Authorization to Proceed is sent electronically to client and filed in Client Folder on CIRQ Intranet. Once signed and received back from client, the development of the Audit Program begins the process.

CIRQ's Managing Director (MD) has primary responsibility for this process. *IEC/ISO 27006 Annex B* is referenced to determine audit complexity and audit time. CIRQ's Technical Advisor will also assist in preparing a Justification for Audit Days matrix which will evaluate the complexity of the client ISMS to determine the amount of time needed for all audit types in the 3yr cycle.

ISO/IEC 27001:2022 Transition information – Application process	**Current clients**: An updated application containing information specific to the 2022 version of the standard will be initiated and completed and added to Client Record during the planning period of the client's annual audit programme. An updated audit time matrix will be added to the client record, to document the additional time needed to perform an effective transition audit. The CIRQ Audit Report template is updated to include all ISO/IEC 27001:2022 requirements and will only be used when a client has a scheduled transition audit as documented in their individual audit programme. **New Clients**: A new application to be completed, reviewed and added to Client Record.

Remote Audits:
CIRQ may allow for Stage 1 document review audits to be executed using information and communication technology (ICT) which can include web-conferencing software like Zoom, Teams, GTM, Webex, etc. CIRQ will also consider allowances for those clients whose organizational site performs work or provides a service using an on-line environment allowing people irrespective of physical location to execute processes. When remote audits are proposed for the audit activities, the CIRQ application review shall include a check that the client and CIRQ Lead Auditor have the necessary hardware and software to support the use of the ICT proposed.

Per CIRQ's own management system requirements, the Managing Director will assign each applicant a unique number, starting with 1000 and that number will be followed by the date the Application was returned with client signatures, and given in 6-digit format (Mo/Day/Yr.). Number will be added to the "Client Account Number" log on the CIRQ Intranet. This number shall be retained throughout the 3-year cycle and beyond and used to track the client within the CIRQ ISMS.

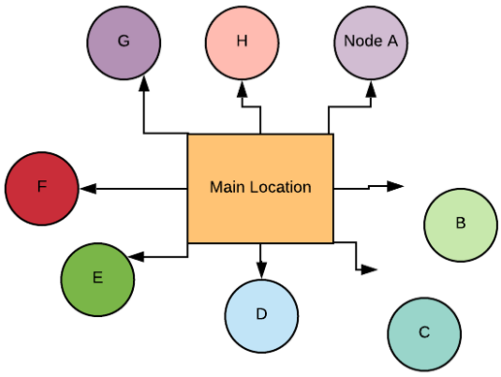
Once all listed documents from this IS1 Section have been submitted by the client, files are uploaded to the CIRQ intranet under Filing Cabinet>>Client Audit Files - Master.

Multi-Site Sampling: The CIRQ multi-site sampling rationale is subjective, based on documented facts for each client providing information on their auditee application.

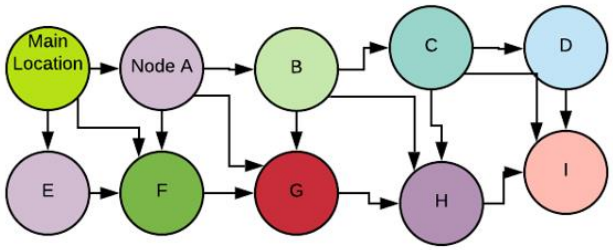
Multi-site sampling as described in ISO/IEC 17021-1:2015 has to be in various locations, that is defined as one organization operating either as a distributed operations in multiple locations as a business or with one data center with multiple locations as hubs in a hub-and-spokes model or operated as a distributed hubs only or having a hub being in a cloud-based hub with hubs being in multiple locations running operations in hubs etc.

This are depicted graphically to explain CIRQ managing multiple sites.

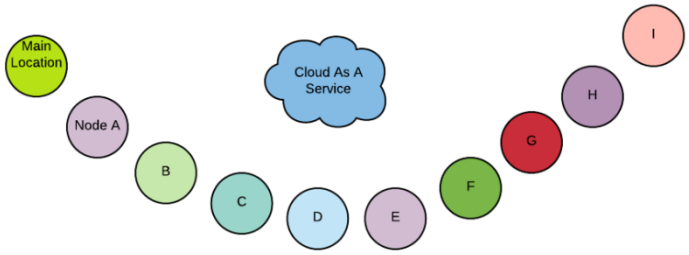
Example 1:



Example 2:



Example 3:



1. CIRQ reviews the application and scope for all sites in the application, and review which sites are operating under the same ISMS or ISMS/PIMS, confirming whether the auditee administers centrally managed internal audits as well as management review under one ISMS.
2. CIRQ reviews whether the auditee has included stated sites in the auditee's internal ISMS audit program.
3. CIRQ reviews stated scope in the application is accurately stated in the application.
4. CIRQ reviews the initial application that identifies and contrasts to the greatest extent possible, identifying the difference between sites and determining:
    a. # of internal audits conducted at main offices and # of internal audits conducted at distributed sites
    b. The compilation of results from management reviews from main site and distributed site
    c. Classification and variation of sites based on operation, functionality and technology used as well as number of employees
    d. Identification of business functions and purposes for various sample size
    e. Complexity of the site based on operations and technology installations
    f. Complexity in cultural differences and working and service delivery styles

g. Types of activities carried out to deliver quality, security, availability and service delivery
h. Variation of design, operation and implementation of controls
i. Potential upstream and downstream interaction with critical information
j. Consideration of privacy issues
k. Consideration of any legal implications
l. Consideration of geo-political and geo-cultural implications
m. Consideration of overall perceived risk for the site
n. Documented security breaches and incidents at the specific sites

5. The CIRQ sample is designed from all sites within the scope of the auditee's stated ISMS scope; this sample is a judgmental choice reflected by the subject matter expert reflecting the factors stated above as well as some will be selected a random element.
    a. The random element selected by CIRQ remains non-negotiable.
6. When CIRQ has included the site in the review, the ISMS significant risks are considered to be audited by CIRQ prior to certification.
7. CIRQ has a provision for addressing any nonconformity being observed, either at the head office or at a single site wherein, the corrective action procedure applies to main site, or the distributed site are covered by the certificate.
8. CIRQ audit addresses the auditee's main office activities ensuring that a single ISMS or ISMS/PIMS applies to all sites and delivers central management at the operational level.
9. CIRQ documents which site is audited during which audit cycle. At its own discretion, CIRQ may include alternate distributed site(s) during a surveillance audit depending on the risks during recertification audit.

Required Records:

- FC 1001 4.0 CIRQ MS Application
- FC 1006 1.7 CIRQ Justification of Audit Time
- FC 1005 1.0 CIRQ Multi-Site Application Review
- FC 1007 1.0 CIRQ Justification for ISMS/PIMS Remote audit
- TC 4001 2.4 CIRQ Standard Certification Agreement
- TC1003 2.1 Internal Cost Quotation Worksheet ISO/IEC 27001:2022/ISO 27701
- TC1002 Estimated Cost Quotation
- FC1003 Authorization to Proceed Form
- CLC 7002 1.2 ISMS Audit Program Checklist – Annual per audit type
- FC 2005 1.0 ISO/IEC 27001:2022 Audit Program Log MASTER
- CIRQ Client Account Numbers (xlswkbk) on Intranet

References:

- IS1-IS10 Auditing, Certification and Reporting Procedures – ISO/IEC 27001:2013 / ISO/IEC 27001:2022
- IEC/ISO 17021-1:2015
- IEC/ISO 27006:2015

Core Process IS2 Initial Stage 1 Audit Planning

ISO 17021 Clauses 7; 9.1.3, 9.2., 9.2.2-9.2.3
ISO 27006, Clauses 5.2.1, IS 7.1.1-7.1.2; Annex B, C

Development of the Audit Program begins in IS 1 and matures as the audit plan evolves. CIRQ requires that a client makes all necessary arrangements for access to internal audit reports and reports of independent reviews of information security.

The objectives of Stage 1 are achieved through obtaining and verifying various sources including interviews, observation of processes and activities, review of documentation and records by:

a) review the client's ISMS or ISMS/PIMS documented information
b) review the client's status and understanding regarding requirements of ISO/IEC 27001:2022 or and ISO/IEC 27001:2022 + ISO/IEC 27701:2019 in particular with respect to the identification of key performance or significant aspects, processes, objectives and operation of the ISMS or ISMS/PIMS
c) obtaining necessary information regarding the scope of the ISMS or ISMS/PIMS, including:
— the client's site(s)
— processes and equipment used
— levels of controls established (particularly in case of multisite clients)
— applicable statutory and regulatory requirements

Another key objective of the Stage 1 audit is to evaluate the client's site-specific conditions and to undertake discussions with the client's personnel to determine the preparedness for Stage 2 and review the allocation of resources for Stage 2. Once the client and CIRQ agree to the details of a Stage 2 with the client, work will be undertaken to focus for planning a Stage 2 audit by gaining a sufficient understanding of the client's ISMS or ISMS/PIMS and site operations in the context of the ISMS or PIMS standard or another normative document. The CIRQ Lead Auditor will evaluate if the internal audits and management reviews are being planned and performed, and that the level of implementation of the ISMS substantiates that the client is ready for stage 2.

The selection and appointment of the audit team is determined for the initial Stage 1 Audit, after a full competency review and evaluation has been performed (as detailed in section VIII. Organization Responsibilities and Authority). The selection and appointment process also considers the audit objectives, scope, criteria and estimated audit time; whether the audit is a combined, joint or integrated; the overall competence of the audit team needed to achieve the objectives of the audit certification requirements (including any applicable statutory, regulatory or contractual requirements); and language and culture considerations made known by the client. All CIRQ audits and certification body/auditor/client documentation take place in the English language.

The client is provided a copy of the lead auditor's resume/CV and/or list of qualifications (as appropriate) to state any objections to the assigned auditor. This is undertaken through evaluation of auditor knowledge, competence, removal of conflicts of interest and statement of confidentiality & non-disclosure. CIRQ will typically assign both the Stage 1 and Stage 2 audits to the same lead auditor, unless there is an unforeseen conflict (e.g., severe illness, weather/travel restrictions, etc.)

During this stage, the Lead Auditor is also sent their Estimated Auditor Fee Form (FC4002) and a Confidentiality and Non-Disclosure Declaration. The Lead Auditor (and the assigned team, when applicable) must sign both and return them to the Managing Director within 72 hours of receipt. The confirmed estimate is filed in the Client Audit Folder and the auditor will submit this form for payment. The signed Confidentiality and Non-Disclosure Declaration is filed in the assigned ISO/IEC 27001:2013 / ISO/IEC 27001:2022 Client planning folder.

The availability of the auditor is checked, and the auditor is tentatively scheduled. Audit dates are suggested and confirmed with client and auditor, and Audit Program Checklist is updated.

Note 1: Stage 1 audits may be performed as remote audits, as requested by the client and approved by audit team and CIRQ, dependent upon completeness of audit documentation requirements.

- If virtual sites are included within the scope, the certification/accreditation documentation shall note that virtual sites are included, and the activities performed at the virtual sites shall be identified.

Note 2: In cases where the client operates shifts, the activities that take place during shift working hours shall be considered when developing the audit program and audit plans.

The Lead Auditor is given the audit details (approved application, locations, dates, etc.) and asked to prepare the Stage 1 Audit Plan for the client; this document serves as the agenda for document review. The Audit Plan is reviewed by the Managing Director and submitted as Draft to the client for approval.

Once agreed by the client, the Audit Plan is marked Final, converted to a .pdf and sent to the client.

Determining audit time: In determining the audit time, CIRQ will consider, justify and record, among other things, the following aspects:

a) the requirements of the relevant ISMS and PIMS standard, as applicable;
b) complexity of the client and its ISMS, and PIMS, when applicable;
c) technological and regulatory context;
d) any outsourcing of any activities included in the scope of the ISMS or PIMS;
e) the results of any prior audits;
f) the number of people in certification in-scope areas
g) size and number of sites, their geographical locations and multi-site considerations;
h) the risks associated with the products, processes or activities of the organization;
i) whether audits are combined, joint or integrated.

Further, audit time estimation and justification will be determined using ISO/IEC 27006:2013 Annexes B Audit Time (normative) & C Methods for audit time calculations (Informative). Observers, technical experts, and other client-approved attendees who may present for the audit will be approved by CIRQ and client during planning*, and not count in the above established duration of the ISMS audit.

ISO/IEC 27001:2022 Transition information – Determining audit time using FC 1006 Audit time matrix	**Current clients:** 1) Minimum of 0.5 auditor day for the transition audit when it is carried out in conjunction with a recertification audit. 2) Minimum of 1.0 auditor day for the transition audit when it is carried out in conjunction with a surveillance audit or as a separate audit. **New Clients:** Audit time is determined at the time of application, as new clients will audit against ISO/IEC 27001:2022 (w/o 2013 version transition).

Audit Program Checklist is updated.

CIRQ, in communication with and approval by the client, will facilitate the inclusion of Observers where applicable to all audit types – initial, surveillance, recertification. Types of observers can include those invited by the client, and those requested by CIRQ with approval from the client, including accreditation assessors, CIRQ trainee auditor or Managing Director.

Note on CIRQ Accreditation Body Witness Auditors as observers:
During CIRQ's annual accreditation cycle, there may be requests to clients from CIRQ to approve witness auditors as observers to the CIRQ audit process. During this process, the ANSI National Accreditation Board (ANAB) may request CIRQ to facilitate a witness audit of a client audit. Like the CIRQ auditor, the ANAB Witness Auditor is observing CIRQ's conformance to the framework standard for certification bodies, ISO/IEC 17021-1:2015. If the ANAB witness auditor, upon its evaluation report gives CIRQ a major or minor non-conformance that occurred during the client audit, there may be the necessity to perform a special audit with CIRQ managing director, auditor and client representatives, as appropriate, to review the non-conformances CIRQ received and record the additional evidence. The Stage 2 Audit Plan and final Stage 2 Audit Report will be updated and revised to document this occurrence.

Note: If the CIRQ Auditor experiences excessive interruption/sidebars with Client Observers/Consultants during either Onsite or Remote Audits, the decision to pause the audit remains at the Lead Auditor's discretion, and the client runs the risk of increasing audit time and audit fees.

Required Records:

- FC 1001 4.0 CIRQ MS Application
- FC 1006 1.7 CIRQ Justification of Audit Time
- FC 1005 1.0 CIRQ Multi-Site Application Review
- FC 6000 2.3 CIRQ ISMS/PIMS Audit Plan
- FC 1007 1.0 CIRQ Justification for ISMS/PIMS Remote audit
- TC 4001 2.4 CIRQ Standard Certification Agreement
- TC1003 2.1 Internal Cost Quotation Worksheet ISO/IEC 27001:2013 / ISO/IEC 27001:2022/ISO 27701
- TC1002 Estimated Cost Quotation
- CLC 7002 1.2 ISMS Audit Program Checklist – Annual per audit type
- FC 2005 1.0 ISO/IEC 27001:2022 Audit Program Log MASTER

References:

- IS1 - IS10 Auditing, Certification and Reporting Procedures – ISO/IEC 27001:2013 / ISO/IEC 27001:2022
- IEC/ISO 17021-1:2015
- IEC/ISO 27006:2015

Core Process IS3 Conducting Stage 1 Initial Audits

ISO/IEC 17021:2015:1, Clauses 9.3.1.2., 9.4.2, 9.4.9, 9.4.10

Upon all confirmed planning for the initial Stage 1 Audit, the Lead Auditor conducts the Stage 1 Audit. The Lead Auditor shall gain prior approval for either a remote or onsite audit by the Managing Director and as documented in the Audit Plan.

The Stage 1 audit will include an Opening and Closing Meeting at each location. The purpose of the opening meeting, usually conducted by the audit team leader, is to provide a short explanation of how the audit activities will be undertaken. The process includes an introduction of the participants, including an outline of their roles, as well as formal communication throughout the audit and the client's ability to ask questions. Previous audit findings will be reviewed, as appropriate. The Lead Auditor will also share the methods by which information can be obtained, via interviews, observation of processes and reviewing documentation. The auditor will provide information about the conditions under which the audit may be prematurely terminated.

Results are compiled into a Stage 1 Audit Report by the auditor who then sends it to the Managing Director. It is then reviewed by the CIRQ Technical Advisor for Certification Review. Upon completion

of that review, the Managing Director sends the Stage 1 Audit Report to the client & files it in the Client Audit planning folder.

The CIRQ lead auditor will end the Stage 1 audit with a formal closing meeting, where attendance shall be recorded, shall be held with the client's management and, where appropriate, those responsible for the functions or processes audited. The purpose of the closing meeting is to present the audit conclusions, including the recommendation regarding certification. Any nonconformities shall be presented in such a manner that they are understood, and the timeframe for responding shall be agreed.

The lead auditor will also:

a) advise the client that the audit evidence obtained was based on a sample of the information, thereby introducing an element of uncertainty
b) review the method and timeframe of reporting, including any grading of audit findings
c) review CIRQ's process for handling nonconformities including any consequences relating to the status of the client's certification
d) the timeframe for the client to present a plan for correction and corrective action for any nonconformities identified during the audit
e) CIRQ's post audit activities
f) information about CIRQ's complaint and appeal handling processes.

All Areas of Concern or Non-Conformances need to be resolved by the client before the client is approved to move to a Stage 2 audit.

Note: Clients are advised to take approx. 3-4 weeks from the date of the Stage 1 Audit to have their Stage 2 Audit scheduled. This allowance provides the client with the ability to clear any findings reported by the Lead Auditor. However, this is only a recommendation. In determining the interval between stage 1 and stage 2, consideration shall be given to the needs of the client to resolve areas of concern identified during Stage 1.

Communications during the Audit.
Where the available audit evidence indicates that the audit objectives are unattainable or suggests the presence of an immediate and significant risk (e.g., safety), the audit team leader shall report this to the client and, if possible, to CIRQ to determine appropriate action. Such action may include reconfirmation or modification of the audit plan, changes to the audit objectives or audit scope, or termination of the audit. The audit team leader shall report the outcome of the action taken to the certification body.

The audit team leader shall review with the client any need for changes to the audit scope which becomes apparent as auditing activities progress and report this to CIRQ. The CIRQ audit team will analyze all information and audit evidence gathered during stage 1 to review the audit findings and agree on the audit conclusions.

No Findings: If there are no findings, clients may choose to have their Stage 2 Audit scheduled sooner at a time that is convenient to both the client and the auditor. These cases are all determined on a case by case basis, in close consultation with the client, the auditor and CIRQ's Managing Director.

Findings: CIRQ and its auditor personnel may use the term "findings" as a general grouping of evidence from a client audit that includes Non-Conformances and Areas of Concern. CIRQ will review the corrections, identified causes and corrective actions submitted by the client to determine if these are acceptable. CIRQ will verify the effectiveness of any correction and corrective actions taken when resolving a Non-Conformance finding from an audit. The evidence obtained to support the resolution of nonconformities shall be recorded. The client shall be informed of the result of the review by the

Technical Advisor for Certification Decisions and CIRQ's Managing Director. CIRQ will inform the client if an additional full audit, an additional limited audit, or documented evidence (to be confirmed during future audits) will be needed to verify effective correction and corrective actions.

NOTE Verification of effectiveness of correction and corrective action can be carried out based on a review of documented information provided by the client, or where necessary, through verification on-site. Usually, this activity is done by a member of the audit team.

Required Records:

- FC 6000 2.3 CIRQ ISMS/PIMS Audit Plan
- WBC 7000 2.0 ISO IEC 27001 Stage 1 Audit Report
- WBC 7005 1.2 CIRQ Closing Meeting Report
- CLC 7002 1.2 ISMS Audit Program Checklist – Annual per audit type
- FC 2005 1.0 ISO/IEC 27001:2013 / ISO/IEC 27001:2022 Audit Program Log MASTER

Core Process IS4 Conducting Stage 2 Audits

ISO/IEC 17021-1:2015, Clause 9.3.1.3, 9.4.1-, 9.5.3.2
ISO/IEC 27006:2015 IS 9.4

After all steps from IS3 are completed, the client is cleared for their Stage 2 Audit. In most cases, CIRQ will confirm and appoint the same Lead Auditor from the Stage 1 process. The purpose of stage 2 is to evaluate the implementation, including effectiveness, of the client's ISMS or ISMS/PIMS. Stage 2 shall take place at the office or other physical site(s) of the client.

By obtaining and verifying information from various sources including interviews, observation of processes and activities, review of documentation and records, it shall include the auditing of at least the following:

a) information and evidence about conformity to all requirements of ISO/IEC 27001:2022 or and ISO/IEC 27001:2022 + ISO/IEC 27701:2019, as applicable
b) performance monitoring, measuring, reporting and reviewing against key performance objectives and targets of ISO/IEC 27001:2022 or and ISO/IEC 27001:2022 + ISO/IEC 27701:2019, as applicable
c) the client's ISMS ability and its performance regarding meeting of applicable statutory, regulatory and contractual requirements
d) operational control of the client's processes
e) internal auditing and management review
f) management responsibility for the client's policies.

An Audit Plan is prepared by the auditor for Stage 2 and reviewed by the MD. The Stage 2 audit is conducted by the Audit Team onsite or remote using ICT, as previously agreed upon, and according to the Stage 2 Audit Plan. The Stage 2 Audit Plan is marked as a Draft and sent to the client, by the MD, for the client's review and approval. When approved by the client (email is acceptable) it is marked as Final, saved as a PDF.

The Lead Auditor will perform the entire audit per the pre-determined Audit Plan number of audit days and include a formal Opening and Closing Meeting for all locations in scope.

The Opening Meeting shall be held with the client's management and, where appropriate, those responsible for the functions or processes to be audited. The purpose of the opening meeting, usually conducted by the audit team leader, is to provide a short explanation of how the audit activities will

be undertaken. As in Stage 1, the client is able to request Observers at their audit, and CIRQ may do the same. Both Client and CIRQ will communicate the request and obtain approval.

Note: If the CIRQ Auditor experiences excessive interruption/sidebars with Client Observers/Consultants during either Onsite or Remote Audits, the decision to pause the audit remains at the Lead Auditor's discretion, and the client runs the risk of increasing audit time and audit fees.

The Stage 2 process includes an introduction of the participants, including an outline of their roles, as well as formal communication throughout the audit and the client's ability to ask questions. Previous audit findings will be reviewed, as appropriate. The Lead Auditor will also share the methods by which information can be obtained, via interviews, observation of processes and reviewing documentation. The auditor will provide information about the conditions under which the audit may be prematurely terminated.

Note: Remote audits for Stage 2 using ICT are allowed if the client can prove, and CIRQ can verify, that the organization is 100% virtual with a cloud based ISMS and the company allows for personnel to work remotely and/or from diverse domestic or international locations. These are considered carefully, on a case by case basis.

The Lead Auditor will conduct the audit using WBC 7001 1.6 CIRQ Audit Report ISO/IEC 27001:2022, which contains all requirements and controls of ISO/IEC 27001:2022 or ISO/IEC 27001:2022 + ISO/IEC 27701:2019, as applicable. This is an internal document for the auditor to capture and document all of their findings. Audit findings summarizing conformity and detailing nonconformity shall be identified, classified and recorded to enable an informed certification decision to be made or the certification to be maintained. Findings include Opportunities for Improvement, which are not documented as non-Conformities, which shall be discussed with the client to ensure that the evidence is accurate and that the nonconformities are understood.

Note: The auditor shall refrain from suggesting the cause of nonconformities or their solution, as this can be a threat to impartiality as auditors cannot serve as consultants at any time during the audit program.

The CIRQ lead auditor will end the Stage 2 audit with a formal closing meeting, where attendance shall be recorded, shall be held with the client's management and, where appropriate, those responsible for the functions or processes audited. The purpose of the closing meeting is to present the audit conclusions, including the recommendation regarding certification presented in a brief written report. Any nonconformities shall be presented in such a manner that they are understood, and the timeframe for responding shall be agreed.

The lead auditor will also:

a) advise the client that the audit evidence obtained was based on a sample of the information, thereby introducing an element of uncertainty
b) review the method and timeframe of reporting, including any grading of audit findings
c) review CIRQ's process for handling nonconformities including any consequences relating to the status of the client's certification
d) the timeframe for the client to present a plan for correction and corrective action for any nonconformities identified during the audit
e) CIRQ's post audit activities
f) information about CIRQ's complaint and appeal handling processes.

The Lead Auditor will confirm that any additional client questions are asked and answered sufficiently. Any diverging opinions regarding the audit findings or conclusions between the audit team and the client shall be discussed and resolved where possible. Any diverging opinions that are not resolved

shall be recorded and referred to CIRQ.

Where the available audit evidence indicates that the audit objectives are unattainable or suggests the presence of an immediate and significant risk (e.g., safety), the audit team leader shall report this to the client and, if possible, to CIRQ to determine appropriate action. Such action may include reconfirmation or modification of the audit plan, changes to the audit objectives or audit scope, or termination of the audit. The audit team leader shall report the outcome of the action taken to the certification body.

The audit team leader shall review with the client any need for changes to the audit scope which becomes apparent as on-site auditing activities progress and report this to CIRQ.

The Stage 2 Audit Report Draft are uploaded by the Lead Auditor to the client folder on the CIRQ Intranet within 72 hours of the last scheduled day of the onsite audit.

The Stage 2 Audit Report will contain:

a) identification of the certification body
b) the name and address of the client and the client's representative
c) the type of audit (e.g., initial, surveillance or recertification audit or special audits)
d) the audit criteria & audit objectives, and confirmation that the audit objectives have been fulfilled.
e) the audit scope, particularly identification of the organizational or functional units or processes audited and the time of the audit, and a conclusion on the appropriateness of the certification scope
f) any deviation from the audit plan and their reasons and any significant issues impacting on the audit program
g) identification of the audit team leader, audit team members and any accompanying persons
h) the dates and places where the audit activities (on site or offsite, permanent or temporary sites) were conducted
i) audit findings reference to evidence and conclusions, consistent with the requirements of ISO/IEC 27001:2022 or ISO/IEC 27001:2022 + ISO/IEC 27701:2019, as applicable
k) significant changes, if any, that affect the ISMS of the client since the last audit took place
l) any unresolved issues, if identified
m) where applicable, whether the audit is combined, joint or integrated
n) a disclaimer statement indicating that auditing is based on a sampling process of the available information
o) recommendation from the audit team
p) the audited client is effectively controlling the use of the certification documents and marks, if applicable
q) verification of effectiveness of taken corrective actions regarding previously identified nonconformities, if applicable.
r) a statement on the conformity and the effectiveness of the ISMS or ISMS/PIMS together with a summary of the evidence relating to:
— the capability of the ISMS/PIMS to meet applicable requirements and expected outcomes
— the internal audit and management review process

It is the Lead Auditor's responsibility to alert the Managing Director that audit documents are ready for review. Once the audit documents are ready for review, the Managing Director alerts the Technical Advisor for Certification Review that an initial certification is ready for a technical review. The technical advisor has 72 hours to alert the Managing Director of their findings. The CIRQ audit team will analyze all information and audit evidence gathered during Stage 2 (including Stage 1) to review the audit findings and agree on the audit conclusions.

If there are no additional findings during the review, the Stage 2 Audit Report moves to the certification decision step (IS5).

However, if the Lead Auditor documents any Areas of Concern or Non-Conformances, the client will have 30 days* to resolve and submit a Root Cause Analysis (RCA) form, maintained as a template within the Stage 2 Audit Report. This template can be copied within the same report for additional Areas of Concern or Non-Conformance findings.

*Note: If CIRQ is not able to verify the implementation of corrections and corrective actions of any major nonconformity within 6 months after the last day of stage 2, the certification body shall conduct another stage 2 prior to recommending certification.

Once the RCA client report is ready for review, the Managing Director alerts the Technical Advisor for Certification Review that an initial certification is ready for a final technical review. The technical advisor will also review any Areas of Concern or Non-Conformances, and either reject or approve the attached Root Cause Analysis. The technical advisor has 72 hours to alert the Managing Director of their findings.

All versions of the draft audit report, containing certification decision review comments from Technical Advisor and Managing Director, with responses from the Lead Auditor, will be retained as individual records in the Client Folder on the CIRQ Intranet. Files will be named "_Draft (1, 2, etc., as appropriate)". Only the approved audit report will be designated as "Final" in the file name in the Client Folder under Audit Report.

Note: This is the procedure for certification decisions pertaining to all client Stage 2 and Recertification Audit Reports and is recorded on the annual Audit Program Checklist and in the CIRQ ISMS Audit Program log.

The Audit Program Checklist is updated and filed in the Client Folder on the CIRQ Intranet.

Required Records:

- FC 6000 2.3 CIRQ ISMS/PIMS Audit Plan
- WBC 7003 1.0 CIRQ Audit Report ISO/IEC 27001:2022+ISO 27701
- WBC 7005 1.2 CIRQ Closing Meeting Report
- CLC 7002 1.2 ISMS Audit Program Checklist – Annual per audit type
- FC 2005 1.0 ISO/IEC 27001:2022 Audit Program Log
- FC 8001 1.5 CIRQ Client Feedback Form

Core Process IS5 Granting Initial Certification

ISO 17021 Clause 7.2.8, 8.1, 8.2, 9.5.2, 9.5.3
ISO 27006, Clause 9.5

Upon completion of all steps in IS4, the final Stage 2 Audit Report is sent as a .pdf file to the client, along with the Client Feedback Form. Prior to making a formal decision to grant certification, the recommendation for certification by the Technical Advisor for Certification Decisions and Managing Director will be undertaken. The audit report will serve as an executive summary for the client, concluding overall compliance within the ISMS to ISO/IEC 27001:2022 or ISO/IEC 27001:2022 + ISO/IEC 27701:2019, as applicable. Information provided during the Application Review will be confirmed by the Managing Director, as it will inform accuracy within the Audit report and certification document.

The information provided by the Lead Auditor will be deemed sufficient with respect to the confirmation that the audit objectives have been achieved, certification requirements have been met and the scope for certification, as well as major nonconformities and nonconformities including review and acceptance of the client's plan for correction and corrective action. The final report feedback form is filed within the Client Folder on the CIRQ Intranet; client feedback is shared with the Lead Auditor, as appropriate.

A draft 3yr Audit Plan is sent to the client for approval. The 3yr Plan plan gives an overview to the amount of days the client can expect for their surveillance and recertification audit days and is kept in the Client Folder.

The ISO/IEC 27001:2022 Audit Program Log is updated; Audit Program Checklist is closed out and filed in the Client Folder on the CIRQ Intranet.

Maintaining Certification:
CIRQ maintains its clients' certification based on demonstration that the client continues to satisfy the requirements of the management system standard. Tracked in the Audit Program Log, this is based on a positive conclusion by the audit team leader at the time of audit without further independent review and decision, provided that:

a) for any major nonconformity or other situation that may lead to suspension or withdrawal of certification, CIRQ requires the audit team leader to report to the certification body the need to initiate a review by a CIRQ Technical Advisor, different from those who carried out the audit, to determine whether certification can be maintained
b) CIRQ Technical Advisor monitor its surveillance activities, including monitoring the reporting by its auditors, to confirm that the certification activity is operating effectively.

ISO/IEC 27001:2022 Transition information – Certification decision	**Current clients:** CIRQ shall make the transition decision based on the result of transition audit and technical review. An updated certificate will be sent to the client if its ISMS meets the requirements of ISO/IEC 27001:2022. Note: *When the certification document is updated because the client successfully completed only the transition audit, the expiration of its current certification cycle will not be changed.* **New Clients:** Certificate issued to new clients will audit to and reflect requirements of ISO/IEC 27001:2022 (w/o 2013 version transition).

Required Records:

- FC 6000 2.3 CIRQ ISMS/PIMS Audit Plan
- WBC 7003 1.0 CIRQ Audit Report ISO/IEC 27001:2022+ISO 27701
- CLC 7002 1.2 ISMS Audit Program Checklist – Annual per audit type
- FC 2005 1.0 ISO/IEC 27001:2022 Audit Program Log
- FC 8001 1.5 CIRQ Client Feedback Form

Core Process IS6 Initial Certification Decision
When certification is granted (or renewed at the Re-Certification audit), the client's name, address, and Statement of Applicability are retrieved and confirmed from the client application and Stage 2 Audit Report.

Via email from CIRQ's Managing Director, the client will be sent the Certificate of Compliance as a .pdf document, along with the following document(s) & file:

- S1 1.2 Terms of Use for CIRQ Certification Mark(s).
- The CIRQ ISO/IEC 27001 Certification Mark (.jpg)
- The CIRQ ISO 27701 Certification Mark (.jpg) as applicable

The newly certified company to the Certification Registry on the CIRQ website.

If certification is delayed or not granted (denied) a letter explaining why is sent to the client.
Audit Program Checklist is updated and closed out.

ISO/IEC 27001:2022 Transition information – Certification decision	**Current clients:** Not applicable; already certified to ISO 27001:2013. **New Clients:** All new clients who implement and audit to ISO/IEC 27001:2022 will receive a certificate (w/o 2013 version transition step).

Required Records:

- WBC 7003 1.0 CIRQ Audit Report ISO/IEC 27001:2022+ISO 27701
- S1 1.4 Terms of Use for CIRQ Certification Mark(s)
- The CIRQ ISO/IEC 27001 Certification Mark (.jpg)
- The CIRQ ISO 27701 Certification Mark (.jpg)
- Certificate, as applicable:
    - TC 7002 1.0 CIRQ Certificate of Compliance ISO/IEC 27001:2022 w/ANAB logo
    - TC 7005 1.0 CIRQ Certificate of Compliance ISO/IEC 27001:2022 & ISO/IEC 27701:2019 w/ANAB logo
- CLC 7002 1.0 ISMS Audit Program Checklist – Annual per audit type
- FC 2005 1.0 ISO/IEC 27001:2022 Audit Program Log

Core Process IS7 Surveillance Audits

ISO/IEC 17021-1:2015, Clause 9.6
ISO 27006 IS 9.6.2

CIRQ shall maintain certification based on demonstration that the client continues to satisfy the requirements of ISO/IEC 27001:2013 / ISO/IEC 27001:2022 or ISO/IEC 27001:2022 + ISO/IEC 27701:2019, as applicable. CIRQ shall conduct surveillance audits at least once a calendar year. The date of the first surveillance audit following initial certification shall not be more than 12 months from the certification decision date. The following process documents both Surveillance 1 and Surveillance 2 Audit planning.

Each surveillance for the relevant ISMS standard shall obtain and verify information from various sources including interviews, observation of processes and activities, review of documentation and records from the following:

a) internal audits and management review
b) a review of actions taken on nonconformities identified during the previous audit
c) complaints handling
d) effectiveness of the ISMS with regard to achieving the certified client's objectives and the intended results of the respective ISMS(s)
e) progress of planned activities aimed at continual improvement

f) continuing operational control
g) review of any changes
h) use of marks and/or any other reference to certification.

Approximately 3 months before the certification anniversary, CIRQ will contact client to undertake an exchange of information relevant to planning surveillance audits. As part of this process, CIRQ will pay special attention to any changes documented by the client in the Pre-Surveillance Audit Questionnaire ISO/IEC 27001:2022 or ISO/IEC 27001:2022+ISO 27701, as applicable, which is emailed to the client at this time. This document is filed in the Client Folder on the CIRQ Intranet and informs the creation of a Surveillance Audit Plan. CIRQ and Lead Auditor will determine if changes to audit program are required based on responses in questionnaire.

Note: Clients will undertake 2 surveillance audits within a 3-year certification cycle. This is documented within the approved CIRQ Management System Application.

ISO/IEC 27001:2022 Transition information – Transition audit	**Current clients:** In collaboration with CIRQ, the client may undertake its transition audit during either a Surveillance or Recertification audit and shall include but is not limited to the following: a gap analysis of ISO/IEC 27001:2022, as well as the need for changes to the client's ISMS; updated SoA; updated risk treatment plan; and the implementation and effectiveness of the new or changed controls chosen by the clients. Note: **New Clients:** If a client has implemented ISO/IEC 27001:2022 and this is established during the application review period and confirmed during a Stage 1 Audit, no transition audit is required.

The client is responsible for alerting CIRQ's Managing Director to any organizational changes that may impact its scope of certification (e.g., acquisition, staff reduction, etc.) that happen at any time – not just around annual audit planning.

Where the available audit evidence indicates that the audit objectives are unattainable or suggests the presence of an immediate and significant risk (e.g., safety), the audit team leader shall report this to the client and, if possible, to CIRQ to determine appropriate action. Such action may include reconfirmation or modification of the audit plan, changes to the audit objectives or audit scope, or termination of the audit. The audit team leader shall report the outcome of the action taken to the certification body.

The audit team leader shall review with the client any need for changes to the audit scope which becomes apparent as on-site auditing activities progress and report this to CIRQ.

The selection and appointment of the audit team is determined as in Section IS1. This is undertaken through evaluation of auditor knowledge, competence, removal of conflicts of interest and statement of confidentiality & non-disclosure. The Lead Auditor is also sent their Estimated Auditor Fee Form (FC4002) and a Confidentiality and Non-Disclosure Declaration. The Lead Auditor (and the assigned team, when applicable) must sign both and return them to the Managing Director within 72 hours of receipt. The confirmed fee estimate is filed in the Client Audit Folder and the auditor will submit this form for payment. The signed Confidentiality and Non-Disclosure Declaration is filed in the ISO/IEC 27001:2022 Client planning folder.

The availability of the auditor is checked, and the auditor is tentatively scheduled. Audit dates are suggested and confirmed with client and auditor, and Audit Program Checklist is updated.

The MD prepares an Internal Cost Quotation Worksheet and an Estimated Cost Quotation (external document), converted to a .pdf file for the client's consideration (approval/decline). The Estimated Cost Quotation will outline the costs for the Surveillance Audit and be communicated to the client.

Direct auditor expenses are not included in the Estimated Cost Quotation but can be drafted/estimated upon client request.

An Audit Plan is prepared by the auditor for 1st and 2nd annual Surveillance Audits and reviewed by the MD. Surveillance audits are conducted by the Audit Team onsite, with possible remote locations, as previously agreed upon, and according to the 1st/2nd Surveillance Audit Plan. It is marked as Draft and sent to the client, by the MD, for the client's review and approval. When approved by the client (email is acceptable) it is marked as Final, saved as a PDF.

ISO/IEC 27001:2022 Transition information – Audit Plan	**Current clients:** The CIRQ Audit Plan template is updated to include all ISO/IEC 27001:2022 requirements and will only be used when a client has a scheduled transition audit as documented in their individual audit programme. **New Clients:** The updated CIRQ Audit Plan template will be used.

The Lead Auditor will perform the entire audit per the pre-determined Audit Plan number of audit days and include a formal Opening and Closing Meeting.

The Opening Meeting shall be held with the client's management and, where appropriate, those responsible for the functions or processes to be audited. The purpose of the opening meeting, usually conducted by the audit team leader, is to provide a short explanation of how the audit activities will be undertaken. The process includes an introduction of the participants, including an outline of their roles, as well as formal communication throughout the audit and the client's ability to ask questions. Previous audit findings will be reviewed, as appropriate. The Lead Auditor will also share the methods by which information can be obtained, via interviews, observation of processes and reviewing documentation. The auditor will provide information about the conditions under which the audit may be prematurely terminated.

Note: A Remote audit strategy for surveillance using ICT is allowed if the client can prove, and CIRQ can verify, that the organization is 100% virtual with a cloud based ISMS and the company allows for personnel to work remotely and/or from diverse domestic or international locations. These are considered carefully, on a case by case basis.

The Lead Auditor will conduct the surveillance audit summarizing conformity and detailing nonconformity shall be identified, classified and recorded to enable an informed certification decision to be made or the certification to be maintained and documented into an Audit Report. Findings include Opportunities for Improvement, which are not documented as non-Conformities, which shall be discussed with the client to ensure that the evidence is accurate and that the nonconformities are understood.

Note: The auditor shall refrain from suggesting the cause of nonconformities or their solution, as this can be a threat to impartiality as auditors cannot serve as consultants at any time during the audit program.

The CIRQ lead auditor will end the 1st/2nd Surveillance audit with a formal closing meeting, where

attendance shall be recorded, shall be held with the client's management and, where appropriate, those responsible for the functions or processes audited. The purpose of the closing meeting is to present the audit conclusions, including the recommendation regarding certification presented in a brief written report. Any nonconformities shall be presented in such a manner that they are understood, and the timeframe for responding shall be agreed.

The lead auditor will also:

a) advise the client that the audit evidence obtained was based on a sample of the information, thereby introducing an element of uncertainty
b) review the method and timeframe of reporting, including any grading of audit findings
c) review CIRQ's process for handling nonconformities including any consequences relating to the status of the client's certification
d) the timeframe for the client to present a plan for correction and corrective action for any nonconformities identified during the audit
e) CIRQ's post audit activities
f) information about CIRQ's complaint and appeal handling processes.

The Lead Auditor will confirm that any additional client questions are asked and answered sufficiently. Any diverging opinions regarding the audit findings or conclusions between the audit team and the client shall be discussed and resolved where possible. Any diverging opinions that are not resolved shall be recorded and referred to CIRQ.

The 1st/2nd Surveillance Audit Report Draft are uploaded by the Lead Auditor to the client folder on the CIRQ Intranet within 72 hours of the last scheduled day of the onsite audit.

The surveillance audit reports will contain:

a) identification of the certification body
b) the name and address of the client and the client's representative
c) the type of audit (e.g., initial, surveillance or recertification audit or special audits)
d) the audit criteria & audit objectives, and confirmation that the audit objectives have been fulfilled.
e) the audit scope, particularly identification of the organizational or functional units or processes audited and the time of the audit, and a conclusion on the appropriateness of the certification scope
f) any deviation from the audit plan and their reasons and any significant issues impacting on the audit program
g) identification of the audit team leader, audit team members and any accompanying persons
h) the dates and places where the audit activities (on site or offsite, permanent or temporary sites) were conducted
i) audit findings reference to evidence and conclusions, consistent with the requirements of ISO/IEC 27001:2022 or ISO/IEC 27001:2022 + ISO/IEC 27701:2019, as applicable
k) significant changes, if any, that affect the ISMS of the client since the last audit took place
l) any unresolved issues, if identified
m) where applicable, whether the audit is combined, joint or integrated
n) a disclaimer statement indicating that auditing is based on a sampling process of the available information
o) recommendation from the audit team
p) the audited client is effectively controlling the use of the certification documents and marks, if applicable
q) verification of effectiveness of taken corrective actions regarding previously identified nonconformities, if applicable.
r) a statement on the conformity and the effectiveness of the ISMS together with a summary of the evidence relating to:

— the capability of the ISMS to meet applicable requirements and expected outcomes
— the internal audit and management review process

It is the Lead Auditor's responsibility to alert the Managing Director that audit documents are ready for review.

If there are no additional findings during the review, the 1st/2nd Surveillance Audit Report is marked as final, is distributed to the client representatives, and is stored within the client folder for the specific year on the CIRQ Intranet.

ISO/IEC 27001:2022 Transition information – Audit report	**Current clients:** The CIRQ Audit Report template is updated to include all ISO/IEC 27001:2022 requirements and will only be used when a client has a scheduled transition audit as documented in their individual audit programme, and the auditor has performed the transition audit. **New Clients:** The updated CIRQ Audit Report template will be used.

However, if the Lead Auditor documents any Areas of Concern or Non-Conformances, the client will have 30 days to resolve and submit a Root Cause Analysis (RCA) form, maintained as a template within the 1st/2nd Surveillance Audit Report. This template can be copied within the same report for additional Areas of Concern or Non-Conformance findings. The lead auditor will review the RCA to ensure that the analysis is sufficient, and the 1st/2nd Surveillance Audit Report is marked as final, is distributed to the client representatives and is stored within the client folder for the specific year on the CIRQ Intranet.

The Audit Program Checklist is updated and filed in the Client Folder on the CIRQ Intranet. The 1st/2nd Surveillance Audit Program Checklist is updated.

Special audits:
CIRQ shall, in response to an application for expanding the scope of a certification already granted, undertake a review of the application and determine any audit activities necessary to decide whether or not the extension may be granted. This may be conducted in conjunction with a surveillance audit.

Required Records:

- FC 8002 2.3 ISMS / PIMS Pre-Surveillance Audit Questionnaire
- FC 1001 4.0 CIRQ MS Application
- FC 6000 2.3 CIRQ ISMS/PIMS Audit Plan
- WBC 7003 1.0 CIRQ Audit Report ISO/IEC 27001:2022+ISO 27701
- WBC 7005 1.2 CIRQ Closing Meeting Report
- FC 4002 Estimated Auditor Fee Form
- FC 5001 Confidentiality and Non-Disclosure Declaration
- TC 1003 2.1 Internal Cost Quotation Worksheet ISO/IEC 27001:2022
- TC 1002 Estimated Cost Quotation
- CLC 7002 1.2 ISMS Audit Program Checklist – Annual per audit type
- FC 2005 1.0 ISO/IEC 27001:2022 Audit Program Log

Core Process IS8 Recertification Audit
ISO/IEC 17021-1:2015, 9.6.3, 9.6.4
ISO 27006:2015 IS 9.6.3

On or about 3 months prior to a client's Recertification Audit, CIRQ's Managing Director shall contact the Client to commence planning. CIRQ and the client shall conduct the audit before the certification expiration date. CIRQ shall make decisions on renewing certification based on the results of the recertification audit, as well as the results of surveillance audits, the review of the ISMS over the period of certification and complaints received from users of certification.

The above-listed Core Processes IS1 – IS7 shall be followed throughout the Recertification Audit planning. Individual Audit Program Checklists will be drafted and completed for each audit format throughout the 3-year audit cycle.

During the recertification audit ISO/IEC 27001:2022 or ISO/IEC 27001:2022 + ISO/IEC 27701:2019, as applicable, the auditor shall obtain and verify information from various sources including interviews, observation of processes and activities, review of documentation and records from the following:

a) internal audits and management review
b) a review of actions taken on nonconformities identified during the previous audit
c) complaints handling
d) effectiveness of the ISMS or ISMS/PIMS with regard to achieving the certified client's objectives and the intended results of the respective ISMS(s)
e) progress of planned activities aimed at continual improvement
f) continuing operational control
g) review of any changes
h) use of marks and/or any other reference to certification

Note: Recertification audit activities may need to have a Stage 1 Audit in situations where there have been significant changes to the ISMS or ISMS/PIMS, the organization, or the context in which the ISMS is operating (e.g., changes to legislation).

CIRQ shall monitor the Audit Program, which shall be confirmed or adjusted with the appropriate audit follow-up and surveillance activities including the frequency and duration of audits.

When recertification activities are successfully completed prior to the expiry date of the existing certification, the expiry date of the new certification can be based on the expiry date of the existing certification. The issue date on a new certificate shall be on or after the recertification decision.

Expiry rule: When the Re-Certification Audit cannot be conducted in the timeframe mentioned above, CIRQ will grant an extension of no more than 15 days.

In a situation where CIRQ has not completed the recertification audit or is unable to verify the implementation of corrections and corrective actions for any major nonconformity prior to the expiry date of the certification, then recertification shall not be recommended, and the validity of the certification shall not be extended. The client shall be informed, and the consequences shall be explained.

Following expiration of certification, CIRQ can restore certification within 6 months provided that the outstanding recertification activities are completed, otherwise at least a stage 2 shall be conducted. The effective date on the certificate shall be on or after the recertification decision and the expiry date shall be based on prior certification cycle.

Short-notice audits:

It may be necessary for CIRQ to conduct audits of certified clients at short notice or unannounced to investigate complaints, or in response to changes, or as follow up on suspended clients. In such cases,

CIRQ will describe and make known in advance to the certified clients, the conditions under which such audits will be conducted, and that CIRQ shall exercise additional care in the assignment of the audit team because of the lack of opportunity for the client to object to audit team members.

Required Records:

- FC 8002 2.3 ISMS / PIMS Pre-Surveillance Audit Questionnaire
- FC 1001 4.0 CIRQ MS Application
- FC 6000 2.3 CIRQ ISMS/PIMS Audit Plan
- WBC 7003 1.0 CIRQ Audit Report ISO/IEC 27001:2022+ISO 27701
- WBC 7005 1.2 CIRQ Closing Meeting Report
- FC 4002 Estimated Auditor Fee Form
- FC 5001 Confidentiality and Non-Disclosure Declaration
- TC 1003 2.1 Internal Cost Quotation Worksheet ISO/IEC 27001:2022
- TC 1002 Estimated Cost Quotation
- CLC 7002 1.2 ISMS Audit Program Checklist – Annual per audit type
- FC 2005 1.0 ISO/IEC 27001:2022 Audit Program Log

Core Process IS9 Certification Body Transfers

ISO 17021-1:2015, Clause 9.1.3.4, 9.5.2, 9.5.3.3
IAF MD 2:2017

In the case where an ISO/IEC 27001:2022 certified organization wishes to transfer its existing certification to CIRQ, all prospective Transfer Clients must go through a Pre-Transfer Review. The transferring client must provide the reasons for seeking a transfer, as well as the following:

- The previous certificate from the initial certification, previous audit report(s) (initial, surveillance, recertification)
- Documentation on nonconformities and corrective actions
- Complaints received and actions taken
- Any relevant consideration to legal compliance relevant to the certification scope
- Number of days of Initial Audit.

CIRQ's Managing Director will confirm CIRQ has obtained and retains in Client Folder all sufficient evidence to approve transfer. Once this documentation has been secured, the Managing Director, along with the technical advisor for certification decisions, initiates an Audit Program and the Core Procedures IS1 – IS8 as appropriate.

It is the transferring client's responsibility to authorize that the issuing certification body provides the information sought by CIRQ. The issuing certification body shall not suspend or withdraw the organization's certification following the notification that the organization is transferring to CIRQ if the client continues to satisfy the requirements of certification.

Required Documents:

- FC 1001 4.0 CIRQ MS Application
- CLC 7002 1.2 ISMS Audit Program Checklist – Annual per audit type
- FC 2005 1.0 ISO/IEC 27001:2022 Audit Program Log
- Previous Certificate
- Previous Audit report(s) Master Client Audit Files/Client 27001 Folder

B. Support Process Definitions – for Core and Core IS Processes

S1. Terms of Use for CIRQ Certification

ISO/IEC 17021-1:2015, Clause 8.3
ISO/IEC 17065:2012, Clause 4.1.3, 7.10

The Insights Association's Certification Institute for Research Quality, LLC. ("CIRQ") has established these Terms of Use to allow for the use of the CIRQ Certification Mark(s) in a professional and legal manner by CIRQ-certified companies in their written and electronic literature and advertising. These Terms define the limitations of use by ISO 20252:2019, ISO/IEC 27001:2022 and/or ISO/IEC 27701:2019 (the "Standard(s)") certified companies of the CIRQ Certification Mark(s); and will be administered by the CIRQ Managing Director and CIRQ Board Chair. These terms cover the use of the CIRQ Certification Mark(s)(s) only. The CIRQ logo is a separate and distinct graphic and is restricted to CIRQ use only.

1. Only companies who have achieved a successful audit to the Standard and have received a Certificate of Compliance from CIRQ are permitted to use the CIRQ Certification Mark(s). The client conforms to CIRQ requirements when making reference to its certification status in communication media such as the internet, brochures or advertising, or other documents.

2. CIRQ does not permit its marks to be applied by certified clients to laboratory test, calibration or inspection reports or certificates.

3. The CIRQ Certification Mark(s) will be delivered to the certified company electronically in both a gif format for website use and a jpeg format for print use. Other formats will be made available as needed. Guidelines for size and color usage will be delivered with the Certification Mark(s).

4. Certification approval and use of the Certification Mark(s) is limited to the scope of audit determined by CIRQ and detailed on the Certificate of Compliance in the Statement of Applicability. Companies who have achieved certification will use the Certification Mark(s) only in such a way so as not to create confusion between matters referred to in the scope of certification and other matters and does not make or permit any misleading statement regarding its certification.

5. Divisions, parents, subsidiaries, sister companies and other affiliated companies are **not** permitted to use the CIRQ Certification Mark(s) unless they have individually received certification by CIRQ to the Standard(s).

6. Companies that have achieved certification but are **not** Insights Association members may only use the CIRQ Certification Mark(s) and are not entitled to use the separate and distinct Insights Association logo in their materials.

7. The use of CIRQ's name and/or the Certification Mark(s) and/or the use of the Insights Association name and/or logo are not an endorsement of the organization that use any such name, Certification Mark(s), or logo. The CIRQ name and Certification Mark(s) and the

Insights Association name and logo shall in no way imply that the product, process or service is certified by this means.

The CIRQ Certification Mark(s) applies only to certification of either/both the company's research project management system (ISO 20252:2019), information security management system (ISO/IEC 27001:2022) or information security management system (ISO/IEC 27001:2022) and privacy information management system (ISO/IEC 27701:2019) according to the Statement of Applicability. The statement of certification is limited to:

— identification (e.g., brand or company name) of the certified client
— the type of management system (e.g., research process or information security) and the applicable standard
— CIRQ as the certification body issuing the certificate

Note: Specific to ISO/IEC 27001:2022 or ISO/IEC 27001:2022 and ISO/IEC 27701:2019, as applicable, the client does not allow reference to its management system certification to be used in such a way as to imply that CIRQ certifies a product (including service) or process.

8. The use of the CIRQ Certification Mark(s) following initial certification is subject to annual review based on the successful result of subsequent annual surveillance audits or the re-certification audit. The client shall amend all advertising material when its scope of certification has been reduced.

9. CIRQ is also accredited to ISO/IEC 17065:2012, ISO/IEC 17021-1:2015 and ISO/IEC 27006:2015 through the ANSI National Accreditation Body (ANAB). As such, CIRQ shall authorize each organization under its accredited certification system only so long as the organization continues to operate in conformance with its certified management system to apply the ANAB accreditation symbol with CIRQ's own symbol only on those organization documents that relate to the certified management system and not on a product or in any way that could imply product, process, or service certification.

10. CIRQ reserves the right to suspend or withdraw a company's certification under the Standard and its use of the CIRQ Certification Mark(s) based on failure to comply with the Standard as determined by the outcome of a CIRQ audit, violation of conformance to the standard, or misuse of the Certification Mark(s). Upon withdrawal of its certification, the client discontinues its use of all advertising matter that contains a reference to certification, as directed by CIRQ.

11. These Terms of Use are subject to review and revision, the continued use of the Certification Mark(s) after any such revision will be subject to such revised Terms of Use.

12. The CIRQ name and Certification Mark(s) are trademarks of CIRQ. CIRQ and Insights Association reserve the right to require that an organization in violation of trademark usage remove them from the organizational website and discontinue use of them should it be determined there is a breach of any conditions laid out in these Terms.

13. CIRQ recommends the following language for use in promotional materials in relation to a company's CIRQ certification: [Insert company name]
    a. *is committed to industry quality and maintains certification to* ***ISO 20252:2019*** *the International Standard for Market, Opinion and Survey Research including Insights and Data Analytics. This certification covers* [insert Statement of Applicability].

b. *is committed to industry quality and maintains certification to* ***ISO/IEC 27001:2022*** *the International Standard for Information technology — Security techniques — Information security management systems. This certification covers* [insert Statement of Applicability].

c. *is committed to industry quality and maintains certification to* ***ISO/IEC 27001:2022*** *the International Standard for Information technology — Security techniques — Information security management* ***systems and ISO/IEC 27701:2019*** *the International Standard for Privacy information management systems. This certification covers* [insert Statement of Applicability].

References:

- CIRQ logo (for internal CIRQ use only):

- Certification Institute for Research Quality aka CIRQ Certification Mark(s) (for use by certified companies according to the Terms outlined above)**:**

S2. Complaint Dispute Appeal and Corrective-Preventive Action Procedure

ISO/IEC 17065:2012, Clause 7.13
ISO/IEC 17021-1:2015, Clauses 9.7, 9.8

a). From Applicants or Certified Companies regarding CIRQ

In the event a customer or Applicant lodges an appeal regarding any application or certification-related decision, or complaint about the staff of CIRQ or its activities related to the auditing and certification process, or a dispute arises, the Managing Director along with two members of the CIRQ Board he/she selects (other than the Insights Association CEO and Insights Association's General Counsel), will form a Review Panel, hereinafter referred to as the Panel. No member of the Panel shall have a direct interest in the subject of the appeal, complaint or dispute in any form. The Managing Director serves as the chairperson of this Panel and documents the fact that all members of the Panel, including him/herself, are free from any financial, commercial or any other pressures that might influence the results of the process. The Managing Director will make the company lodging the appeal, complaint, or dispute aware of this fact.

This Panel will review the appeal to determine its validity or review the complaint or dispute to substantiate its content. If valid or substantiated, the Panel will proceed with the review process, and make the company lodging the appeal, complaint or dispute aware of the timeline for the review process. Submission, investigation and decision on complaints/disputes/appeals shall not result in any discriminatory actions against the complainant.

CIRQ strongly prefers that appeals, complaints or disputes be submitted in writing to the Managing Director of CIRQ by registered mail, or equivalent, within reasonable timeframes following the occurrence of the event which caused the appeal, complaint or dispute. Upon receipt, the Managing Director will acknowledge receipt to the sender and convene the Panel as soon as is reasonably possible.

If requested by members of the Panel to provide information in relation to an appeal, complaint or dispute, the staff involved in the event or audit of a company, or a decision related to an application shall do so. The provision of information will be without prejudice toward all others.

Panel members shall have an obligation of confidentiality concerning anything that might come to their knowledge during their function on this Panel, with regard to the certified company or applicant. They have the right to consult experts and to take all measures and make all provisions, including the convening of one or more sessions, deemed necessary for a sound judgment.

All communications regarding the appeal, complaint or dispute must be documented in writing and kept in the appropriate Appeal/Complaint/Dispute file on the CIRQ Intranet site. Members of the Panel shall judge in all fairness. The members are, however, bound by all applicable policies and procedures as documented in CIRQ's Quality Manual. The Panel decides on the appeal, complaint or dispute by a majority of votes and the Managing Director informs the parties concerned, in writing, of the judgment including the rationale for the decision, and any subsequent corrective actions required. The judgments of the Panel are considered binding. The Managing Director shall follow up to ensure that recommended actions have been taken and are effective according to the Corrective Action procedures, document the outcome in the appropriate Appeal/Complaint/Dispute file, inform the other Panel members, and update the appropriate register.

Note: The decision to be communicated to the complainant shall be made by, or reviewed and approved by, CIRQ personnel not previously involved in the subject of the complaint.

b). From companies or from individuals about a certified company

Individuals participating in a research project conducted by a certified company or another company that becomes aware of a certain practice employed by a certified company may contact CIRQ to file a complaint about the certified company. In these instances, a number of steps will occur:

1. The individual or company will be requested to contact the Insights Association, so that Insights Association can review the situation against the Insights Association Code of Standards and Ethics for Survey Research and take appropriate action.
2. the complaint will be passed on to the certified company and they will be asked to take appropriate action to address the complaint; and
3. A record of the complaint will be saved in the Client Master file on the CIRQ Intranet site and entered into the Complaint/Appeal/Dispute Log.

Depending on the severity of the complaint as it relates to the requirements of the ISO standard to which the company is certified, it may be followed-up on at the next audit (for less severe complaints) or a random audit may be scheduled to follow up on it prior to the next scheduled audit (more severe complaints). CIRQ shall determine, together with the certified client and the complainant, whether and, if so to what extent, the subject of the complaint and its resolution shall be made public.

Required Records:

- Appeal/Complaint/Dispute Forms (FS2001) submitted to CIRQ
- Complaint/Dispute/Appeal and Corrective & Preventive Actions Log (FS2002)

References:

- S2 Complaint Dispute Appeal AND Corrective-Preventive Action Procedure (Level 2)
- WBC 7003 1.0 CIRQ Audit Report ISO/IEC 27001:2022+ISO 27701

S3. Internal Audits and Corrective Actions

ISO/IEC 17065:2012, Clauses 8.6, 8.7, 8.8
ISO/IEC 17021-1:2015, Clause 10.2.6

Internal Audits: CIRQ will periodically conduct internal audits of its Quality System in order to ensure that:

a. all policies and procedures are being implemented as described in this manual and in the more detailed Level 2 Procedures.
b. the QS remains suitable, adequate, and effective; and
c. opportunities for improvement are identified and acted upon.

When the level of customer activity reaches a substantive level, more specific procedures will be identified to address the frequency, style and quantity of internal audits to be conducted.

Internal auditors may be employees of CIRQ or may be consultants used by CIRQ. In either case, they shall be thoroughly familiar with CIRQ's Quality System, and ISO 17065:2012 and ISO/IEC 17021-1:2015 on which it is based.

Prior to each audit, the audit scope shall be defined, and auditors assigned so that (where possible) they will not audit their own work and will not have direct responsibilities for the activities to be audited. When audits take place, they shall consider the results of previous audits, the importance of the activities to be audited to the Quality System, as well as the maturity and stability of the QS. When and if Non-Conformances are discovered or customer complaints occur, the audit frequency should be increased, as appropriate.

Corrective Actions: CIRQ will review the corrections, identified causes and corrective actions submitted by the internal auditor to determine if these are acceptable. CIRQ will verify the effectiveness of any correction and corrective actions taken. The evidence obtained to support the resolution of nonconformities will be recorded in the Internal Master Audit Schedule.

Verification of effectiveness of correction and corrective action can be carried out based on a review of documented information provided by the client, or where necessary, through verification on-site. Usually this activity is done by a member of the internal audit team.

Required Records

- Internal Audit +Mgmt Review Schedule Master (FS3001)
- Internal Audit Checklist (FS3002)
- Internal Audit Report (FS3002)

References:

- S3 Level 2 procedures on the CIRQ Intranet site
- CIRQ Quality Manual

S4. Management Reviews

ISO/IEC 17065:2012, Clauses 8.5.2-8.5.3
ISO/IEC 17021-1:2015, Clauses 10.2.5.2-10.2.5.3

CIRQ's Managing Director shall periodically review the continuing suitability, adequacy and effectiveness of the QS with the CIRQ Board. These management reviews shall include:

- An assessment of improvement opportunities for CIRQ based on:
  - internal audits
  - process performance
  - status of preventive/corrective actions
  - customer feedback
- Discussion and agreement regarding any change to the Quality System, including the quality policy and quality objectives
- Update on the Info. Technology support for CIRQ
- Recent and upcoming audit activity with customers
- Status of certifications (granted, denied, suspended, or withdrawn)
- Status and trends related to complaints, disputes and appeals
- Review Risk Register and actions to address risks
- Review of CIRQ's finances

Outputs from Management Reviews shall include decisions and actions related to:

a) Corrective actions needed,
b) Improvement to the QS and its processes,
c) Improvement in service, related to meeting customer requirements, and
d) Resource needs.

The Managing Director shall ensure that agreed upon corrective actions are implemented and report the outcomes back to the CIRQ Board within an agreed upon timeframe.

Management Reviews shall be held once each year, at a minimum. In addition, the Managing Director or the CIRQ Board may review quality issues periodically and may decide to hold additional Management Reviews as needed. Results of all Management Reviews are recorded by the Managing Director and retained on the CIRQ Intranet.

Required Records:

- Agenda & Meeting Minutes from Mgmt. Reviews

References:

- S4 Level 2 procedures on the CIRQ Intranet site
- Internal Audit +Mgmt Review Schedule Master (FS3001)
- Mgmt. Review Agenda Guidelines (GLS4001)

S5. Handling, Control, Retention and Security of Records/Documents

ISO/IEC 17065:2012, Clauses 7.12, 8.3, 8.4
ISO/IEC 17021-1:2015, Clause 8.2, 8.5, 10.2.4
ISO/IEC 27006:2015, Clause 8.4.1 IS 8.4

This procedure covers the document retention, control and security procedures, in compliance with the above noted clauses of ISO/IEC 17065:2012, ISO/IEC 17021-1:2015 and ISO/IEC 27006:2015 and includes:

- CIRQ Intranet System security and controls

- Record maintenance system
- Record retention
- Confidentiality of information obtained during certification
- Record destruction
- Third party disclosure

CIRQ shall maintain the following types of records, which will be continuously updated on the secure, password protected CIRQ Intranet.

1. Updated information regarding the annual moderation of CIRQ and CIRQ processes
2. The CIRQ Quality Manual (referred to as Level 1 documentation)
3. CIRQ Procedures for operating a certification body, Core, Core IS and Support (referred to as Level 2 documentation)
4. Forms, checklists, templates and other support documentation that become required records (referred to as Level 3 documentation)
5. Actual records required by ISO/IEC 17065:2012 and ISO/IEC 17021-1:2015 including records relating to CIRQ rules and procedures for granting, maintaining, suspending, or revoking certification
6. CIRQ personnel documentation
7. Records relating to the certification management processes and outcomes of ISO 20252:2019, ISO/IEC 27001:2022 and ISO/IEC 27701 certified companies.

References:

- The S5 procedure in Level 2 on the CIRQ Intranet site.

S6. Documentation

ISO/IEC 17065:2012 - Clause 8.2
ISO/IEC 17021-1:2015, Clause 8.2, 8.5, 10.2.4
ISO/IEC 27006:2015, Clause 8.4.1 IS 8.4

The following information will be documented and maintained by CIRQ, updated at least annually by the Managing Director and made available upon request:

- Information regarding the fact that CIRQ is an accredited certification body established to certify survey research providers to the ISO 20252:2019, ISO/IEC 27001:2022 and ISO/IEC 27701:2019 standards and explain why this accreditation is necessary. This information will also indicate that CIRQ's Quality System is audited by external audits assigned by the American National Standards Institute's National Accreditation Body (ANAB), and that it will be audited in the same fashion annually.
- A statement briefly describing its product certification system which will include the rules and procedures for granting, extending, maintaining, suspending or withdrawing certification.
- An overview of the steps involved in the auditing and certification process.
- A directory of certified companies and their scope of certification (Certification Register)
- CIRQ Audit & Certification Fees.
- CIRQ finances.
- Rights and duties of applicants and certified companies regarding the use of the Certification Mark(s) and the acceptable ways a Company shall refer to the certification granted.
- Information regarding the handling of complaints, appeals, and disputes.

To support auditing and certification services, CIRQ has established, documented, and maintains a Quality System (QS). Documentation for this system exists at several levels that start with a very broad and general perspective at Level 1 and become more detailed and specific at subsequent levels. A Document Register will be maintained to track versions and will be stored on the CIRQ Intranet in

CIRQ Records.

These document levels are described below:

Level 1 Documents consist primarily of the Quality Policy, the Quality Objectives, and this Quality Manual, along with several other documents that are controlled and only change on a very infrequent basis such as the Audit & Certification Fees. The Quality Manual contains the Quality Policy and the Quality Objectives and also references other policies and the processes constituting the Quality System, which have been established to conform to the requirements of ISO/IEC 17065:2012 and ISO/IEC 17021-1:2015.

The Quality Manual also contains references to QS procedures (Level 2 Documents), which further detail the processes defined later in this document. The Quality Manual and other Level 1 documents are controlled and maintained on the CIRQ Intranet site in the CIRQ Headquarters folder (Level 1) within the Document Vault.

Level 2 Documents include detailed procedures required by ISO/IEC 17065:2012 and ISO/IEC 17021-1:2015. They define steps taken to ensure the quality of services offered by CIRQ, show who is responsible for implementing the procedure, and indicate timelines for key steps of various procedures. Each Core, Core IS, and Support procedure is controlled and identified with a unique number corresponding to the process it describes (i.e., C2 for the Core #2 procedure, C3 for the Core #3 procedure, etc.). Related forms, checklists, templates, etc., reference materials, and required records are documented in the procedures. All of these Level 2 documents are controlled and maintained on the CIRQ Intranet site in the Document Vault within the Level 2 Procedures folder.

Level 3 Documents are the Standard Forms, Checklists, Templates, and Workbooks, required when implementing particular tasks of a procedure, where the absence of such documents may adversely affect quality. A document number and name are printed in the footer of each page to identify the controlled Level 3 documents. The document numbering system is as follows: the first letter represents whether the item is a Form, Template, Checklist, etc., the next letter and the first number identify the procedure that the document relates to (i.e., C1, S1, etc.) and the final 3 numbers indicate whether it is the first, second, third document, etc. related to that procedure. Revision status is indicated by adding a 1.1, 1.2, 1.3, etc. to the end of the document's original number. All of these Level 3 documents are stored and maintained on the CIRQ Intranet site in the Document Vault within the Level 3 folder.

Level 4 Documents are the Records created as a result of the CIRQ Quality System to provide objective evidence of compliance to requirements and of the effective operation of the QS. Level 4 documents include all records required by ISO/IEC 17065:2012 and ISO/IEC 17021-1:2015. All Level 4 records are stored and maintained on the CIRQ Intranet site in the Filing Cabinet. If the records are client-specific they are maintained in the master client folder and if they are specific to CIRQ operations, and not to a specific client, they are stored in the CIRQ Records folder.

Note: The CIRQ MD maintains all client folders on a company-owned, password protected laptop as a temporary space until completed/finalized documents can proceed to being uploaded into the Client Folder(s) on the CIRQ Intranet. During annual internal audits, it should be considered that client-specific audit documents are not missing; rather, they have been placed in the temporary client folder to be reviewed and approved for completion. Full review of the annual CLC Annual Audit Checklist serves as the guide to ensure all documentation is migrated to the CIRQ Intranet client folder at the completion of an audit.

To further control and maintain CIRQ documentation the following rules shall apply:

- Each applicant shall be assigned a unique identifying number upon receipt of their completed Request for Quotation (or Application) and will retain this number throughout the 3 year cycle and beyond. The numbering format shall start with a four digit sequential number beginning with 1000, followed by the date the Request for Quotation (Application) is received in a 6 digit format (xxxxxx). EXAMPLE: If the first Request for Quotation is received on March 5, 2010, that company would be numbered as '1000030510'.

Certificates of Compliance for ISO 20252:2019, ISO/IEC 27001:2022, and ISO/IEC 27001:2022 + ISO/IEC 27701:2019, as applicable will be numbered with the first 4 digits of the unique client number described above.

- Electronic records specific to a particular company shall be labeled starting with the company name, followed by the company number followed by the document name, followed by the date the record was created. An EXAMPLE follows:
    - XYZ Research '1000030510_ Audit Report_05.08.18
- Only the CIRQ Managing Director shall have rights to make revisions to any controlled document and shall notify all appropriate CIRQ personnel when a revision occurs.
- Access to the CIRQ Intranet site will be controlled to CIRQ personnel as follows
    - The CIRQ Managing Director is the only person who shall have read and write privileges
    - The Training and Audit Advisor, The Technical Advisor, and the Auditors will have read only rights and will be able to save records to their personal folder, or to assigned client folders on this site on an ad hoc basis. As of this 2019 revision, the Managing Director of CIRQ is its only employee. At the discretion of the Managing Director, the Training and Audit Advisor may be given read and write privileges to assist with internal audits or other updates to the quality system.
    - CIRQ Board members will have "read only" access to the Level 1 folder in the Vault.

References:

- CIRQ Intranet
- S6 Documentation procedure at Level 2 on the Intranet

S7. Human Resource

ISO/IEC 17065:2012, Clause 6.1
ISO/IEC 17021-1:2015, Clause 7.3, Annex A (normative)

The policies and procedures contained in the CIRQ Organization Handbook apply to employees of CIRQ. In addition, there are Level 2 procedures in S7 that shall apply to CIRQ staff as listed below:

- Hiring procedures including Confidentiality & Conflict of Interest Orientation
- Training of staff (new and existing) regarding the QS
- Performance Evaluations
- Sub-contracting

Required Records:

- Training Records on CIRQ Intranet
- Independent Contractor/Consultant Agreement Template (TS7001, TS7002, TS7003)
- New Auditor Training Assessment Report (FS7001)
- Auditor Assessment (FS7003)

References:

- S7 procedure in Level 2 on the CIRQ Intranet site
- Independent Contractor/Consultant Agreement Template (TS7001, TS7002, TS7003)

- New Auditor Training Assessment Report (FS7001)
- Auditor Assessment Form (FS7003)
- Annex A Verification Matrix

S8. Changes in Certification Requirements

ISO 17065:2012, 7.4, 7.5, 7.6, 7.7, 7.8, 7.10, 7.12

This procedure describes the steps that shall be taken when changes occur in ISO 20252 or ISO/IEC 27001 and ISO/IEC 27701:2019 or in CIRQ's certification scheme applying to these standards. These changes may require notification to clients and/or CIRQ staff.

CIRQ will communicate changes affecting certification and shall include, if required, the following:

- Initial, surveillance and recertification audits
- Audit report review
- Audit report and certification decision
- Issuance of revised formal certificate to extend or reduce the scope of certification
- Issuance of certification documentation of revised surveillance activities

CIRQ shall include the rationale for excluding any of the above activities (e.g. when a certification requirement that is not a product requirement changes, and no evaluation, review or decision activities are necessary).

Required Records:

- Written communications to clients describing change stored in Client folder on CIRQ Intranet
- Written communications to staff describing change stored in Personnel folder on CIRQ Intranet
- Updates to Changes in Certification Requirements Register (DS8001) on CIRQ Intranet, Level 3 in the Document Vault

References:

- S8 Procedure in Level 2 on the CIRQ Intranet site

S9 Australia Audit & Certification Procedure

*Note: This support process is not in effect beginning February 2022. CIRQ made the decision to place ADIA partnership on hold and may resume in the future.

This procedure describes the steps that shall be taken when an Australian small to medium sized market research company, who is also a member in good standing of the Australian Data and Insights Association (ADIA), completes an ISO 20252:2019 RFQ with CIRQ and is approved by ADIA to participate.

Required Records:

- Request for Quotation and client Quality Manual
- Completed WBC 3003 1.6 ISO 20252 2019 Client Self-Assessment Quality Manual and RFQ & Standard Cert Agreement and Auth to Proceed
- CLC 7001 1.4 Audit Program Checklist

References:

- ADIA CIRQ MOU Dec 2021 – ISO 20252:2019 Guidelines

- S9 Procedure in Level 2 on the CIRQ Intranet site

S10 Expiration of Certification Procedure

ISO/IEC 17021-1:2015 9.6.3.2.5

This procedure describes the steps that shall be taken when a company is approaching the expiration date of their ISO 20252:2019 certification. It also covers the process in which a client may withdraw its certification, or suspension, in cases where its ISMS has persistently or seriously failed to meet requirements.

For ISO/IEC 27001:2022, following suspension, withdrawal, or expiration of certification, CIRQ can restore certification within 6 months provided that the outstanding recertification activities for ISO/IEC 27001:2022 are completed, otherwise at least a stage 2 audit shall be conducted. The effective date on the certificate shall be on or after the recertification decision and the expiry date shall be based on the prior certification cycle.

Note: This requirement is also used for expired certificates, and the certification documents will also show the gap in certification.

The process for CIRQ suspending a client certification can occur in cases when, for example:

— the client's certified ISMS has persistently or seriously failed to meet certification requirements, including requirements for the effectiveness of the ISMS, as discovered during the course of an audit, receipt of a complaint from a clients' customer, etc.
— the certified client does not allow surveillance or recertification audits to be conducted at the required annual frequencies as set forth in the 3yr audit plan
— the certified client has voluntarily requested a suspension

During the suspension process, which is unlikely to exceed 6 months, the client's management system certification is temporarily invalid. CIRQ's managing director will schedule a phone call with the client representative to review the S1 Terms of Use of CIRQ Certification Marks to review all sections relevant to claims, statements, and text indicating ISO/IEC 27001:2022 certification. A .pdf letter emailed to the client and appropriate representatives will follow to document the terms of the suspension (e.g., steps the clients must take to cease and immediately terminate all claims of its certification) as well as the process to restore certification.

As mentioned above, the client can request restoration of its certification within 6 months, in cases of suspension, withdrawal or expiration. In cases of suspension, the client must resolve all issues that caused the suspension, follow the CIRQ process and all requirements for doing so.

CIRQ shall restore the suspended certification if the issue that has resulted in the suspension has been resolved. Failure to resolve the issues that have resulted within 45 days shall result in withdrawal or reduction of the scope of certification. CIRQ will reduce the scope of certification to exclude the parts not meeting the requirements when the certified client has persistently or seriously failed to meet the certification requirements for those parts of the scope of certification. Any such reduction shall be in line with the requirements of the standard used for certification.

For clients who decide to seek certification after withdrawal of certification CIRQ will require the client to start the application through certification process over again. The Core Process Definitions for ISMS Certification, which covers the certification process in detail, begins on page 35.

Required Records:

- Written communication to client notifying them of upcoming expiration date, stored in Client folder on CIRQ Intranet

- FC 2005 1.0 ISO/IEC 27001:2022 Audit Program Log
- CLC 7001 1.4 Audit Program Checklist
- S1 Terms of Use of CIRQ Certification Marks

References:

- S10 Procedure in Level 2 on the CIRQ Intranet site

S11. Risk Management Procedure

ISO/IEC 17021-1:2015, Clause 5.2.3

In order to maintain the impartiality and credibility of CIRQ as an auditing and certification body, an assessment of risks will be undertaken on an as needed basis, and minimally at least once a year. Identified risks and the threats posed will be documented on the Risk Register along with an assessment of the level of risk (High, Medium, Low) and steps taken to prevent or correct situations that occur.

Required Records:

- Risk Register on CIRQ Intranet, Level 2 in the Document Vault

References:

- S11 Procedure in Level 2 on the CIRQ Intranet site

XII. APPENDIX

A. References

(ISO/IEC 17065:2012 - Clause 2)

- ISO/IEC 17065:2012
- ISO 20252:2019
- ISO/IEC 17021-1:2015
- ICO/IEC 27006:2013
- ISO/IEC 27001:2022
- ISO/IEC 27701:2019
- *Accreditation requirements for organisations providing certification services to ISO 20252: 2019 Market, opinion and social research including insights and data analytics within the territorial jurisdictions of Australia, UK and USA* (2020)
- CIRQ Organization Handbook 2020
- Insights Association's Code of Standards and Ethics for Marketing Research and Data Analytics 2021
- Insights Association's Employee Handbook
- Federal legislation in the U.S.
  - HIPPA
  - SOC/SOC2
  - GLB
  - COPPA
- Privacy Shield requirements

- GDPR

CIRQ Quality Manual for Personnel Signature

I acknowledge that I have reviewed the most current available revision of the CIRQ Quality Manual, containing the full scope of CIRQ's audit processes, certification requirements and other relevant requirements, available in PDF file format and on the CIRQ.org website.

_____

Print name

_____

Signature

_____

Date