Appendice integrativa – Norma di certificazione: ISO 37301

Edizione: Aprile 2025

CAPITOLO 1 – GENERALITÀ

Nella presente Appendice sono definite le procedure supplementari e/o sostitutive, applicate da RINA per la certificazione di Sistemi di Gestione della compliance, 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 ad Organizzazioni il cui Sistema di Gestione sia stato riconosciuto conforme a tutti i requisiti previsti dalla norma:

ISO 37301:2021

Oltre a quanto stabilito dal Regolamento generale per la Certificazione dei Sistemi di Gestione RC/C 40, per ottenere la certificazione da parte di RINA, un Sistema di Gestione Anticorruzione deve soddisfare inizialmente e nel tempo i requisiti della norma ISO 37301:2021 e quelli aggiuntivi previsti dagli Organismi di Accreditamento per lo schema ISO 37301.

CAPITOLO 2 - NORMA DI RIFERIMENTO / REQUISITI PER LA CERTIFICAZIONE

La certificazione ISO 37301:2021 viene rilasciata ad un soggetto giuridico nella sua interezza, e a tutti i suoi dipartimenti/filiali, processi e attività realmente svolte.

Deve essere chiarito nel campo di applicazione se l'organizzazione detiene il controllo su altre organizzazioni, specificando le caratteristiche di tale controllo (es. partecipazioni al capitale, vincoli contrattuali, etc.), nel caso in cui queste rientrino nello scopo del certificato.

Non è possibile limitare l'applicazione della norma ad alcuni processi o funzioni, né a specifici siti dell'organizzazione o delle organizzazioni controllate.

È ammissibile che in prima istanza lo scopo di certificazione sia limitato ai processi aziendali coinvolti nella gestione dei rischi di compliance più rilevanti. Tali rischi e processi dovranno essere individuati dall'organizzazione attraverso la valutazione "compliance risk assessment".

Nel caso in cui l'organizzazione richieda, sulla base del compliance risk assessment, di intraprendere un percorso progressivo di certificazione, dovrà presentare il programma di estensione dello scopo di certificazione ai processi aziendali al fine di raggiungere la completa copertura degli ambiti di compliance.

Nell'ambito del/i processo/i individuati, l'organizzazione dovrà però obbligatoriamente includere "tutti" gli ambiti di compliance (es. privacy e protezione dei dati, safety, antiriciclaggio, responsabilità amministrativa, security a altri) attinenti a quel processo

Il Sistema di Gestione della compliance per essere completamente operativo, oltre a quanto stabilito dal Regolamento Generale per la Certificazione di Sistemi di Gestione, deve assicurare che:

- Sia stata determinata la dimensione, struttura e l'autorità decisionale dell'organizzazione
- Siano stati determinati i luoghi ei settori in cui opera l'organizzazione
- Siano stati determinati la natura, la dimensione e la complessità delle attività e delle operazioni dell'organizzazione;
- Sia stato determinato modello di business dell'organizzazione;
- Siano state determinate le parti interessate rilevanti per il sistema di gestione della compliance e i loro requisiti
- Siano stati determinati i soggetti sui quali l'organizzazione ha il controllo e le entità che esercitano il controllo sulla organizzazione;

- Siano stati determinati soci in affari dell'organizzazione;
- Sia stata effettuata una mappatura degli obblighi di compliance che includono i requisiti di natura mandatoria, che un'organizzazione deve rispettare ma anche di natura volontaria, che un'organizzazione sceglie di rispettare.
- Sia stata effettuata la valutazione dei rischi di compliance su tutti i processi e attività
- Siano stati individuati ruoli, responsabilità e autorità per la gestione della compliance, con specifici requisiti e attribuzione di compiti e poteri necessari per supervisionare e assicurare la conformità del sistema di e relazionare al top management sull'effettiva attuazione ed efficacia del sistema stesso;
- Sia stata adottata una Compliance Policy, che possa incoraggiare anche le segnalazioni di sospetti di violazioni e ritorsioni

L'Organizzazione deve disporre di un documento in cui sia determinato lo scopo, considerando quanto previsto dai requisiti 4.1, 4.2, 4.3, 4.4 e 4.5 della Norma ISO 37301:2021 e delle informazioni documentate così come previste dal punto 7.5 della norma di riferimento

Nello stabilire il programma di audit, sono prese in considerazione le dimensioni dell'organizzazione, il campo di applicazione e la complessità del Sistema di Gestione. Al fine della determinazione della classe di complessità si considerano i prodotti e i processi forniti, il livello di efficacia del Sistema di Gestione, il risultato degli audit precedenti o di altri audit già effettuati, oltre che fattori interni ed esterni quali indagini giudiziarie, infortuni, operazioni multinazionali, governance complessa, dimensioni aziendali, settore di attività e requisiti normativi.

CAPITOLO 3 - CERTIFICAZIONE INIZIALE

Oltre a quanto stabilito dal Regolamento generale per la certificazione di Sistemi di Gestione RC/C 40, a integrazione di quanto previsto al punto 3.1 del Regolamento generale per la certificazione dei sistemi di gestione, l'organizzazione deve fornire a RINA informazioni in merito a:

- Obblighi di conformità applicabili all'organizzazione con riferimento alla normativa cogente, normativa volontaria (ISO, linee guida, best practices) disposizioni/clausole contrattuali critiche normativa regolamentare di settore;
- la valutazione degli obblighi di conformità cui sono associati i rischi più rilevanti per tutti i processi/attività;
- il documento di valutazione del rischio "compliance risk assessment" definito dall'organizzazione in conformità a quanto richiesto dalla norma ISO 37301 al par. 4.6;
- il perimetro entro cui è applicato il Sistema di gestione per la compliance, indicando i processi i siti e gli uffici convolti;
- il programma di estensione della certificazione a tutti i processi i siti e gli uffici aziendali coinvolti (ove applicabile);
- l'analisi di contesto;
- la mappatura dei processi (interni ed esterni) e l'elenco delle relative leggi, norme e regolamenti applicabili;
- le relazioni societarie con terzi e i riferimenti legislativi specifici;
- l'indicazione delle imprese terze e la relativa compliance, nonché le modalità di gestione;
- l'analisi degli episodi o minacce di violazione della compliance e le contromisure adottate;
- le registrazioni riguardanti le modalità di gestione delle cause giudiziarie e dei provvedimenti in cui è coinvolta l'organizzazione e, ove applicabile, le evidenze del coinvolgimento e dell'intervento dell'Organismo di Vigilanza.

In riferimento alla documentazione che l'Organizzazione dovrà rendere disponibili a RINA, non si richiede obbligatoriamente la disponibilità del manuale di gestione dell'Organizzazione e l'elenco delle procedure interne. La documentazione di cui sopra è valutata dal RINA per conformità alla norma di riferimento e ai requisiti del presente Regolamento.

CAPITOLO 4 - MANTENIMENTO DELLA CERTIFICAZIONE

Si applica quanto definito nel Regolamento per la certificazione di Sistemi di gestione RC/C 40

CAPITOLO 5 - RICERTIFICAZIONE

Si applica quanto definito nel Regolamento per la certificazione di Sistemi di gestione RC/C 40

CAPITOLO 6 - ESECUZIONE DEGLI AUDIT

Si applica quanto definito nel Regolamento per la certificazione di Sistemi di gestione RC/C 40

CAPITOLO 7 -GESTIONE DEI CERTIFICATI DI CONFORMITA'

Si applica quanto definito nel Regolamento per la certificazione di Sistemi di gestione RC/C 40

CAPITOLO 8 - MODIFICA DELLA CERTIFICAZIONE E COMUNICAZIONE CAMBIAMENTI

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

Oltre a quanto previsto nel Regolamento per la certificazione di Sistemi di gestione RC/C 40 e quanto previsto dalle "CONDIZIONI GENERALI DI CONTRATTO PER LA CERTIFICAZIONE DI SISTEMI, PRODOTTI E PERSONALE", un'organizzazione certificata o in corso di certificazione deve informare tempestivamente e tenere aggiornato RINA nel momento in cui venisse coinvolta in qualche situazione critica tale da compromettere la garanzia della certificazione del sistema (esempio notizie di pubblico interesse che ledono la reputazione dell'impresa, o coinvolgimento in procedimento giudiziario per la violazione della compliance).

Allo stesso modo l'organizzazione dovrà avvisare tempestivamente RINA di qualunque procedimento giudiziario in corso, e delle conseguenti azioni adottate per il contenimento degli effetti di tale evento, quindi dell'analisi delle cause radice e delle relative azioni correttive.

L'informativa è dovuta anche se le vicende dovessero coinvolgere figure apicali per altri ambiti o siti/processi non certificati.

RINA, a fronte di tali segnalazioni, provenienti direttamente dall'organizzazione o da altre fonti, effettuerà i necessari accertamenti e approfondimenti specifici e potrà adottare i provvedimenti del caso tra cui: archiviazione della segnalazione, sanzioni, rafforzamento dell'attività ispettiva, definiti in funzione dell'adeguatezza della risposta e strategie adottate dall'organizzazione.

CAPITOLO 9 - PARTICOLARITA' PER ORGANIZZAZIONI MULTISITO

Oltre a quanto stabilito dal Regolamento generale per la certificazione di Sistemi di Gestione RC/C 40, laddove in un sito dell'organizzazione siano gestiti dei rischi significativi alla luce dalla valutazione dei rischi di compliance, il governo di tali rischi dovrà essere valutato in sede di certificazione iniziale e nelle successive sorveglianze sulla base del campionamento individuato nel piano triennale.

CAPITOLO 10 - TRASFERIMENTO DI CERTIFICATI ACCREDITATI

Si applica quanto definito nel Regolamento per la certificazione di Sistemi di gestione RC/C 40

CAPITOLO 11 - SOSPENSIONE, RIPRISTINO E REVOCA DELLA CERTIFICAZIONE

Si applica quanto definito nel Regolamento per la certificazione di Sistemi di gestione RC/C 40 e 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 per la certificazione di Sistemi di gestione RC/C 40

CAPITOLO 13 - CONDIZIONI CONTRATTUALI

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