REGOLAMENTO TECNICO PER LA CERTIFICAZIONE DI BUSINESS CONTINUITY MANAGEMENT SYSTEM

INDICE

1.GENERALITA'

Il presente documento descrive le procedure applicate da Dasa-Rägister per la Certificazione di Business Continuity Management System (BCM) ed è da considerarsi complementare, e quindi non sostitutivo, a quanto definito nel "Regolamento Contrattuale per la Certificazione di Sistemi di Gestione".

L'Organizzazione richiedente la Certificazione deve:

a) stabilire, documentare, attuare e mantenere un efficace Sistema di Gestione e aggiornarlo quando necessario in conformità ai requisiti della norma di riferimento
b) definire lo scopo e il campo di applicazione del Sistema di Gestione specificando i servizi ed i siti ai quali è indirizzato il Sistema di Gestione
c) assicurare che i pericoli che ci si può ragionevolmente aspettare che accadano in relazione ai servizi compresi nel campo di applicazione del sistema siano identificati, valutati e controllati;
d) identificare e documentare il controllo di eventuali processi affidati all'esterno che hanno effetti sulla conformità dei servizi
e) mantenere a disposizione di Dasa-Rägister le registrazioni di tutti i reclami ricevuti e delle relative azioni conseguenti
f) mantenere aggiornata la raccolta delle norme, leggi e regolamenti cogenti applicabili alle attività, processi, servizi inclusi nel campo di applicazione della Certificazione.

Il Certificato è emesso a fronte del completamento, con esito positivo, della Verifica Iniziale (Initial Audit), la sua validità è subordinata al superamento delle Verifiche di Sorveglianza periodiche (Surveillance Audit) e ad una completa rivalutazione (Re-Audit) entro il termine della scadenza.

Qualora la richiesta di Certificazione provenga da Organizzazioni già certificate da enti accreditati e con Certificato in corso di validità, Dasa-Rägister subentra nelle attività in accordo con la pianificazione del precedente ente, recependo eventuali rilievi ed effettuando il relativo Audit secondo le modalità previste dal presente regolamento.

Prima dell'esecuzione di ogni Audit, Dasa-Rägister comunica all'Organizzazione l'Audit Team che condurrà la valutazione e l'eventuale documentazione che dovrà essere resa disponibile.

Per ogni Audit sono previste:

- una riunione iniziale tra l'Audit Team e l'Organizzazione finalizzata alla presentazione delle parti e all'illustrazione delle procedure di verifica
- la verifica, in campo e a campione, della conformità ai requisiti della norma di riferimento e della presa in carico delle prescrizioni legali riferibili al campo di applicazione della Certificazione
- la redazione del rapporto finale (Audit Report) con i risultati e le conclusioni della verifica e l'eventuale pianificazione delle attività successive
- una riunione finale tra l'Audit Team e l'Organizzazione per illustrare l'esito della verifica e consegnare l'Audit Report. In questa fase l'Organizzazione può sollevare e formalizzare eventuali riserve.

In occasione di ogni audit (iniziale, sorveglianza e rinnovo), saranno valutati i seguenti aspetti:

- la completezza e correttezza dello scopo di certificazione;
- l'aggiornamento della valutazione dei rischi generale e, in particolare, quella dellabusiness impact analisys (BIA);
- che la valutazione dei rischi e la BIA abbiano un senso per le parti interessate, che le misure predisposte dall'organizzazione, per rispondere agli scenari di rischio, siano coerenti con tali valutazioni e che, in particolare, sia stata stabilita la tolleranza al rischio per i processi oggetto della gestione della continuità operativa;
- che tali valutazioni tengano conto anche delle prestazioni, affidabilità ed esposizione a rischi specifici dei fornitori e che, laddove applicabile, sia stata effettuata una specifica valutazione per i servizi dati in "outsourcing";
- l'adeguatezza dell'addestramento delle risorse umane e delle relative esercitazioni, con riferimento alla copertura degli scenari interruttivi individuati dall'analisi di impatto sul business;
- che il sistema di gestione per la continuità operativa garantisca che l'organizzazione sia in grado di conoscere, gestire come documenti di origine esterna e rispettare le pertinenti disposizioni di legge, comprendendo quali siano gli obblighi e le opportunità disponibili;
- che le scelte dell'organizzazione sui comportamenti da adottare in relazione alla continuità operativa siano congruenti, almeno, con le disposizioni di legge applicabili.

Qualora l'Organizzazione affidi all'esterno alcuni processi e questi possano avere un'influenza diretta sulla conformità dei prodotti/processi oggetto di certificazione, Dasa-Rägister si riserva il diritto, a suo insindacabile giudizio, di eseguire audit presso i fornitori di tali processi.

2. PRE-AUDIT

Prima della Verifica Iniziale è possibile effettuare un Audit preliminare (Pre-Audit) con lo scopo di individuare il grado di preparazione dell'Organizzazione in relazione ai requisiti della norma e di identificare quelle situazioni che potrebbero compromettere il buon esito dell'Initial Audit.

Può essere condotto un solo Pre-Audit per ogni Richiesta di Certificazione avente una durata proporzionale alle dimensioni dell'Organizzazione.

3. VERIFICA INIZIALE (INITAL AUDIT)

L'Initial Audit è suddiviso in due momenti di valutazione la cui durata ed estensione dipendono dalle dimensioni e dalle caratteristiche dell'Organizzazione nonché dalla presenza di eventuali sedi secondarie o altri siti da verificare (così come previsto dai requisiti degli enti di accreditamento):

a) Stage 1 Audit finalizzato alla verifica della documentazione e della pianificazione del Sistema di Gestione nonché alla programmazione dello Stage 2
b) Stage 2 Audit avente come scopo la valutazione dell'adeguatezza e conformità del Sistema di Gestione dei servizi

Lo Stage 2 può essere effettuato solo dopo il completamento dello Stage 1 e deve aver luogo entro e non oltre nove mesi dalla prima verifica altrimenti questa deve essere ripetuta.

3.1. STAGE 1 AUDIT

Lo Stage 1 Audit viene effettuato presso la sede dell'Organizzazione e prevede le seguenti finalità:

a) valutare la documentazione del Sistema di Gestione;
b) valutare il sito dell'Organizzazione e le specifiche condizioni dei luoghi presso cui è svolta l'attività oggetto di certificazione;
c) scambiare informazioni con il personale al fine di stabilire il grado di preparazione per lo Stage 2 Audit
d) verificare il livello di implementazione del Sistema di Gestione;
e) identificare il campo di applicazione del Sistema di Gestione e i siti dell'Organizzazione a cui esso è applicabile;
f) valutare l'esigenza di eseguire audit presso eventuali outsourcer dell'Organizzazione, qualora i processi a questi affidati possano influenzare significativamente la conformità del prodotto/servizio dell'Organizzazione;
g) riesaminare l'assegnazione di risorse e concordare con l'Organizzazione i dettagli dello Stage 2 Audit.

Le risultanze dello Stage 1 Audit saranno documentate nell'Audit Report e comunicate all'Organizzazione dall'Audit Team, compresa l'identificazione di ogni rilievo che nello Stage 2 Audit potrebbe essere classificato come Non Conformità.

3.2. STAGE 2 AUDIT

Lo Stage 2 Audit è normalmente programmato in un secondo momento rispetto allo Stage 1 Audit. Qualora le condizioni lo consentano (assenza di rilievi ostativi, adeguatezza dei tempi già pianificati, ragionevole fiducia sullo stato di implementazione del Sistema di Gestione), gli Audit possono essere uno conseguente all'altro.

Durante lo Stage 2 Audit, oltre a quanto specificato al §1, è prevista la valutazione di:

a) risoluzione dei rilievi emersi in Stage 1;
b) Sistema di Gestione e le sue prestazioni, anche con riferimento al rispetto delle prescrizioni legali;
c) informazioni ed evidenze circa la conformità a tutti i requisiti della norma o di altro documento normativo applicabile al Sistema di Gestione;
d) monitoraggio, la misurazione, la rendicontazione e il riesame delle prestazioni, con riferimento agli obiettivi e ai traguardi definiti;
e) modalità di gestione e tenuta sotto controllo dei processi;
f) audit interni ed il riesame della direzione.

Eventuali Non Conformità che dovessero emergere al termine dello Stage 2 Audit devono essere prese in carico dall'Organizzazione e la loro gestione comunicata a Dasa-Rägister (tramite le modalità indicate nell'Audit Report). Quest'ultimo deve essere approvato dal Lead Auditor prima di proseguire con le successive fasi del processo di Certificazione.

In caso di Non Conformità Maggiori è necessario verificare l'efficacia del trattamento, che deve avvenire entro sei mesi dalla data dello Stage 2 Audit altrimenti quest'ultimo deve essere ripetuto. La valutazione può avvenire su base documentale o tramite un Follow-Up Audit (§ 5). In assenza di tale verifica non è possibile proseguire con la fase di Delibera.

3.3. RILASCIO DELLA CERTIFICAZIONE

La Certificazione viene rilasciata a seguito del parere positivo del Comitato di Delibera (Decision Committee) che valuta i documenti relativi all'Audit e prendendo anche in considerazione eventuali informazioni inerenti l'Organizzazione raccolte dal mercato o comunque di pubblico dominio.

In questa fase il Comitato di Delibera:

- può richiedere all'Organizzazione di fornire eventuali informazioni mancanti;
- può disporre un Follow-Up Audit o documentale per integrare eventuali mancanze della verifica.

Il parere positivo del Comitato di Delibera consente:

- l'emissione del Certificato la cui validità è triennale e decorre dalla data della Delibera;
- l'iscrizione e la pubblicazione dei dati dell'Organizzazione nel Registro Certificazioni.

Il Comitato di Delibera può anche disporre Surveillance Audit ad intervalli più frequenti (ad esempio semestrali) a seguito di:

- proposta dell'Audit Team o esito della verifica tale per cui sia necessario monitorare il Sistema di Gestione con frequenza maggiore rispetto all'anno;
- specifica richiesta dell'Organizzazione.

In caso di non concessione della Certificazione, le ragioni di tale decisione vengono comunicate formalmente all'Organizzazione, precisando gli scostamenti rispetto ai requisiti richiesti che la stessa si deve impegnare a correggere entro un termine di tempo proposto e accettato da Dasa-Rägister. Tale termine non deve in ogni caso essere superiore a sei mesi, superati i quali deve essere ripetuto l'intero Initial Audit.

4. VERIFICHE DI SORVEGLIANZA (SURVEILLANCE AUDIT)

Dopo l'Initial Audit, e con le stesse modalità, al fine di accertare il continuo rispetto di quanto stabilito dalla normativa di riferimento, viene periodicamente effettuato un Surveillance Audit che consiste in una verifica dell'Organizzazione relativamente ad alcuni aspetti del Sistema di Gestione identificati nel Programma delle Sorveglianze lasciato all'Organizzazione al termine della Verifica Iniziale (le Sorveglianze garantiscono, comunque, che l'equivalente di una valutazione completa del Sistema di Gestione sia portata a termine nell'arco di tre anni). La verifica può, in ogni caso, essere condotta anche su altri punti a discrezione del Lead Auditor.

Eventuali Non Conformità segnalate all'Organizzazione dovranno essere prese in carico da quest'ultima. L'efficacia del trattamento e delle eventuali Azioni Correttive viene verificata nel corso del successivo Audit di Sorveglianza salvo i casi in cui, in funzione della gravità e complessità, si ritenga necessaria una verifica supplementare (Follow-Up Audit – § 5).

Per le Non Conformità Maggiori viene concesso all'Organizzazione un tempo massimo di sei mesi entro il quale Dasa-Rägister dovrà effettuare un Follow-Up Audit al fine di verificare l'efficacia dei trattamenti. Qualora questo non abbia luogo nei tempi previsti, la Certificazione verrà sospesa per un periodo massimo di sei mesi trascorsi i quali la Sospensione si trasformerà in Revoca.

La documentazione prodotta durante gli Audit di Sorveglianza viene sottoposta al Comitato di Delibera nei seguenti casi:

- siano state rilevate Non Conformità Maggiori;
- sia stato modificato il programma di Certificazione (per esempio, riduzioni, estensioni...);
- su esplicita richiesta dell'Audit Team, che può segnalare quelle situazioni che possono avere influenza sulla validità del Certificato.

I Surveillance Audit hanno, quantomeno, cadenza annuale e la prima verifica deve essere effettuata entro i dodici mesi dalla data della Verifica Iniziale.

5. VERIFICA SUPPLEMENTARE (FOLLOW-UP AUDIT)

Il Follow-Up Audit ha come oggetto la valutazione di aspetti specifici, in relazione all'obiettivo per cui è stato disposto. La valutazione può, comunque, essere condotta anche su altri punti a discrezione del Lead Auditor.

Il Follw-Up Audit, in funzione degli aspetti da valutare, può consistere:

- in una verifica documentale, qualora la valutazione possa essere effettuata attraverso l'analisi di idonei documenti forniti dall'Organizzazione a Dasa-Rägister;
- in una verifica in campo, svolta con le stesse modalità degli altri audit, qualora gli aspetti da valutare richiedano un sopralluogo presso l'Organizzazione.

Qualora il Follow-Up Audit per la verifica dell'efficacia del trattamento delle Non Conformità Maggiori abbia esito negativo, la Certificazione verrà sospesa fino a che non sia stata valutata l'efficacia del nuovo trattamento e, comunque, per un periodo massimo di sei mesi, trascorsi i quali la Sospensione si trasformerà in Revoca.

6. RIESAME DEL SISTEMA DI GESTIONE (RE-AUDIT)

La validità del Certificato è confermata a seguito dell'esito positivo di una verifica completa (Re-Audit) condotta con gli stessi criteri della Verifica Iniziale.

Eventuali Non Conformità segnalate all'Organizzazione dovranno essere prese in carico da quest'ultima. Per le Minori l'efficacia del trattamento e delle eventuali Azioni Correttive viene verificata nel corso del successivo Surveillance Audit salvo i casi in cui, in funzione della gravità e complessità, si ritenga necessaria:

a) una verifica documentale supplementare (Follow-Up documentale) con l'invio di documenti da parte dell'Organizzazione a Dasa-Rägister;
b) una verifica supplementare presso l'Organizzazione (Follow-Up Audit).

In caso di Non Conformità Maggiori è necessario verificare l'efficacia del trattamento entro la data di scadenza del Certificato al fine di poterne deliberare il rinnovo. Ciò implica che il Re-Audit deve essere effettuato con sufficiente anticipo al fine di permettere la gestione di eventuali Non Conformità. Qualora non si riesca a completare l'iter entro i tempi previsti, si procederà con la Revoca del Certificato. In quest'ultimo caso l'Organizzazione che desideri nuovamente ottenere la Certificazione dovrà riattivare l'iter effettuando un Initial Audit (§ 3).

7. CLASSIFICAZIONE DEI RILIEVI

I rilievi riscontrati durante l'Audit sono classificati in Non Conformità Maggiori, Non Conformità Minori e Osservazioni**.**

Una Non Conformità si definisce "Maggiore" quando si ha:

- assenza o non effettiva implementazione di uno o più degli elementi richiesti dal Sistema di Gestione, o una situazione che genera dubbi significativi circa la capacità di soddisfare i requisiti del prodotto o del servizio;
- un elevato numero di Non Conformità Minori riferite ad un singolo processo/requisito, che potrebbe comportare la totale inadeguatezza del prodotto o del Sistema di Gestione, oppure una situazione che potrebbe causare il rilascio di un prodotto non conforme o non rispondente a requisiti cogenti;
- la mancata risoluzione di una o più Non Conformità Minori rilevate durante il precedente Audit.

Una Non Conformità si definisce "Minore" quando:

- il Sistema di Gestione non dimostra la capacità di controllare completamente uno o più aspetti individuati dall'Organizzazione ma fornisce fiducia del controllo del relativo processo;
- un requisito della norma non è stato interpretato o applicato in modo completo e corretto, o non è stato adeguatamente documentato.

L'Audit Team può fornire "Osservazioni" quando identifica aree di miglioramento relative ad attività che comunque risultano essere conformi. Sebbene non richiedano la formalizzazione né la comunicazione a Dasa-Rägister di alcuna gestione, si richiede in ogni caso all'Organizzazione di fornire evidenza dell'analisi delle stesse in occasione delle verifiche successive.

I rilevi che dovessero emergere durante il Pre-Audit non vengono classificati.