Appendice integrativa – Norma di certificazione: ISO/IEC27001 ed estensione alle linee guida ISO/IEC27xxx

Edizione: marzo 2023

CAPITOLO 1 - GENERALITÀ

Nella presente Appendice sono definite le procedure supplementari e/o sostitutive, applicate da RINA per la certificazione di sistemi gestione per la qualità, rispetto a quanto già definito nel Regolamento generale per la certificazione di sistemi di gestione RC/C 40.

RINA rilascia la certificazione in accordo ai requisiti della norma ISO/IEC 17021-1:2015 ed ISO/IEC 27006:2015/Amd.1:2020 ad Organizzazioni il cui Sistema di Gestione sia stato riconosciuto conforme a tutti i requisiti previsti dalla norma:

ISO/IEC 27001:2022 (UNI CEI EN ISO/IEC 27001:2017)

e fino al 29 aprile 2024, in alternativa, per la norma.

ISO/IEC 27001:2013 (UNI CEI EN ISO/IEC 27001:2017)

La certificazione è integrabile con le linee guida:

ISO/IEC 27017: 2015
ISO/IEC 27018: 2019
ISO/IEC 27701: 2019
ISO/IEC 27035-1:2016, ISO/IEC 27035-2:2016, ISO/IEC27035-3:2020

Dal 30 aprile 2024, tutte le nuove certificazioni ed i rinnovi dovranno essere emesse esclusivamente a fronte della ISO/IEC 27001:2022.

CAPITOLO 2 - NORMA DI RIFERIMENTO / REQUISITI PER LA CERTIFICAZIONE

Oltre a quanto stabilito dal Regolamento generale per la Certificazione dei Sistemi di Gestione, per ottenere la certificazione da parte di RINA, un Sistema di Gestione per la Qualità deve soddisfare inizialmente e nel tempo i requisiti della norma ISO/IEC 27001 con eventuali integrazioni alle linee guida e quelli aggiuntivi previsti dagli Organismi di Accreditamento (es. Circolare tecnica Accredia n. 02/2018 …).

L'estensione alle linee guida deve avvenire a fronte di una certificazione ISO/IEC 27001, in corso di validità, accreditata da un Organismo di Accreditamento che aderisce all'accordo di mutuo riconoscimento IAF/MLA (IAF – International Accreditation Forum/MLA - Multilateral Agreements). Lo scopo della certificazione ISO/IEC 27001 deve essere compatibile con i processi delle Linee Guida di cui si chiede l'integrabilità.

Se l'organizzazione è in possesso della certificazione ISO/IEC 27001 emessa da altro Ente di Certificazione con accreditamento MLA, deve richiedere il trasferimento della certificazione a RINA prima dell'estensione alle Linee Guida come descritto al capitolo 10 del Regolamento generale per la certificazione dei Sistemi di Gestione.

Se l'organizzazione non è in possesso della certificazione ISO/IEC 27001 emessa da altro Ente di Certificazione con accreditamento MLA, deve richiedere a Rina una nuova certificazione.

È ammessa l'estensione della certificazione alla linea guida ISO/IEC 27017:2015 da sola, mentre l'estensione alla linea guida ISO/IEC 27018:2019 deve essere sempre preceduta dall'estensione alla ISO/IEC 27017:2015. È ammessa l'estensione contestuale alle linee guida ISO/IEC 27017:2015 e ISO/IEC 27018:2019.

È ammessa l'estensione della certificazione alle linee guida ISO/IEC 27701:2019 e ISO/IEC 27035 parte 1, 2 e 3 singolarmente.

CAPITOLO 3 - CERTIFICAZIONE INIZIALE

Si applica quanto definito nel Regolamento generale per la certificazione di Sistemi di gestione RC/C 40 a e a quanto previsto dalle "CONDIZIONI GENERALI DI CONTRATTO PER LA CERTIFICAZIONE DI SISTEMI, PRODOTTI E PERSONALE".

In aggiunta si applica quanto segue.

Le Organizzazioni che desiderino ottenere la certificazione del loro Sistema di Gestione della Sicurezza delle Informazione e/o l'estensione alle linee guida devono inviare a RINA oltre al modulo Questionario Informativo anche lo specifico ALLEGATO AL QUESTIONARIO INFORMATIVO PER OFFERTA ISO/IEC 27001 (ISMS) e ISO/IEC 27XXX:20YY, disponibile sul sito www.rina.org, compilato in tutte le sue parti.

In particolare, il Questionario informativo richiede che siano fornite informazioni su:

- Datacenter presso cui sono dislocati i server che gestiscono il servizio / Siti ove sono ubicati asset critici;
- Fattori relativi all'attività svolta e all'organizzazione;
- Fattori relativi all'ambiente IT;
- Fattori che potrebbero determinare riduzioni o incrementi della durata del tempo di audit.

Queste informazioni devono pervenire da un rappresentante autorizzato dell'organizzazione richiedente.

Se il Sistema di Gestione della Sicurezza delle informazioni comprenda documentazione (procedure, registrazioni, ecc.) classificata come "riservata" e/o comunque non disponibile ai fini della certificazione. RINA valuterà la sussistenza delle condizioni per poter proseguire l'iter di certificazione.

L'audit per l'estensione alle linee guida deve essere svolto interamente presso il sito o i siti dell'Organizzazione compresi i data center presso cui è dislocata l'infrastruttura ICT. Nel caso la tipologia di infrastruttura ICT non permettesse di svolgere un audit on site (es. fornitori come AWS, AZURE), dovranno essere verificati gli accordi contrattuali tra l'Organizzazione e i fornitori e gli aspetti di controllo operativo attuati.

I documenti di certificazione possono fare riferimento a norme nazionali e internazionali come fonte/i di controlli per quelli che sono considerati necessari nella Dichiarazione di Applicabilità dell'organizzazione. Il riferimento sui documenti di certificazione deve essere indicativo delle fonte/i di controlli applicati nella Dichiarazione di Applicabilità e non come una certificazione rispetto alle norme stesse.

CAPITOLO 4 - MANTENIMENTO DELLA CERTIFICAZIONE

Si applica quanto definito nel Regolamento generale per la certificazione di Sistemi di gestione RC/C e a quanto previsto dalle "CONDIZIONI GENERALI DI CONTRATTO PER LA CERTIFICAZIONE DI SISTEMI, PRODOTTI E PERSONALE".

CAPITOLO 5 - RICERTIFICAZIONE

Si applica quanto definito nel Regolamento generale per la certificazione di Sistemi di gestione RC/C e a quanto previsto dalle "CONDIZIONI GENERALI DI CONTRATTO PER LA CERTIFICAZIONE DI SISTEMI, PRODOTTI E PERSONALE".

In aggiunta si applica quanto segue.

In occasione dell'audit di ricertificazione del Sistema di Gestione, previsto ogni tre anni, l'Organizzazione deve inviare a RINA oltre al modulo Questionario Informativo anche lo specifico **ALLEGATO AL QUESTIONARIO INFORMATIVO PER OFFERTA ISO/IEC 27001 (ISMS) e ISO/IEC 27XXX:20YY**, disponibile sul sito www.rina.org, compilato in tutte le sue parti come descritto al punto 3 del presente regolamento.

CAPITOLO 6 - ESECUZIONE DEGLI AUDIT

Si applica quanto definito nel Regolamento generale per la certificazione di Sistemi di gestione RC/C e a quanto previsto dalle "CONDIZIONI GENERALI DI CONTRATTO PER LA CERTIFICAZIONE DI SISTEMI, PRODOTTI E PERSONALE".

In aggiunta si applica quanto segue:

L'audit per l'estensione alle linee guida deve essere svolto interamente presso il sito o i siti dell'Organizzazione compresi i data center presso cui è dislocata l'infrastruttura ICT come descritto al punto 3 del presente regolamento.

Il tempo di audit on site non deve essere inferiore al 70% del tempo totale di audit.

CAPITOLO 7 -GESTIONE DEI CERTIFICATI DI CONFORMITA'

Si applica quanto definito nel Regolamento generale per la certificazione di Sistemi di gestione RC/C e a quanto previsto dalle "CONDIZIONI GENERALI DI CONTRATTO PER LA CERTIFICAZIONE DI SISTEMI, PRODOTTI E PERSONALE".

CAPITOLO 8 - MODIFICA DELLA CERTIFICAZIONE E COMUNICAZIONE CAMBIAMENTI

Si applica quanto definito nel Regolamento generale per la certificazione di Sistemi di gestione RC/C e a quanto previsto dalle "CONDIZIONI GENERALI DI CONTRATTO PER LA CERTIFICAZIONE DI SISTEMI, PRODOTTI E PERSONALE".

CAPITOLO 9 - PARTICOLARITA' PER ORGANIZZAZIONI MULTISITO

Si applica quanto definito nel Regolamento generale per la certificazione di Sistemi di gestione RC/C e a quanto previsto dalle "CONDIZIONI GENERALI DI CONTRATTO PER LA CERTIFICAZIONE DI SISTEMI, PRODOTTI E PERSONALE".

In aggiunta si applica quanto segue.

Il campionamento dei siti da sottoporre ad audit può comprende anche i data center presso cui è dislocata l'infrastruttura ICT. Rina valuta l'applicabilità del campionamento oltre ai criteri definiti nel Regolamento generale per la certificazione di Sistemi di gestione anche

- i risultati degli audit interni della sede centrale e dei siti o di precedenti audit di certificazione;
- complessità del Sistema di Gestione;
- complessità dei sistemi IT dei diversi siti;
- potenziale interazione con i sistemi IT critici o con i sistemi IT che gestiscono dati sensibili;
- la valutazione del rischio.

La funzione centrale dell'Organizzazione deve inoltre partecipare alla definizione e gestione della politica di sicurezza, valutazione del rischio, analisi e trattamento, definizione, gestione e analisi dei controlli, definizione e gestione della Dichiarazione di Applicabilità.

CAPITOLO 10 - TRASFERIMENTO DI CERTIFICATI ACCREDITATI

Si applica quanto definito nel Regolamento generale per la certificazione di Sistemi di gestione RC/C e a quanto previsto dalle "CONDIZIONI GENERALI DI CONTRATTO PER LA CERTIFICAZIONE DI SISTEMI, PRODOTTI E PERSONALE".

In aggiunta si applica quanto segue.

Qualora un'Organizzazione con certificazione in corso di validità rilasciata da un altro Organismo di Certificazione di Sistemi di Gestione, accreditato da un Organismo di Accreditamento che aderisce all'accordo di mutuo riconoscimento IAF/MLA, voglia trasferire la propria certificazione a RINA, deve inviare a RINA oltre al modulo Questionario Informativo anche lo specifico **ALLEGATO AL QUESTIONARIO INFORMATIVO PER OFFERTA ISO/IEC 27001 (ISMS) e ISO/IEC 27XXX:20YY**, disponibile sul sito www.rina.org, compilato in tutte le sue parti, come descritto al punto 3.1 del presente regolamento, copia del certificato del Sistema di Gestione e copia del documento Dichiarazione di Applicabilità il cui riferimento è riportato sul certificato.

CAPITOLO 11 - SOSPENSIONE, RIPRISTINO E REVOCA DELLA CERTIFICAZIONE

Si applica quanto definito nel Regolamento generale per la certificazione di Sistemi di gestione RC/C e a quanto previsto dalle "CONDIZIONI GENERALI DI CONTRATTO PER LA CERTIFICAZIONE DI SISTEMI, PRODOTTI E PERSONALE".

CAPITOLO 12 - RINUNCIA ALLA CERTIFICAZIONE

Si applica quanto definito nel Regolamento generale per la certificazione di Sistemi di gestione RC/C e a quanto previsto dalle "CONDIZIONI GENERALI DI CONTRATTO PER LA CERTIFICAZIONE DI SISTEMI, PRODOTTI E PERSONALE".

CAPITOLO 13 - CONDIZIONI CONTRATTUALI

Si applica quanto definito nel Regolamento generale per la certificazione di Sistemi di gestione RC/C e a quanto previsto dalle "CONDIZIONI GENERALI DI CONTRATTO PER LA CERTIFICAZIONE DI SISTEMI, PRODOTTI E PERSONALE".

REGOLAMENTO SPECIFICO PER LA TRANSIZIONE DELLA CERTIFICAZIONE DALLA ISO/IEC 27001: 2013 (UNI CEI EN ISO/IEC 27001:2017) ALLA ISO/IEC 27001: 2022

A.1 – RICHIESTA DI TRANSIZIONE

Durante il periodo di transizione l'Organizzazione già certificata ISO/IEC 27001: 2013 (UNI CEI EN ISO/IEC 27001:2017) può scegliere di effettuare il passaggio alla nuova norma:

1. in concomitanza di un audit di sorveglianza, con un incremento minimo dei tempi di audit di 1 giorno/uomo
2. in concomitanza di un audit di ricertificazione, con un incremento minimo dei tempi di audit di 0,5 giorni/uomo
3. tra due audit programmati con un impegno minimo di 1 giorno/uomo

La richiesta di effettuazione della transizione deve essere inoltrata a RINA da un rappresentante autorizzato dell'organizzazione richiedente.

A.2 – ESECUZIONE DELL'AUDIT DI TRANSIZIONE

L'audit di transizione consiste in un audit on-site per la verifica dell'applicazione dei nuovi requisiti di conformità della ISO/IEC 27001: 2022.

Per le modalità di esecuzione dell'audit si veda quanto stabilito dal Regolamento generale per la certificazione di Sistemi di Gestione.

L'audit di transizione includerà i seguenti elementi:

- la gap analysis della ISO/IEC 27001:2022, nonché la necessità di modifiche al Sistema di Gestione della Sicurezza delle informazioni;
- 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 dall'organizzazione;

Durante il periodo di transizione, qualora si riscontrino non conformità maggiori rispetto alla ISO/IEC 27001: 2022 non risolte entro i termini previsti del Regolamento generale per la certificazione di Sistemi di Gestione, tali non conformità non influenzeranno negativamente il mantenimento della certificazione in corso di validità, purché, ovviamente, venga accertato che il sistema di gestione della sicurezza delle informazioni continui a mantenere la conformità alla ISO/IEC 27001: 2022.

La periodicità e l'estensione dei successivi audit per il mantenimento della certificazione rimangono invariati e seguono quanto previsto dal programma triennale di audit.

A.3 – PARTICOLARITA' PER ORGANIZZAZIONI CON CERTIFICAZIONE INTEGRATA CON LINEE GUIDA ISO/IEC 27XXX:20YY

L'audit di transizione, per le organizzazioni già certificate ISO/IEC 27001: 2013 (UNI CEI EN ISO/IEC 27001:2017) con integrazione alle linee guida elencate al punto 1.2 del presente regolamento, in aggiunta a quanto definito al punto A.2 del presente regolamento, includerà una verifica della Dichiarazione di Applicabilità (SoA) per quanto concerne i controlli specifici definiti nelle linee guida, nuovi o modificati scelti dall'organizzazione.

A.4 – EMISSIONE DEL CERTIFICATO DI CONFORMITA' ALLA ISO/IEC 27001: 2022

A completamento, con esito favorevole, dell'audit di transizione e previa convalida da parte di RINA, è rilasciato un Certificato di Conformità alla nuova edizione della norma la cui validità sarà calcolata in base alla precedente data di decisione per la certificazione/ricertificazione.

A.5 – VALIDITA' DEI CERTIFICATI IN CONFORMITA' ALLA ISO/IEC 27001: 2013 (UNI CEI EN ISO/IEC 27001:2017)

Le certificazioni di conformità ai requisiti della norma certificata ISO/IEC 27001: 2013 (UNI CEI EN ISO/IEC 27001:2017) scadranno il 31 ottobre 2025.

L'Organizzazione che, dopo la data di scadenza del certificato, intenda nuovamente accedere alla certificazione deve presentare una nuova domanda seguendo l'intero iter previsto per la certificazione iniziale.