Schema per la certificazione dei sistemi di gestione della sicurezza delle informazioni (SGSI), secondo lo Schema ISO/IEC 27001 e integrazione delle linee guida ISO/IEC 27017:2015 e ISO/IEC 27018:2019

09	16/02/2026	Recepimento del Piano di Transizione alla ISO/IEC 27006-1:2024	CC	DIR GOV	DIR CC
08	19/03/2024	Integrazione delle linee guida ISO/IEC 27017:2015 e ISO/IEC 27018:2019	CC	GEA DIR GOV	DIR CC
07	26/06/2023	Modifiche § 6.2 sui tempi di rinnovo	CC	GEA DIR GOV	DIR CC
06	08/06/2023	Recepimento dei rilievi Accredia esame documentale di rinnovo di (CAB) del 20/03/2023	SG	ISG	DIR
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
Rev.	***Data***	***Descrizione***	***Redatto***	***Verificato***	***Approvato***
IDENTIFICAZIONE: 00428CS_09_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

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

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	Information security, cybersecurity and privacy protection — Information security management systems —Requirements
UNI CEI EN ISO IEC 27006-1 2024	Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems Sicurezza delle informazioni, cybersecurity e protezione della privacy- Requisiti per gli organismi che forniscono servizi di audit e certificazione dei sistemi di gestione per la sicurezza delle informazioni
IAF MD 29:2024	Transition requirements for ISO/IEC 27006-1:2024
Circolare tecnica DC N° 39/2024	Accreditamento ISO/IEC 17021-1 a fronte della ISO/IEC 27001 e ISO/IEC 27701
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	Information security, cybersecurity and privacy protection — Information security management systems — Requirements
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
ISO/IEC 27017:2015	(Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services)
ISO/IEC 27018:2019	(Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors)

3.0 DEFINIZIONI

Ai fini del presente Schema valgono le definizioni riportate nella norma ISO/IEC 27001 e nella UNI CEI EN ISO IEC 27006-1 2024 a cui si rimanda.

Le norme ISO/IEC 27017 e 27018 sono invece standard a livello internazionale per contribuire a garantire il rispetto dei principi e delle norme privacy, da parte dei providers di public cloud che se ne dotano.

Le norme, infatti, sono specificamente indirizzate ai service providers di public cloud che elaborano dati personali (PII - Personally Identifiable Information) e che agiscano in qualità di Data (PII)Processor.

Definiscono delle linee guida basate su ISO / IEC 27002, prendendo in considerazione i requisiti normativi per la protezione dei dati personali che possono essere applicabili nel contesto del panorama dei rischi di sicurezza informatica di un fornitore di servizi public cloud. Trattandosi di Linee guida, le norme ISO 27017 e 27018 non sono quindi norme certificabili: ciò nonostante, è possibile ottenere una integrazione di un certificato ISO/IEC 27001 esistente e rilasciato da un Ente Certificatore riconosciuto, a dimostrazione della capacità del Provider di assicurare la protezione dei dati personali, basato sulla integrazione delle Norme citate con la Norma ISO/IEC 27001.

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 (0227BI) e nell'Istruzione "Definizione dei tempi di audit per i Sistemi di Gestione" (0310BI).

Le organizzazioni che volessero chiedere l'aggiunta delle estensioni ISO/IEC 27017:2015 e ISO/IEC 27018:2019, come addendum alla Norma ISO/IEC 27001:2013 devono tenere in considerazione i seguenti requisiti espressi dall'Ente di Accreditamento:

- La Norma 27017:2015 può essere oggetto di estensione della certificazione anche da sola.
- Ove si intenda considerare tale estensione anche in ottica di Protezione Dati Personali, l'estensione alla Norma ISO/IEC 27017:2015 dovrà essere integrata con la Norma ISO/IEC 27018:2019.
- Non è ammessa l'estensione alla sola Norma ISO/IEC 27018:2019.

Se l'organizzazione è in possesso di altra certificazione ISO/IEC 27001 con altro organismo, dovrà richiedere il trasferimento della stessa ad ICIM, per consentire l'emissione del certificato integrato.

Relativamente ai tempi di valutazione per eventuali estensioni sulle linee guida occorre considerare un impegno di almeno mezza giornata per il sito principale e mezza giornata per ogni sito campionato, per linea guida.

Relativamente ai datacenter oggetto del servizio CLOUD (per le estensioni alle linee guida ISO/IEC 27017/27018) prima del rilascio della certificazione devono essere verificati tutti i data center presso cui sono dislocati i server che gestiscono il cloud.

Se i Data Center utilizzati per le attività "cloud" sono in outsourcing presso fornitori in possesso di certificazioni ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018 accreditate e riconosciute a livello MLA si potrà evitare di aggiungere tempo di audit presso tali siti. In tutti gli altri casi, dovranno essere aggiunte tante mezze giornate quanti sono i siti in outsourcing da verificare "de visu". Nel caso di siti ove non fosse possibile svolgere un audit diretto (es. fornitori come AWS, AZURE), dovrà essere utilizzata presso il sito centrale mezza giornata aggiuntiva, per la valutazione degli aspetti contrattuali e di controllo operativo con tali fornitori. Questo ultimo requisito è applicabile solamente nel caso di Data Center in possesso di certificazioni TIER III o TIER IV.

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;
    - 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 critica[2]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 critica[2] - 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.

Raccomandazione 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 ISO/IEC 27001:2022

a) l'audit di transizione non si baserà solo sulla revisione dei documenti, in particolare per la revisione dei controlli tecnologici;

b) l'audit di transizione deve includere, almeno, quanto segue:

- la gap analysis della ISO/IEC 27001:2022, nonché la necessità di modifiche allo schema MS (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;

c) l'OdC può condurre l'audit di transizione da remoto se garantisce il raggiungimento degli obiettivi dell'audit di transizione;

d) l'OdC prenderà la decisione di transizione in base al risultato dell'audit di transizione;

e) tutte le certificazioni basate su ISO/IEC 27001:2013 scadranno o saranno ritirate alla fine del periodo di transizione;

f) quando il documento di certificazione viene aggiornato al completamento con successo dell'audit di transizione, la scadenza del suo attuale ciclo di certificazione non verrà modificata, a meno che la transizione venga verificata nell'audit di rinnovo.

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 PIANO DI TRANSIZIONE ALLA ISO/IEC 27006-1:2024

6.1 Periodo di transizione

Gli organismi di certificazione devono completare la transizione alla norma ISO/IEC 27006-1:2024 entro il 31 marzo 2026. Ciò significa che, dopo la fine del periodo di transizione, qualsiasi certificazione conforme alla norma ISO 27001 dovrà basarsi esclusivamente sulla nuova edizione della norma ISO/IEC 27006-1:2024

6.2 Certificati

Le revisioni della norma ISO/IEC 27006-1:2024 non influiscono né sulla validità né sulla data di scadenza dei certificati esistenti.

6.3 Audit e rapporto di audit

Gli audit secondo la norma ISO/IEC 27006-1:2024 potranno essere effettuato solo una volta completata positivamente da parte di ICIM l'estensione e la transizione dell'accreditamento rilasciato da Accredia.

- Audit iniziali/rinnovo: Dopo il termine di transizione, ICIM applicherà la nuova norma per le suddette attività di certificazione.

- Audit da remoto: sono stati inseriti nella norma nuovi requisiti per l'effettuazione di audit da remoto. La conduzione di tali audit deve essere preventivamente valutata dal Responsabile del gruppo di Audit tramite una analisi del rischio che garantisca l'efficacia di tale metodologia nel raggiungimento degli obiettivi di audit. In caso di esito negativo dell'analisi, l'audit in remoto non potrà essere svolto.

a. nel caso in cui alcune o nessuna Unità Operativa sia fisicamente presente (es. una Organizzazione esegue il lavoro o fornisce un servizio online che consente alle persone coinvolte di eseguire processi indipendentemente dalla natura fisica del sito), il rapporto di audit e il documento di certificazione devono dichiarare che le attività del cliente sono condotte in remoto

b. Rimozione del limite 30%: Le attività di audit da remoto potranno superare il 30% del tempo totale.

- Calcolo dei tempi di audit: Aggiornamento delle metodologie per il calcolo dei tempi di audit (Allegato C), con particolare attenzione:

1. alle organizzazioni multi-sito con eventuale variazione dei tempi di Audit (rif. C.6 della norma ISO/IEC 27006-1:2024)

2. alla determinazione del numero di persone coinvolte nel processo di certificazione (rif. C.2.1 e C.3.4 della norma ISO/IEC 27006-1:2024)

- **Audit iniziali/rinnovo**: Dopo il termine di transizione, ICIM applicherà la nuova norma per le suddette attività di certificazione.

- **Audit da remoto**: sono stati inseriti nella norma nuovi requisiti per l'effettuazione di audit da remoto. La conduzione di tali audit deve essere preventivamente valutata dal Responsabile del gruppo di Audit tramite una analisi del rischio che garantisca l'efficacia di tale metodologia nel raggiungimento degli obiettivi di audit. In caso di esito negativo dell'analisi, l'audit in remoto non potrà essere svolto.

b. nel caso in cui alcune o nessuna Unità Operativa sia fisicamente presente (es. una Organizzazione esegue il lavoro o fornisce un servizio online che consente alle persone coinvolte di eseguire processi indipendentemente dalla natura fisica del sito), il rapporto di audit e il documento di certificazione devono dichiarare che le attività del cliente sono condotte in remoto

c. Rimozione del limite 30%: Le attività di audit da remoto potranno superare il 30% del tempo totale.

- **Calcolo dei tempi di audit**: Aggiornamento delle metodologie per il calcolo dei tempi di audit (Allegato C), con particolare attenzione:

  - alle organizzazioni multi-sito con potenziale incremento dei tempi di Audit (rif. C.6 della norma ISO/IEC 27006-1:2024)

  - alla determinazione del numero di persone coinvolte nel processo di certificazione (rif. C.2.1 e C.3.4 della norma ISO/IEC 27006-1:2024)

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

7.1 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 la sicurezza delle informazioni in termini di integrità, disponibilità e riservatezza;

- Valutare sistematicamente l'evidenza, la gestione, e le azioni correttive conseguenti agli incidenti 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.

7.2 Rinnovo della Certificazione

Allo scadere di ogni triennio il rinnovo della certificazione richiede un ulteriore esame documentale e comporta un audit del SGsi dell'Organizzazione, da pianificarsi nei 6 (sei) mesi precedenti la scadenza del certificato.

Non sono ammesse proroghe alle scadenze dei certificati. Tuttavia, è possibile dare continuità al certificato scaduto alle seguenti condizioni:

- se entro 3 mesi dalla scadenza del certificato è eseguita la verifica di rinnovo;
- se fra 3-6 mesi dalla scadenza del certificato, è eseguita la verifica di ripristino con i tempi di una nuova certificazione (Fase 2);
- evidenziando sul certificato il lasso temporale di mancata copertura della certificazione.

L'audit di rinnovo si deve concludere positivamente e in tempo utile (almeno 2 mesi prima la scadenza del certificato), per permettere l'approvazione da parte di ICIM della proposta di rinnovo del certificato e la sua conseguente riemissione, nei tempi opportuni.

Quando l'Organizzazione non ottemperi al soddisfacimento di tale tempistica e quindi, non ottenga il rinnovo del certificato entro i termini di scadenza, il certificato deve intendersi scaduto dal giorno successivo alla data di scadenza riportata sul certificato[3].

È responsabilità dell'organizzazione, garantire a ICIM l'esecuzione dell'audit di rinnovo nel rispetto dei tempi indicati nel presente paragrafo.

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.

[3] Qualora ritardi accumulati nel processo di rinnovo del certificato, per effetto di audit eseguiti nel NON rispetto dei termini temporali indicati nel presente documento, dovessero comportare disguidi tecnici, economici o operativi per l'organizzazione interessata, ICIM si ritiene sollevata da ogni responsabilità a riguardo.

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

8.0 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).

9.0 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.

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