REGOLAMENTO PARTICOLARE PER LA CERTIFICAZIONE DEI SISTEMI DI GESTIONE PER LA CONTINUITA' OPERATIVA RSCO

Valido dal 2017-08-29

Italia

INDICE

Descrizione della revisione	Recepimento requisiti di ISO/IEC 17021-1:2015 e ISO/IEC TS 17021-6:2014. Revisione a seguito modifiche organizzative TÜV Italia.

	Reparto	Data	Nome	Firma
Preparazione :	CTSSI	2017-07-10	Danilo Diomede	*Documento privo di firme in quanto approvato nel sistema di gestione digitale di TÜV Italia Srl*
Verifica :	RQMS	2017-08-29	Sara Brandimarti	
Verifica :	UMRS	2017-08-29	Stefano Parini	
Approvazione :	MDMS	2017-08-29	Andrea Coscia	

1. Scopo ed entrata in vigore

Scopo di questo documento è integrare il Regolamento Generale per la Certificazione dei Sistemi di Gestione (RGSG) adottato da TÜV Italia s.r.l. (nel seguito denominata TÜV Italia), ai fini specifici della certificazione dei sistemi di gestione per la Continuità operativa (SGCO o, in modo del tutto equivalente in inglese, BCMS).
Il presente regolamento entra in vigore nella data riportata in intestazione.

2. Campo di applicazione

Questo regolamento si applica alle attività di certificazione di sistemi di gestione per la continuità operativa (SGCO) svolte sia sotto accreditamento ACCREDIA, che fuori dall'accreditamento.
Esso non pregiudica l'applicabilità di altri regolamenti inerenti ulteriori schemi certificativi per cui l'organizzazione risulti certificata da TÜV Italia e/o da altri Organismi di Certificazione.

Le normative applicabili come riferimento per gli SGCO sono:

- la norma UNI EN ISO 22301:2014 "Sicurezza della società - Sistemi di gestione della continuità operativa – Requisiti", edizione nazionale della norma ISO 22301:2012.
- la norma UNI EN ISO 22313:2015 "Sicurezza della società - Sistemi di gestione della continuità operativa – Linee guida", edizione nazionale della norma ISO 22313:2012.
- La norma nazionale UNI CEI EN ISO/IEC 17021-1:2015 "Valutazione della conformità - Requisiti per gli organismi che forniscono audit e certificazione di sistemi di gestione"
- La norma nazionale UNI CEI ISO/IEC TS 17021-6:2015 "Valutazione della conformità - Requisiti di competenza per le attività di audit e la certificazione di sistemi di gestione della continuità operativa"

Inoltre sono riferimento obbligatorio per l'accreditamento i documenti emessi da ACCREDIA e reperibili nel sito www.accredia.it :

- Regolamento per l'accreditamento degli Organismi di certificazione ed ispezione RG-01
- Regolamento per l'accreditamento degli Organismi di certificazione del sistema di gestione RG-01-01
- Circolare n. 01/15 del 19/01/2015 (DC2015SSV021)
- Eventuali Regolamenti Tecnici

Per avere un riscontro puntuale delle attività svolte sotto accreditamento ACCREDIA, si può consultare direttamente il sito www.accredia.it oppure il sito www.tuv.it dove è possibile prendere visione dei certificati di accreditamento con i relativi allegati, inerenti ai settore coperti dall'accreditamento medesimo.

3. Termini e definizioni

La terminologia utilizzata nel presente regolamento è in accordo alle seguenti norme:

- ISO 22300:2012 "Societal security — Terminology"
- UNI EN ISO 9000:2015 "Sistemi di gestione per la qualità – Fondamenti e terminologia";
- UNI CEI EN 45020:2007: "Normazione ed attività connesse – Vocabolario generale".
- ISO/IEC 17000:2004 "Conformity assessment- Vocabulary and general principles

Gli acronimi impiegati nel testo del presente regolamento particolare sono:

- SGCO (Sistema di Gestione per la Continuità Operativa), equivalente a BCMS (Business Continuity Management System)
- BCP (Business Continuity Plan), in italiano "Piano di continuità operativa"

- BIA (Business Impact Analysis), in italiano "Analisi dell'impatto sul business"

Per la definizione di:
- Carenza (CA)
- Nonconformità (NC)
- Osservazione (OSS):
- Commento (COM)

si veda il Regolamento generale RGSG.

4. Responsabilità

Vale quanto riportato nel Regolamento Generale RGSG, par. 4.

5. Controllo del regolamento

Il presente regolamento particolare è a disposizione degli interessati sul sito internet www.tuv.it .
In ogni caso le organizzazioni possono richiederne copia in formato cartaceo o digitale.

Inoltre vale quanto riportato nel Regolamento Generale RGSG, par. 5.

6. Iter di certificazione

6.1 Generalità

Vale quanto riportato nel Regolamento Generale RGSG, par. 6.1, con le seguenti integrazioni:

- La Norma riporta nelle sezioni da 4 a 10 una serie di requisiti obbligatori per gli SGCO, che non possono essere cioè oggetto di esclusione.
- Da quanto sopra deriva che TÜV Italia, quale organismo di certificazione degli SGCO, ha il compito di valutare la documentazione ed attuazione di tutti i requisiti delle sezioni da 4 a 10; TÜV Italia si riserva la facoltà di giudicare l'adeguatezza delle scelte operate dall'organizzazione
- Nell'esecuzione delle proprie verifiche TÜV Italia esamina inoltre l'esistenza e la congruenza dei collegamenti tra i diversi elementi del SGCO quali: la politica, gli obiettivi generali e di dettaglio, i risultati della analisi di impatto sul business e della valutazione dei rischi, le strategie di trattamento dei rischi, le responsabilità, i programmi formativi e di comunicazione, le procedure, i test di attuazione dei BCP, ecc.
- Per quanto concerne il rispetto dei requisiti cogenti (per disposizione di leggi, regolamenti, direttive, ecc.), il principio generale è che il mantenimento e la valutazione della conformità ai suddetti requisiti cogenti ricadono sotto la responsabilità dell'organizzazione che gestisce il SGCO e che ne rilascia apposita attestazione a TÜV Italia (attraverso il modulo RL fornito dal responsabile del team di audit); TÜV Italia si limita ad eseguire verifiche a campione per acquisire fiducia che il SGCO sia efficace sotto questo punto di vista e che – nell'eventualità di non conformità rispetto ai requisiti cogenti – l'organizzazione metta in atto idonee azioni correttive.
- Può accadere che l'organizzazione gestisca processi produttivi e/o di servizio che ricadono sotto il controllo di un unico SGCO, ma che sono distribuiti in luoghi geografici diversi, ossia in più siti; in tale situazione TÜV Italia può emettere un unico certificato, ma si riserva la decisione di verificare ogni singolo sito, oppure di campionarne alcuni e verificare solo questi (TÜV Italia prende tale decisione sulla base delle apposite prescrizioni e raccomandazioni del documento IAF MD1 e ISO/IEC 17021 in edizione vigente, nonché dei Regolamenti emessi da ACCREDIA).

6.2 Modalità di svolgimento degli audit e programma di audit

Vale quanto riportato nel Regolamento Generale RGSG, par. 6.2, con le seguenti integrazioni:

L'organizzazione, all'atto della richiesta di certificazione, è tenuta a comunicare se intende avvalersi della facoltà di negare al team di audit l'accesso a documenti che contengano informazioni considerate riservate o sensibili (per esempio informazioni relative al personale, ai clienti, ai fornitori, alle strategie di continuità operativa); in tale caso il TÜV Italia valuterà se le informazioni cui può avere accesso sono sufficienti ai fini della valutazione del SGCO; qualora non lo fossero, l'organizzazione ed il TÜV Italia devono raggiungere – ove possibile – un accordo sulle modalità di accesso a tutte le informazioni indispensabili per la valutazione del SGCO; se l'accordo viene raggiunto, l'iter di certificazione non non può essere iniziato. Detto accordo può consistere nel fatto che l'organizzazione autorizzi il team di audit ad accedere ad informazioni, riservate o sensibili, solo per il tempo dell'audit e in base a modalità concordate.

In caso di di sistemi di gestione multipli (riferiti cioè a più di una norma certificabile), l'audit può essere eseguito e condurre al rilascio della certificazione, purché tutti i requisiti della norma di riferimento per gli SGCO siano stati soddisfatti, ed inoltre tutte le informazioni documentate siano disponibili, conformi ai requisiti citati, e siano identificate le interfacce con gli altri sistemi di gestione.

6.3 Avvio dell'iter di certificazione

Vale quanto riportato nel Regolamento Generale RGSG, par. 6.3

6.4 Visita preliminare (preaudit)

Vale quanto riportato nel Regolamento Generale RGSG, par. 6.4.

6.5 Audit di 1° Stadio (Esame iniziale della documentazione + visita iniziale)

Vale quanto riportato nel Regolamento Generale RGSG, par. 6.5, con le seguenti integrazioni:

L'audit di 1° stadio sarà eseguito interamente presso l'Organizzazione.

a) Verifica della documentazione del SGCO (1° fase del 1° stadio)

La verifica della documentazione del SGCO viene eseguita sempre, con le eventuali limitazioni dovute ai motivi di cui al paragrafo 6.2.

Per documentazione del SGCO si intende quanto segue:

- i documenti individuati dalla Norma col termine "documented information"
- l'elenco dei requisiti cogenti applicabili nell'ambito del SGCO, integrato dall'attestazione scritta del rispetto di tali requisiti rilasciata dall'organizzazione (su modulo RL).

Tra i documenti specificati nella norma e soggetti a verifica documentale vi sono, in particolare, i documenti relativi alla BIA, alla valutazione del rischio, alla policy di continuità operativa ed agli obiettivi correlati, alle procedure documentate per la continuità operativa.

Si sottolinea inoltre che nei suddetti documenti deve essere chiaramente riportato il campo di applicazione del SGCO, nonché il suo perimetro. Eventuali interfacce / interazioni con servizi o attività non incluse nel campo di applicazione devono essere individuate e comprese nella valutazione dei rischi (per esempio questo potrebbe essere il caso del processo logistico correlato alla produzione industriale di beni).

L'esame della documentazione è volto ad accertare che essa sia innanzitutto completa, ossia soddisfi tutti i requisiti della Norma e del presente regolamento; inoltre la documentazione deve

essere chiara, ossia non deve lasciare adito a dubbi interpretativi, deve essere congruente tra le sue varie parti e deve essere facilmente leggibile.

b) Visita iniziale (2° fase del 1° stadio)
La visita iniziale viene eseguita sempre e consiste in una verifica in campo presso il sito (o se necessario anche i siti) dell'organizzazione.
Essa consente a TÜV Italia di meglio comprendere:
- la dimensione e le caratteristiche del SGCO dell'organizzazione;
- il suo grado di idoneità ad affrontare l'iter di certificazione;
- l'applicabilità di norme e requisiti legislativi relativi alla continuità operativa;
- il tipo di esperienza richiesta al team incaricato dell'audit di 2° stadio;
- l'entità delle risorse necessarie per svolgere l'audit di 2° stadio.

Inoltre la visita iniziale consente all'organizzazione di approfondire i seguenti aspetti (qualora non già risolti ad esempio in occasione dell'eventuale preaudit di cui al par. 6.4):
- dettagli dell'iter di certificazione;
- programmazione più precisa dei tempi necessari per giungere alla certificazione;
- definizione esatta del campo di applicazione del SGCO;
- identificazione di eventuali carenze nella attuazione del SGCO.

L'esito dell'esame della documentazione è riportato, assieme ai risultati della visita iniziale, in un apposito rapporto, emesso a conclusione dell'audit di 1° stadio. Copia del rapporto viene consegnata anche all'organizzazione; se necessario, esso può essere illustrato al cliente in occasione di un incontro diretto col cliente stesso. Qualora l'attuazione del SGCO risulti carente, il cliente ne viene informato tramite il suddetto rapporto, che elenca le carenze da sanare prima dell'esecuzione del 2° stadio.
Inoltre, qualora emergano scostamenti rispetto a quanto comunicato dall'organizzazione in sede di formulazione offerta, TÜV Italia si riserva di valutare la necessità di modificare la propria offerta economica.

6.6 Audit di 2° Stadio (per la verifica iniziale del sistema di gestione o audit per la certificazione)

Vale quanto descritto nel Regolamento Generale RGSG, par. 6.6, con le seguenti integrazioni:

Al momento dell'audit di stadio 2 il SGCO dell'organizzazione deve risultare già operativo; in particolare l'organizzazione deve aver definito obiettivi per la continuità operativa misurabili e – ove applicabile - quantificati, deve aver eseguito almeno un riesame della direzione documentato ed un ciclo completo di audit interni secondo i requisiti della sezione 9 della Norma e, infine, deve rispettare le prescrizioni dei paragrafi 8 e 11 del presente regolamento.

L'audit viene effettuato sulla base di un piano di audit concepito in modo da tenere conto dell'esito delle attività già svolte (audit di 1° stadio), dando rilevanza agli elementi del SGCO risultati più significativi (BIA, valutazione dei rischi per la continuità operativa e relativa consistenza dei risultati; definizione degli scenari interruttivi e dei piani di continuità operativa; predisposizione ed attuazione di strategie e processi per la formazione, comunicazione, allertamento e la risposta agli eventi interruttivi; riesame dell'efficacia del sistema SGCO e misura dell'efficacia dei processi di risposta agli incidenti, di continuità operativa e di ripristino dell'operatività, etc.); pertanto il piano comprende, in linea di principio, tutti i requisiti della norma di riferimento, ma può anche non includere quei requisiti che sono risultati attuati in modo completamente soddisfacente nel corso dell'audit di 1° stadio.
Tale piano viene anticipato all'organizzazione almeno una settimana prima dell'audit.
L'audit per la certificazione ha lo scopo di accertare che il SGCO sia messo in pratica in accordo alla relativa documentazione (policy ed obiettivi, BIA, valutazione del rischio, organizzazione e procedure di incident response, di business continuity e di recovery, requisiti di legge, eventuali altri

requisiti cogenti, programmi, ecc.) e in maniera efficace, e soddisfi quindi i requisiti della norma di riferimento.
Inoltre il team di audit ha l'obiettivo di verificare che:

- l'analisi dell'impatto sui processi di eventi interruttivi sia adeguata ai processi dell'organizzazione ed alla loro criticità sul piano giuridico;
- l'organizzazione abbia stabilito adeguate procedure per l'identificazione, l'esame e la valutazione dei rischi per la continuità operativa, e che l'applicazione delle strategie per il suo perseguimento sia coerente e congrua con la politica, con gli obiettivi ed i target definiti dall'organizzazione stessa;
- le misurazioni di efficacia dei controlli siano consistenti.

6.7 Emissione iniziale della certificazione e successivi rinnovi

Vale quanto descritto nel Regolamento Generale RGSG, par. 6.7.

6.8 Audit di sorveglianza

Vale quanto descritto nel Regolamento Generale RGSG, par. 6.8, con le seguenti integrazioni:

Al momento di tale audit il SGCO dell'organizzazione deve dare evidenza dell'esecuzione del riesame della direzione e di un ciclo di audit interni secondo i requisiti della sezione 9 della Norma con una frequenza almeno annuale.

Inoltre come minimo, oltre a quanto stabilito nel RGSG, l'audit di sorveglianza ha l'obiettivo di riesaminare :

- l'efficacia del SGCO con riferimento al raggiungimento degli obiettivi stabiliti nella politica per la continuità operativa;
- il funzionamento delle procedure per la valutazione periodica della conformità legislativa e normativa;
- l'esecuzione di test dei Piani di Continuità Operativa
- le azioni intraprese a fronte di situazioni non conformi rilevate nel precedente audit;
- la gestione di reclami proposti dalle parti interessate all'attenzione di TÜV Italia;
- eventuali cambiamenti nella definizione degli scenari di continuità operativa alla base dei Piani di Continuità Operativa;
- il programma di audit in funzione delle modifiche intervenute (inclusi elementi di contesto, rischi, aspetti legislativi, richieste o segnalazioni dalle parti interessate);
- l'uso appropriato del certificato.

6.9 Audit di rinnovo

Vale quanto descritto nel Regolamento Generale RGSG, par. 6.9.

Inoltre, al momento di tale audit il SGCO dell'organizzazione deve dare evidenza dell'esecuzione del riesame della direzione e di un ciclo di audit interni secondo i requisiti della sezione 9 della Norma.

6.10 Audit speciali o audit non programmati o eventuale riduzione del campo di applicazione della certificazione

Vale quanto descritto nel Regolamento Generale RGSG, par. 6.10.

6.10.1 Eventuale riduzione del campo di applicazione della certificazione

TÜV Italia ha il diritto di ridurre il campo di applicazione della certificazione per escludere le parti che non soddisfano i requisiti, qualora l'organizzazione abbia mancato, in modo persistente o grave di rispettare i requisiti della certificazione relativamente a quelle parti di campo di applicazione della certificazione.Tale riduzione sarà congruente con i requisiti della norma utilizzata per la certificazione.

7. Registro delle organizzazioni certificate

Vale quanto descritto nel Regolamento Generale RGSG, par. 7.

8. Modalità di riferimento alla certificazione. Uso del certificato e del marchio

Vale quanto descritto nel Regolamento Generale RGSG, par. 8.

Per i sistemi di gestione certificati solo in accordo in accordo alla Norma, il marchio applicabile, salvo aggiornamenti, è il seguente:

Nota: nel caso di ulteriori certificazioni di sistema di gestione ottenute con TÜV Italia potrà essere inviato – se disponibile - un marchio specifico che faccia riferimento anche agli altri schemi per i quali si è conseguita la certificazione.

9. Sospensione della certificazione

Vale quanto descritto nel Regolamento Generale RGSG, par. 9.

10. Ritiro / annullamento della certificazione

Vale quanto descritto nel Regolamento Generale RGSG, par. 10.

11. Gestione dei reclami e delle segnalazioni da parte delle organizzazioni clienti e dalle parti interessate

Vale quanto descritto nel Regolamento Generale RGSG, par. 11.

Inoltre nello specifico l'organizzazione dovrà evidenziare nella propria procedura di gestione dei reclami le modalità operative relative a:

- Eventuali comunicazioni alle autorità, se richiesto dall'ambito regolamentato.
- Rivalutazione dell'impatto sul business e del relativo livello di rischio.
- Valutazione delle interazioni con altri elementi del SGCO

12. Documentazione o informazioni documentate del sistema di gestione e relativa accessibilità per le verifiche di TÜV Italia srl

Vale quanto descritto nel Regolamento Generale RGSG, par. 12.

Inoltre si sottolinea che qualora le informazioni contenute nella documentazione di sistema e nei rapporti di verifica siano tali da non poter essere distribuite in forma controllata a TÜV Italia o a soggetti terzi, l'organizzazione è tenuta a comunicare formalmente a TÜV Italia le motivazioni per cui non è possibile effettuare tale distribuzione controllata.

13. Modifiche al sistema di gestione

Vale quanto descritto nel Regolamento Generale RGSG, par. 13.

14. Modifiche alle regole del sistema di certificazione

Vale quanto descritto nel Regolamento Generale RGSG, par. 14.

15. Prescrizioni particolari per organizzazioni già certificate da altro organismo

Vale quanto descritto nel Regolamento Generale RGSG, par. 15.

Inoltre, considerato che gli accordi di mutuo riconoscimento IAF MLA non riguardano lo schema ISO 22301, per valutare la fattibilità tecnica e prima di procedere con l'iter di certificazione sarà necessario verificare l'esistenza di accordi bilaterali fra Accredia e l'ente di accreditamento sotto il quale è stata certificata l'organizzazione richiedente.

16. Riservatezza

Vale quanto descritto nel Regolamento Generale RGSG, par. 16.

17. Ricorsi (o Appelli)

Vale quanto descritto nel Regolamento Generale RGSG, par. 17.

18. Reclami nei confronti di TÜV Italia

Vale quanto descritto nel Regolamento Generale RGSG, par. 18.

19. Contenziosi

Vale quanto descritto nel Regolamento Generale RGSG, par. 19.

20. Condizioni economiche

Vale quanto descritto nel Regolamento Generale RGSG, par. 20.