Schema per la certificazione dei sistemi di gestione della sicurezza delle informazioni (SGSI), secondo lo Schema ISO/IEC 27001

05	13/03/2023	Errata Corrige Circolare tecnica DC N° 04/ 2023 - Circolare Tecnica Accredia DC N° 15/2023	OPE	DIR ISG	DIR OPE
04	06/03/2023	Nuova norma ISO/IEC 27001:2022	OPE	DIR ISG	DIR OPE
03	22/01/2022	Recepimento dei rilievi Accredia in merito alle disposizioni della norma ISO/IEC 27006:2015/Amd 1:2020	OPE	DIR ISG	DIR OPE
02	24/09/2020	Recepimento delle disposizioni della norma ISO/IEC 27006:2015/Amd 1:2020	OPE	DIR ISG	DIR OPE
01	08/09/2018	Recepimento rilievi Accredia	OPE	DIR ISG	DIR OPE
00	27/01/2017	Prima emissione. Annulla e sostituisce il 0019CR	SG	ISG	DIR
Rev.	*Data*	*Descrizione*	*Redatto*	*Verificato*	*Approvato*
IDENTIFICAZIONE: 00428CS_05_IT					

ICIM SpA Società soggetta all'attività di direzione e coordinamento di ICIM GROUP Srl
Piazza Don Enrico Mapelli, 75 - 20099 Sesto San Giovanni (MI) - Tel. +39 02 725341 Fax +39 02 72002098 - www.icim.it - info@icim.it
Capitale sociale € 260.000,00 int. versato ed esistente - C.F./P.IVA e Iscriz. Reg. Imprese di Milano n. 12908230159 – R.E.A. n. 1596292

SOMMARIO

1.0 SCOPO E CAMPO DI APPLICAZIONE

Il presente Schema di Certificazione definisce i requisiti particolari a cui un'Organizzazione che richiede la certificazione del proprio Sistema di Gestione per la Sicurezza delle Informazioni (SSGI) deve conformarsi per ottenere e mantenere la certificazione rilasciata da ICIM e per l'iscrizione nel relativo Registro delle Organizzazioni in possesso della certificazione.

Il presente Schema di Certificazione costituisce parte integrante del Regolamento di Certificazione dei Sistemi di Gestione (0002CR) e del Regolamento Generale ICIM (0001CR).

Sull'applicazione del presente Schema sorveglia un Comitato per la salvaguardia dell'Imparzialità (CI), nel quale sono rappresentate le componenti interessate alla certificazione.

Il certificato ICIM è il documento con il quale ICIM attesta che l'Organizzazione richiedente opera con un SGSI conforme alle norme di riferimento.

2.0 RIFERIMENTI NORMATIVI

Norme e documenti validi alla data di emissione del presente documento

ICIM 0001CR	Regolamento generale ICIM per l'erogazione dei servizi
ICIM 0002CR	Regolamento per la certificazione dei sistemi di gestione
UNI CEI ISO/IEC 27001	Tecnologie informatiche - Tecniche per la sicurezza - Sistemi di gestione per la sicurezza delle informazioni - Requisiti
UNI CEI ISO/IEC 27002	Tecnologie informatiche - Tecniche per la sicurezza - Raccolta di prassi sui controlli per la sicurezza delle informazioni
ISO/IEC 27006	Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems
UNI CEI EN ISO/IEC 27001:2014	Tecnologie informatiche – Tecniche di sicurezza – Sistemi di gestione della sicurezza dell'informazione
UNI CEI EN ISO/IEC 27001:2017	Tecnologie informatiche – Tecniche di sicurezza – Sistemi di gestione della sicurezza dell'informazione
Circolare informativa N° 27/2017	Comunicazione Accredia in merito all'adeguamento delle certificazioni per lo schema SSI
ISO/IEC 27006:2015/Amd 1:2020	Disposizioni in materia di transizione degli accreditamenti degli Organismi di Certificazione (OdC) di sistemi di gestione dalla norma ISO/IEC 27006:2015 alla norma
IAF MD 26:2022	Transition Requirements for ISO/IEC 27001:2022 issue 1
ISO/IEC 27001:2022	Tecnologie informatiche – Tecniche di sicurezza – Sistemi di gestione della sicurezza dell'informazione
Circolare Tecnica Accredia DC N° 04/2023	Disposizioni in materia di transizione delle certificazioni accreditate a fronte della norma ISO/IEC 27001 e relativo adeguamento degli accreditamenti degli Organismi di Certificazione accreditati per lo schema SSI (ISMS) per l'edizione 2022.

Circolare Tecnica Accredia DC N° 15/2023	Errata Corrige Circolare tecnica DC N° 04/ 2023
ISO/IEC 27002:2022	Information security, cybersecurity and privacy protection — Information security controls

3.0 DEFINIZIONI

Ai fini del presente Schema valgono le definizioni riportate nella norma ISO/IEC 27001 e nella ISO/IEC 27006 a cui si rimanda.

4.0 CONDIZIONI GENERALI

Perché venga attivata la procedura di certificazione da parte di ICIM, l'Organizzazione richiedente deve:

- disporre di un SGSI che risponda alle esigenze del modello definito dalla normativa di riferimento e dalle eventuali prescrizioni particolari stabilite per tipologia di processo/prodotto/servizio;
- accettare le condizioni fissate dal presente Schema e le condizioni contrattuali per la certificazione.

I siti aziendali oggetto della certificazione sono sottoposti, prima della stipula delle condizioni contrattuali, ad una valutazione critica da parte di ICIM, in relazione a:

- impatto sui parametri di riservatezza, integrità, disponibilità dei dati
- influenza sul perimetro fisico di protezione, logico e organizzativo.

Durante la visita di valutazione o sorveglianza del SGSI l'Organizzazione che ha presentato la domanda di certificazione ad ICIM deve garantire agli auditor ICIM il libero accesso alle aree aziendali, alle informazioni e alla documentazione necessarie per svolgere il programma della visita.

L'Organizzazione ha la facoltà di negare l'accesso a ICIM a informazioni ritenute confidenziali o sensibili. ICIM si riserva il diritto, qualora ritenga impossibile svolgere la valutazione di certificabilità in assenza di questo accesso, di declinare la richiesta.

L'eventuale verifica conseguente a variazioni può comportare modifiche dei corrispettivi applicati ovvero l'addebito di oneri aggiuntivi. I criteri operativi e gestionali attuati da ICIM in occasione di Variazioni anagrafiche per trasferimento della titolarità/cambio di ragione sociale dell'Organizzazione certificata sono definiti da ICIM nell'Istruzione "Variazione anagrafica e dati amministrativi" (0228BI).

ICIM eroga le proprie attività di valutazione con personale appositamente qualificato e rispondente a requisiti e caratteristiche stabilite nella procedura ICIM "Criteri per la selezione dei valutatori" (0282BP).

Le prestazioni soddisfacenti da parte di tutto il personale ICIM coinvolto nelle attività di audit e certificazione, nel rispetto delle prescrizioni applicabili, sono garantite attuando forme di monitoraggio documentale e operativo in accordo alla procedura ICIM 0281BP - Monitoraggio degli auditor e personale interno ABS.

L'Organizzazione in possesso di certificazione ICIM può utilizzare il Marchio di Conformità ICIM e altri marchi di conformità, per il cui uso sia data esplicita autorizzazione, conseguenti ad adesioni e/o ad accordi di riconoscimento con organizzazioni nazionali e internazionali o per specifici schemi di certificazioni su documentazione tecnica e pubblicitaria purché sia fatto in modo da non essere interpretato come una certificazione di prodotto e vengano soddisfatti i requisiti ICIM per l'utilizzo del Marchio di Conformità così come definiti nel documento ICIM 0002CR.

Il Marchio di Conformità ICIM non deve essere applicato su un prodotto, né in modo tale che si possa credere che esso certifichi la conformità di un prodotto.

5.0 PROCEDURA PER LA CERTIFICAZIONE DEL SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI (SGSI)

5.1 Processo commerciale

Il processo commerciale si compone delle seguenti fasi:

- Compilazione della Richiesta d'Offerta (RdO);
- Verifica RdO e Riesame Offerta;
- Emissione e invio Offerta;
- Follow up;
- Chiusura Contratto e invio Domanda di Certificazione accettata;
- Riesame Contratto

Responsabilità, criteri operativi e regole tecniche applicabili per la conduzione di tali attività sono specificate nell'Istruzione Commerciale 0025BI - Modalità di predisposizione offerte per la certificazione SGSI (Information Security).

5.2 Audit iniziale

Il processo ICIM per la certificazione del SGSI dell'Organizzazione è strutturato in due fasi:

- Audit di Fase 1 - esame documentale + audit preliminare (in sito)
- Audit di Fase 2 - audit di valutazione (in sito).

L'audit di Fase 1 ha, in aggiunta a quanto già definito del Regolamento 0002CR, lo scopo di:

- verificare la completezza e l'adeguatezza delle informazioni generali (es.: settore merceologico, prodotti o servizi forniti, sedi, stabilimenti, numero di addetti, ecc.);
- valutare se il SGSI dell'Organizzazione richiedente è conforme alla normativa di riferimento e al campo di applicazione ed è operativo, esaminando come minimo i seguenti documenti:
  - Manuale del SGSI, o in alternativa documentazione equivalente che descriva gli elementi base del SGSI
  - Analisi dei Rischi correlati alla sicurezza delle informazioni
  - Dichiarazione di applicabilità del SGSI (SOA - Statement of Applicability) in conformità alla ISO / IEC 27001: 2022. Il riferimento sui documenti di certificazione deve essere chiaramente indicato come solo una fonte di verifica per i controlli applicati nella Dichiarazione di Applicabilità e non una certificazione della stessa.
  - Pianificazione delle verifiche ispettive interne;
  - Riesame della direzione;
- comprendere il significato del SGSI nel contesto della politica e degli obiettivi dell'organizzazione del cliente (analisi preliminare di business); tale analisi è tesa a confermare quanto rilevato, in fase di analisi documentale, da parte delle funzioni interne ICIM.
- valutare se il livello di attuazione del SGSI dell'Organizzazione è adeguato a poter pianificare la successiva visita di Valutazione di Fase 2.

La Fase 1 viene solitamente condotta presso la sede dell'Organizzazione[1], a tutela della riservatezza della documentazione aziendale (in particolare per quanto riguarda l'analisi dei rischi e la dichiarazione d'applicabilità).

In particolari condizioni, quali, ridotte dimensioni dell'Organizzazione, limitata complessità dei processi, rischi di bassa rilevanza, previo accordo con l'azienda, la Fase 1 può essere condotta in parte direttamente in sede ICIM. In tal caso l'attività in ICIM si limita alla valutazione di documenti non critici per la sicurezza delle informazioni. In ogni caso, per valutare la coerenza tra scopo della certificazione e business aziendale, e il livello di preparazione dell'organizzazione per la Fase 2, viene eseguito per lo meno un sopralluogo in azienda a completamento della Fase 1.

Anche in questo caso, vengono adottate adeguate misure tecniche di protezione della riservatezza e dell'integrità dei documenti aziendali.

Nel rapporto viene anche confermato quanto valutato nella Fase 1 in merito al significato del SGSI in relazione alla politica e agli obiettivi dell'organizzazione (analisi preliminare di business).

L'audit di Fase 2 invece, è attivato in seguito all'esito positivo dell'audit di Fase 1, in accordo all'Organizzazione, ed ha lo scopo di (in aggiunta a quanto già definito del Regolamento 0002CR):

- verificare che l'organizzazione dimostri che l'analisi delle minacce di sicurezza sia adeguatamente considerata ai fini dell'operatività aziendale
- verificare che l'organizzazione possieda procedure per l'identificazione, esame e valutazione delle minacce di sicurezza, che siano coerenti con la politica e gli obiettivi manageriali.

ICIM ha definito responsabilità e modalità operative per la pianificazione di tali audit nella propria "Istruzione operativa per la gestione della pianificazione degli audit" (0185BI).

Eventuali deviazioni del Sistema dell'Organizzazione rispetto ai requisiti dettati dalla norma di riferimento, rilevati dagli auditor ICIM, devono essere classificate in:

Non conformità maggiore o critica2 - si intende l'assenza di uno o più di elementi della norma di riferimento o una situazione che genera dubbi significativi circa la capacità del sistema di conseguire gli obiettivi predisposti, con particolare riferimento al soddisfacimento degli aspetti cogenti e ai requisiti del prodotto.

Non conformità minore o non critica2 - si intende l'incapacità di soddisfare uno dei requisiti della norma di riferimento che, basandosi sul giudizio e l'esperienza, non genererà verosimilmente un non funzionamento del SGA o una riduzione della capacità del sistema di garantire processi e prodotti in condizioni controllate.

Raccomandazione2 - si intende la formulazione di indicazioni per il miglioramento del SGA dell'organizzazione. La raccomandazione non è vincolante per l'organizzazione.

Le non conformità emesse dal Gruppo di Audit sono classificate come sopra in funzione della loro Estensione, Sistematicità, Criticità, Influenza.

La classificazione della non conformità viene chiaramente indicata sul modulo di registrazione e motivata all'Organizzazione.

In ogni caso, le non conformità di carattere legislativo vengono sempre classificate non conformità Critiche (C).

[1] Ove lo ritenga tecnicamente opportuno, ICIM si riserva la possibilità di condurre off-site la parte di esame della documentazione del SGSI dell'organizzazione al fine di meglio preparare la visita in campo.

[2] ICIM ha rinominato le non conformità nel seguente modo:

- Non Conformità Critiche (C) = Non Conformità
- Non Conformità Non Critiche (NC) = Osservazioni

A fronte delle non conformità emerse nel corso dell'audit, l'Organizzazione deve:

- definire il trattamento delle non conformità;
- identificare le cause delle non conformità;
- proporre, ove necessario, un'azione correttiva per rimuovere le cause della non conformità.

Entro due settimane dalla data della visita, l'Organizzazione propone le azioni di risoluzione delle non conformità e le eventuali azioni correttive, indicando e sottoscrivendo nel modulo di registrazione delle non conformità le modalità di attuazione e i relativi tempi che verranno valutati da ICIM.

Se si evidenziano commenti o necessità di chiarimenti, ICIM informa l'organizzazione per iscritto.

In assenza di commenti, le risoluzioni proposte si considerano accettate da ICIM.

5.3 Esito della valutazione

L'esito dell'audit viene considerato:

- positivo se tutti gli elementi sono giudicati conformi alle prescrizioni della norma di riferimento, oppure se qualche elemento presenta "non conformità", purché tali "non conformità" siano classificate da ICIM come non critiche (NC), ovvero non pregiudichino sostanzialmente l'adeguatezza del SGSI applicato e le azioni correttive proposte dall'organizzazione valutata, siano giudicate da ICIM adeguate e congruenti come tempistica di attuazione con il programma di audit;
- insoddisfacente se vengono riscontrate non conformità classificate come Critiche (C), ovvero le non conformità si riferiscono a gravi carenze del SGSI valutato e/o al mancato rispetto di leggi e regolamenti applicabili.

5.4 Audit di transizione

L'audit di transizione deve includere, almeno, quanto segue:

- la gap analysis della ISO/IEC 27001:2022, nonché la necessità di modifiche al SSI (ISMS);
- l'aggiornamento della Dichiarazione di Applicabilità (SoA);
- se applicabile, l'aggiornamento del piano di trattamento dei rischi;
- l'implementazione e l'efficacia dei controlli nuovi o modificati scelti dai clienti.

5.4.1 Certificazioni già rilasciate a fronte della ISO/IEC 27001:2013

Tutte le certificazioni emesse sotto accreditamento a fronte della ISO/IEC 27001:2013 dovranno essere transitate al nuovo standard entro il **31 ottobre 2025**, in caso contrario l'OdC dovrà provvedere alla loro revoca.

5.4.2 Nuove Certificazioni a fronte della ISO/IEC 27001:2022

Dal 30 aprile 2024, tutte le nuove certificazioni ed i rinnovi dovranno essere emesse esclusivamente a fronte della ISO/IEC 27001:2022. L'attività di adeguamento deve prevedere una durata minima di 0,5 giorni/uomo aggiuntivi se effettuata attraverso un audit di rinnovo e di 1 giorno/uomo se effettuata attraverso un audit separato o di sorveglianza.

6.0 MANTENIMENTO E RINNOVO DELLA CERTIFICAZIONE SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

6.1 Mantenimento della certificazione

ICIM attua una sorveglianza del SGSI dell'Organizzazione in possesso di certificazione al fine di verificare la permanenza della conformità ai requisiti certificati. Tale sorveglianza avviene mediante visite la cui frequenza è almeno annuale.

La data del primo audit di sorveglianza, successivo alla certificazione iniziale, non deve superare i 12 (dodici) mesi dall'ultimo giorno dell'audit di Fase 2.

Nel periodo di validità della certificazione, 3 (tre) anni, vengono eseguite n. 2 (due) visite di sorveglianza.

Ogni audit di sorveglianza deve riesaminare parte dei processi dell'Organizzazione, affinché tutti i processi, relativamente al SGSI, vengano riesaminati entro ogni ciclo di 3 (tre) anni.

Nel corso della sorveglianza sul SGSI, è obbligatorio:

- Valutare sistematicamente l'evidenza, la gestione, e le azioni correttive conseguenti ai reclami cliente ricevuti dall'organizzazione certificata nel periodo intercorso dall'ultima verifica;
- Valutare, nel corso del triennio, tutte le minacce e le vulnerabilità che l'organizzazione, per le sue caratteristiche, presenta, in merito alla sicurezza delle informazioni;
- Verificare il mantenimento di una registrazione di tutti gli eventi correlati alla sicurezza delle informazioni (es. intrusioni, violazioni della privacy, ecc.).

ICIM, durante l'attività di sorveglianza, attua un appropriato controllo sull'uso, da parte dell'Organizzazione, della certificazione ICIM.

6.2 Rinnovo della Certificazione

Il rinnovo della certificazione è effettuato allo scadere di ogni triennio; richiede un ulteriore esame della documentazione del SGSI e comporta l'effettuazione da parte di ICIM di un audit di rinnovo presso l'Organizzazione svolto, di regola, secondo gli stessi criteri previsti per la Fase 2.

L'audit di rinnovo, da eseguire presso l'Organizzazione, viene effettuato con finalità e secondo modalità analoghe a quelle descritte nel Regolamento 0002CR.

Qualora in fase di rinnovo vengano rilevate delle non conformità, ICIM e l'Organizzazione concorderanno un periodo di tempo entro il quale dovranno essere corrette. Tale periodo di tempo verrà scelto in base alla criticità delle non conformità in relazione ai rischi individuati, e all'assicurazione della continuità di business e della fornitura di prodotti e servizi da parte dell'organizzazione. Qualora tale necessità di correzione non fosse soddisfatta da parte dell'azienda, il certificato verrà sospeso o ritirato.

Questo comporta di pianificare l'audit di rinnovo nei 6 (sei) mesi precedenti la scadenza del certificato e comunque di eseguirlo almeno un mese prima della data di scadenza.

Al termine del triennio, ICIM invierà quotazioni di rinnovo relative al successivo periodo di validità della certificazione.

7.0 TRASFERIMENTO DI CERTIFICATI ACCREDITATI

In aggiunta a quanto già indicato nel Regolamento di Certificazione dei Sistemi di Gestione (0002CR), ICIM ha definito i criteri e le modalità per effettuare il trasferimento ad ICIM delle certificazioni, in corso di validità ed accreditate, da altri OdC nell'istruzione "Criteri per il trasferimento delle certificazioni dei

Sistemi di Gestione" (0412BI) il cui contenuto è conforme alle disposizioni dettate dal documento IAF MD2 (Transfer of Accredited Certification of Management System).

8.0 SOSPENSIONE, RINUNCIA O REVOCA DELLA CERTIFICAZIONE

ICIM gestisce le attività di sospensione, rinuncia e revoca della certificazione di conformità alla norma ISO/IEC 27001 in accordo al regolamento 0001CR e alla "Procedura operativa sospensioni, rinunce e revoche" (0184BP) disponibile su richiesta.

Tutte le certificazioni emesse sotto accreditamento a fronte della ISO/IEC 27001:2013 dovranno essere transitate al nuovo standard entro il 31 ottobre 2025, in caso contrario ICIM dovrà provvedere alla loro revoca.