REGOLAMENTO DI CERTIFICAZIONE

SGSI

SISTEMI DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI
ISO 27001

DATI IDENTIFICATIVI DEL DOCUMENTO

REV.	DATA EMISSIONE	REDATTO DA: IL RESPONSABILE QUALITÀ	APPROVATO DA: LA DIREZIONE DI RISK CONTROL ADVISORY
00	2023-09-15	Firmato in originale	Firmato in originale

TABELLA DELLE REVISIONI

REV.	DATA REVISIONE	DESCRIZIONE/SINTESI DELLA REVISIONE
00	2023-09-15	Prima emissione

SOMMARIO

Art. 1 – Scopo e campo d'applicazione

Il presente Regolamento definisce e regola i rapporti tra RISK CONTROL ADVISORY quale Organismo di Certificazione, nel seguito OdC e le Organizzazioni richiedenti la certificazione del proprio.

Inoltre, definisce le modalità e condizioni per il rilascio, il rifiuto, il mantenimento della certificazione, l'estensione o la riduzione del campo di applicazione della certificazione, il rinnovo, la sospensione o il ripristino a seguito della sospensione, e la revoca della certificazione, nonché le regole per l'uso del certificato e del marchio di certificazione RISK CONTROL ADVISORY.

L'accesso ai servizi di certificazione è consentito a qualsiasi Organizzazione che ne faccia richiesta in osservanza al presente regolamento, escludendo l'applicazione di condizioni discriminatorie di qualsivoglia natura.

La consulenza nella definizione ed applicazione di Sistemi di Gestione Aziendale non rientra tra i servizi forniti da RISK CONTROL ADVISORY in quanto, in accordo con quanto stabilito dalle norme per l'accreditamento degli Organismi di certificazione, RISK CONTROL ADVISORY non svolge tale attività al di là delle normali funzioni informative e d'assistenza alle Organizzazioni da certificare e certificate. RISK CONTROL ADVISORY inoltre non affida all'esterno attività di audit, non offre né fornisce servizi di audit interni ai propri clienti certificati e non certifica sistemi di gestione per cui abbia eventualmente fornito servizi di audit interni, se non dopo almeno due anni dalla conclusione degli audit stessi. RISK CONTROL ADVISORY non certifica altri Organismi di certificazione per le attività di certificazione di sistemi di Gestione della Sicurezza delle Informazioni.

La certificazione RISK CONTROL ADVISORY non è più semplice, più facile, più rapida o meno costosa nel caso in cui l'Organizzazione cliente abbia utilizzato i servizi di una società di consulenza piuttosto che un'altra. L'attività certificativa di RISK CONTROL ADVISORY non è collegata ad attività di organizzazioni che erogano servizi di consulenza, per cui, nell'eventualità in cui vi siano società di consulenza che affermino in modo inappropriato che la certificazione RISK CONTROL ADVISORY sarà influenzata dal fatto di aver richiesto il servizio consulenziale alla società stessa, saranno presi i provvedimenti del caso.

Art. 2 – Normativa di riferimento

NORMA	TITOLO
ISO/IEC 17021-1:2015	"Valutazione della conformità - Requisiti per gli organismi che forniscono audit e certificazioni di sistemi di gestione. Parte 1 - Requisiti"
ISO/IEC 27001	"Sistemi di Gestione della Sicurezza delle Informazioni"
UNI EN ISO 19011:2012	"Linee guida per gli audit dei sistemi di gestione"
Requisiti Organismi Accreditamento	Disponibili sul sito web dell'Organismo di Accreditamento
Documenti IAF MD	Disponibili su http://www.iaf.nu/articles/Mandatory_Documents_/38

Art. 3 – Definizioni

La certificazione è "Attestazione di parte terza della conformità di prodotti, processi, sistemi o persone" (*cfr* ISO/IEC 17000:2004).

Il Certificato di conformità rilasciato dall'OdC è il documento che attesta che l'Organizzazione richiedente opera con un SGSI conforme alla Norma di riferimento ISO 27001.

Le definizioni relative ai termini utilizzati per le attività riguardanti la certificazione dei Sistemi di Gestione per la Sicurezza delle Informazioni sono quelle riportate nella ISO 27001 "Sistemi di Gestione della Sicurezza delle Informazioni" con le seguenti precisazioni:

Organizzazione: Termine utilizzato per indicare il soggetto che fornisce un prodotto o un servizio richiedente la certificazione;

OdC: Organismo di certificazione;

CT: Comitato Tecnico di certificazione;

Sito: Luogo o luoghi in cui l'Organizzazione attua il Sistema di Gestione per la Sicurezza delle Informazioni oggetto della richiesta di certificazione;

Valutazione/Verifica: Attività mediante la quale RISK CONTROL ADVISORY verifica che l'Organizzazione operi in conformità al modello di Sistema di Gestione per la Sicurezza delle Informazioni di riferimento;

Sorveglianza: Attività mediante la quale RISK CONTROL ADVISORY verifica il mantenimento della conformità del SGSI ai requisiti specificati;

Gruppo di Verifica Ispettiva (GVI): Gruppo di Ispettori incaricato dall'OdC di eseguire la valutazione del SGSI dell'Organizzazione;

Area Tecnica: insieme dei processi necessari a soddisfare le attese del cliente e relativi requisiti legali e regolamentati applicabili per i prodotti e servizi dell'organizzazione.

Anomalia: Non Conformità e Osservazione;

Rilievo: Non Conformità, Osservazione e Commento;

Non Conformità: assenza o mancata applicazione di uno o più requisiti della norma che ha diretta influenza sul SGSI; mancato rispetto dei requisiti cogenti e/o regolamentari relativi a prodotti/servizi rientranti nell'oggetto di certificazione.

Osservazione: uno o più requisiti di norma sono parzialmente disattesi senza pregiudicare l'efficacia del SGSI; episodio isolato in cui è disatteso un requisito di norma senza che ciò pregiudichi l'efficacia del SGSI; applicazione della Norma non pienamente conforme a requisiti quali carenze formali o procedurali nella gestione dei processi (il SGSI è comunque sotto controllo).

Commento: rilievo non conseguente al riscontro di una situazione oggettiva di mancato soddisfacimento di un requisito, ma finalizzato a prevenire che tale situazione si verifichi (in quanto potenzialmente realizzabile) e/o a fornire indicazioni per il miglioramento delle prestazioni dell'Organizzazione.

Tipologie di Verifiche:

VPC: verifica preliminare di certificazione

VIC: verifica iniziale di certificazione (suddivisa sempre in stage 1 e stage 2)

VPS: verifica programmata di sorveglianza

VSS: verifica supplementare di sorveglianza

VRC: verifica di rinnovo certificazione/ricertificazione (effettuata in un'unica fase oppure divisa in stage 1 e stage 2)

Tutte le verifiche, ad eccezione della Preliminare (VPC), possono, in relazione alle necessità dell'OdC, essere effettuate con gli ispettori dell'Ente di accreditamento.

Art. 4 – Gestione dell'Imparzialità

La direzione e tutto il personale RCA si impegnano all'imparzialità nell'attività di certificazione.

RCA gestisce eventuali conflitti di interesse e garantisce l'obiettività delle attività svolte dal personale sia interno sia esterno che opera in nome e per conto di RCA.

Tutte le possibili fonti da cui può derivare un eventuale conflitto di interessi sono state individuate all'origine ed eliminate; se non previste, vengono segnalate direttamente dagli operatori come forma di prevenzione.

Allo stesso modo, RCA non intrattiene rapporti commerciali e/o di altra natura che possano alterarne l'imparzialità.

Le relazioni che possono essere fonti di potenziale minaccia all'imparzialità possono derivare da fattori quali:

- la proprietà;
- l'amministrazione;
- il personale impiegato nell'organizzazione;
- risorse finanziarie;
- la vendita di servizi;
- attività di marketing;
- rapporti economico/commerciali;
- pubblicità ingannevole;
- altro.

Per gestire le potenziali minacce sopra menzionate, le valutazioni dei rischi e il sistema di gestione RCA hanno identificato azioni di controllo che sono state messe in atto per eliminare ogni possibile fonte di conflitto di interessi o minacce all'imparzialità.

Le principali azioni messe in atto da RCA sono:
- tutte le funzioni interne ed esterne sottoscrivono un impegno a gestire il conflitto di interessi;
- nel processo di erogazione del servizio sono presenti diversi filtri, ovvero diverse risorse, che svolgono attività di controllo della conformità dei processi in atto;
- le attività di revisione pratica, le decisioni per la certificazione sono svolte da personale che non ha assolutamente preso parte alle attività di verifica
- il coinvolgimento dei Soggetti Interessati che hanno diritto di accesso alle informazioni riguardanti le attività di RCA.

In aggiunta a quanto sopra, il divieto assoluto di:
- svolgere attività di consulenza diretta o indiretta;
- offrire diversi servizi ad uso commerciale nei confronti delle organizzazioni clienti;
- associare il nome e il logo RCA ad attività che promuovono favori e vantaggi nel processo di certificazione.

4.0 COINVOLGIMENTO DEGLI INTERESSATI

Agli Interessati è garantita la possibilità di richiedere informazioni sulla gestione del processo di certificazione imparziale attraverso le informazioni presenti sul sito www.RCA.com.

RCA individua e sollecita il coinvolgimento dei principali o di tutti i possibili portatori di interessi.

Le parti interessate possono includere rappresentanti di:

- clienti delle organizzazioni certificate;
- rappresentanti delle associazioni industriali e di categoria;
- rappresentanti degli organi governativi di controllo;
- rappresentanti di altri enti pubblici;
- rappresentanti di organizzazioni non governative;
- rappresentanti di strutture pubbliche non governative;
- rappresentanti delle organizzazioni dei consumatori;
- rappresentanti delle associazioni di categoria.

Gli interessati possono richiedere informazioni a info@RCA.com in merito alle procedure poste in essere per garantire l'imparzialità nel processo di certificazione RCA e al loro funzionamento, con riferimento, ad esempio, a:

- Stato attività e schemi di certificazione accreditati e non accreditati;
- Andamento delle certificazioni;
- Risultati degli audit interni;
- Risultati dei riesami della direzione;
- Risultati degli audit dell'Organismo di Accreditamento;
- Esiti della valutazione periodica dei rischi per l'imparzialità;
- Tariffe.

Sarà cura della Direzione RCA rispondere ad ogni richiesta in modo tempestivo e al fine di confermare l'assoluta imparzialità delle attività di certificazione, nel rispetto della normativa applicabile in materia di protezione dei dati.

Art. 5 – Condizioni Generali

L'Organizzazione deve avere un sistema di gestione documentato (Manuale, Procedure) in accordo ai requisiti della normativa di riferimento prescelta per la certificazione e deve dimostrare di utilizzare operativamente il sistema di gestione in accordo ai requisiti della documentazione del sistema e della normativa di riferimento relativamente al campo di applicazione del sistema stesso.

In particolare, ogni Organizzazione può richiedere la certificazione del proprio SGSI a condizione che:

- disponga di un SGSI che soddisfi i requisiti della norma di riferimento indicata nella richiesta d'offerta;
- abbia applicato integralmente il SGSI predetto da almeno 4 mesi;
- abbia completato almeno un intero ciclo di verifiche ispettive interne ed effettuato un riesame da parte della direzione;
- accetti le condizioni previste dal presente Regolamento;
- garantisca l'assistenza al Gruppo di Valutazione dell'OdC durante la visita di valutazione con particolare riguardo alla tutela della sicurezza ed incolumità degli Ispettori come previsto dalla legislazione vigente, autorizzi l'accesso alle aree ed alle informazioni necessarie per svolgere la verifica ispettiva.

Art. 6 – Certificazione del Sistema di Gestione per la Sicurezza delle Informazioni

6.1 – Presentazione della Domanda

L'Organizzazione che intende avviare l'iter certificativo con RISK CONTROL ADVISORY deve presentare apposita richiesta di preventivo utilizzando il modulo fornito dall'OdC (modello M-DCT01-0106), nella quale deve indicare il consulente/società di consulenza che ha supportato l'organizzazione nell'implementazione dell'SGSI (informazione che l'Organizzazione si impegna a mantenere aggiornata in corso di mantenimento della certificazione).

Ricevuta la richiesta, l'OdC emette, in base agli elementi forniti ed al vigente tariffario, l'"Offerta economica" che rimarrà valida per un periodo di 60 giorni dalla data di emissione.

L'OdC, sulla base delle indicazioni fornite dall'Organizzazione, in particolar modo relativamente al numero di addetti, alle attività e, se applicabile, al numero ed alla localizzazione delle sedi distaccate e/o dei cantieri, quantifica la durata delle verifiche e definisce il settore EA di riferimento per l'Organizzazione nonché il campo di applicazione (Oggetto) della Certificazione e le Aree Tecniche coinvolte. Il numero di addetti, le attività aziendali e le eventuali sedi distaccate/cantieri saranno oggetto di verifica e conferma durante il primo audit in azienda.

I tempi di verifica potranno essere modificati anche successivamente alla certificazione in base alle informazioni aggiornate annualmente relative al numero di addetti, ai siti produttivi/cantieri aperti ed operativi, alla loro complessità e alla loro dislocazione geografica.

In caso si rilevino discordanze rispetto a quanto comunicato, sia in fase di richiesta di preventivo, sia annualmente, potranno verificarsi le seguenti possibilità:

- riduzione dello scopo di certificazione;
- definizione di un supplemento di verifica ispettiva da effettuarsi comunque entro un periodo massimo di 60 giorni;
- adeguamento del piano di verifica in corso;
- non concessione della certificazione.

Eventuali costi aggiuntivi, dovuti a supplementi di verifica, saranno fatturati a carico dell'Organizzazione certificanda/certificata nelle modalità previste nell'offerta.

In caso di mancata accettazione dell'offerta entro i 60 giorni, ovvero di mancato inizio dell'iter di certificazione nei 12 mesi dall'emissione dell'offerta, nel caso in cui sia stata accettata, questa decade automaticamente senza obbligo di penali a carico dell'Organizzazione.

Quest'ultima ha peraltro la facoltà di ripresentare, con le stesse modalità, una nuova richiesta di preventivo alla quale farà seguito la nuova offerta dell'OdC.

L'insieme dei documenti: "Richiesta di preventivo" (modello M-DCT01-0106), "Offerta economica" (modello M-DCT01-0103) "Regolamento di Certificazione di SGSI" (modello M-DCT01-0105) e, quando applicabile, "Regolamento di Certificazione di SGSI - Addendum" (modello M-DCT01-0105A) costituisce l'accordo contrattuale tra l'Organizzazione richiedente e l'OdC per l'attività di certificazione. Il contratto è valido salvo rinuncia da trasmettere nelle modalità previste all'art. 9 del presente Regolamento.

Le verifiche saranno effettuate sia presso la sede dell'Organizzazione, sia presso i suoi siti produttivi e/o cantieri, affinché il GVI possa riscontrare la reale applicazione di tutti i requisiti della norma ISO 27001, relativamente alle tipologie di attività oggetto della certificazione.

Tutte le attività/opere rientranti nello scopo di certificazione devono essere verificate presso le sedi/siti produttivi/cantieri nel corso del periodo di durata della validità della certificazione.

Nel caso in cui RISK CONTROL ADVISORY decida di non accettare una domanda di certificazione, come risultato del riesame della domanda stessa, vengono documentate e chiarite al cliente le ragioni che hanno portato alla non accettazione.

6.2 – Visita Preliminare di Certificazione

La VIC può essere preceduta da una Verifica Preliminare di Certificazione (VPC).

Su richiesta dell'Organizzazione, RISK CONTROL ADVISORY svolge, prima che sia avviato l'iter di certificazione, una verifica ispettiva preliminare al fine di valutare lo stato di applicazione del Sistema di Gestione per la Sicurezza delle Informazioni.

La suddetta attività non influisce sulle successive attività del processo di verifica, che non potranno subire riduzioni di durata o modifiche nella prassi definita per l'esecuzione delle verifiche ispettive a seguito di risultati particolari della verifica preliminare.

Non sarà possibile, ad esempio, non verificare un qualsiasi paragrafo della norma perché già visto in sede di verifica preliminare, così come non sarà possibile ridurre il numero di giornate/uomo come calcolate in fase di offerta.

La Verifica Preliminare di Certificazione (VPC) è quindi a tutti gli effetti fuori dall'iter di certificazione.

Le VPC hanno durata non superiore ad 1 g/u e sono condotte seguendo la stessa metodologia delle verifiche ispettive documentali ordinarie. RISK CONTROL ADVISORY non gestisce il feedback con l'azienda (accettazione delle AC, verifica della chiusura, ecc.).

Le verifiche ispettive preliminari sono sempre svolte a titolo oneroso, in base a quanto stabilito nel tariffario in vigore per il costo della giornata/uomo.

6.3 – Programmazione e Pianificazione Verifiche Ispettive

Con almeno 5 gg di anticipo rispetto alla data di effettuazione di ogni audit, il Responsabile del GVI (RGVI) trasmette all'Organizzazione il piano della verifica ispettiva, contenente, tra l'altro, le date ed i siti dove saranno condotte le attività in campo, la durata attesa delle attività, i ruoli dei membri del GVI. L'RGVI sviluppa inoltre un programma di audit per il ciclo completo di certificazione, comprendente, per la certificazione iniziale, l'audit iniziale (stage1+stage2), gli audit di sorveglianza nel primo e secondo anno, e l'audit di rinnovo al terzo anno. Per i cicli di certificazione successivi il programma di audit parte con la decisione del rinnovo della certificazione e comprende le due sorveglianze ed il rinnovo al terzo anno. Il programma di audit copre tutti i requisiti del sistema di gestione nel suo complesso e può essere rivisto dall'RGVI a valle di ogni audit, in funzione di modifiche ai requisiti di certificazione, ai requisiti legali, ai requisiti di accreditamento, così come a cambiamenti di ogni genere che possano influenzare la conformità del sistema di gestione alla norma di riferimento, al variare di condizioni relative ad addetti e attività aziendali compresi nel sistema di gestione, alla localizzazione di eventuali cantieri/siti temporanei ad alle attività in essi svolte, ecc..

6.4 Gruppi di Verifica Ispettiva

Contestualmente alla trasmissione del piano di audit, all'Organizzazione è comunicato il GVI che eseguirà la verifica ispettiva. L'Organizzazione ha facoltà di ricusare il GVI attraverso una comunicazione scritta da inoltrare ad RISK CONTROL ADVISORY, entro 5 giorni dalla comunicazione dell'OdC. La ricusazione deve essere supportata da fondate motivazioni. RISK CONTROL ADVISORY fornisce su richiesta eventuali altre informazioni di base su ogni membro del GVI.

Il GVI RISK CONTROL ADVISORY comprende sempre competenze di audit e di SGSI e viene qualificato con riferimento alle aree tecniche relative all'Organizzazione oggetto di verifica.

I compiti assegnati prevedono che il GVI:

a) esamini e verifichi la struttura, le politiche, i processi, le procedure, le registrazioni e i documenti dell'organizzazione cliente;

b) stabilisca se questi soddisfino tutti i requisiti pertinenti al campo di applicazione previsto;

c) verifichi se i processi e le procedure siano stabiliti, applicati e mantenuti attivi in modo efficace, così da costituire una base di conformità del sistema di gestione del cliente;

d) comunichi al cliente, per sue azioni conseguenti, eventuali incongruenze tra politica, obiettivi, traguardi e risultati.

Alle verifiche ispettive possono inoltre partecipare:

- Ispettori in addestramento od Osservatori dell'OdC;
- Consulenti dell'Organizzazione.

Questi ultimi possono presenziare in qualità di osservatori, quindi senza diritto di intervento nell'attività di verifica.

Il costo dell'eventuale partecipazione di "Ispettori in addestramento" è a carico dell'OdC stesso.

Allo scopo di accertare che le modalità di valutazione adottate da RISK CONTROL ADVISORY siano conformi alle norme di riferimento, l'Organismo di Accreditamento può richiedere:

- la partecipazione di suoi osservatori agli audit effettuati da RISK CONTROL ADVISORY;

- l'effettuazione di visite presso l'Organizzazione certificata, direttamente attraverso l'uso di proprio personale.

La partecipazione di osservatori agli audit e/o l'eventuale visita condotta direttamente attraverso l'uso di personale dell'Organismo di Accreditamento è preventivamente concordata tra RISK CONTROL ADVISORY e l'Organizzazione.

Qualora l'Organizzazione non conceda il proprio benestare, la validità del certificato è sospesa fino a quando non viene concesso il benestare alla verifica, per un periodo massimo di 3 mesi.

Scaduti i 3 mesi, in assenza di benestare alla verifica, la certificazione viene revocata.

Le modalità di accertamento utilizzate dagli Organismi di Accreditamento, sono riportate in appositi regolamenti e/o comunicazioni / circolari disponibili sui siti web degli stessi.

L'Organizzazione dovrà rendere disponibile all'Organismo di Accreditamento la documentazione che RISK CONTROL ADVISORY ha preso a riferimento durante gli audit precedenti.

Nel caso invece di visite di sorveglianza supplementari non programmate, con breve preavviso (generalmente 1 settimana), di cui al punto 6.8 del presente Regolamento, il GVI sarà scelto con particolari cautele in quanto i membri non potranno essere ricusati.

6.5 – Conduzione delle verifiche ispettive

Le Verifiche Ispettive, di stage 1, stage2, sorveglianza, rinnovo e supplementari, sono strutturate nel seguente modo:

- una riunione iniziale, con la Direzione ed i Responsabili dell'Organizzazione, per confermare le finalità e le modalità della Verifica e il Piano di Verifica;
- la verifica e l'approfondimento di rilievi riscontrati nel corso di verifiche documentali e/o in campo precedenti;
- l'audit vero e proprio, in caso di esito positivo delle verifiche di cui al punto precedente e di risoluzione di ogni eventuale divergenza di interpretazione fra RISK CONTROL ADVISORY e Organizzazione, comprendente la Verifica nei luoghi dell'Organizzazione al fine di misurare la corretta attuazione del SGSI in accordo alla documentazione di riferimento;
- una riunione finale per presentare alla Direzione dell'Organizzazione i risultati e le conclusioni del GVI in merito alla rispondenza del SGSI al modello di riferimento, precisando eventuali Non Conformità, Osservazioni e Commenti riscontrati. Al termine della riunione, il Responsabile del GVI (RGVI) rilascia alla Direzione dell'Organizzazione un Rapporto di Verifica che descrive i risultati della verifica e con le eventuali Non Conformità riscontrate, le Osservazioni e i Commenti.

I risultati della verifica e l'entità dei rilievi riscontrati vengono ratificati direttamente dal RGVI che su mandato dell'OdC ha facoltà di confermare all'Organizzazione, a conclusione delle attività di verifica, i risultati ottenuti.

6.6 – Follow-up delle verifiche ispettive

Qualora, nel corso delle verifiche di cui sopra, tenuto conto della natura campionaria delle medesime, venissero, incidentalmente, riscontrate dal GVI inosservanze di requisiti di legge non riguardanti aspetti direttamente correlati al sistema valutato, ma correlati ad altri aspetti delle attività svolte dall'Organizzazione per esempio aspetti di natura ambientale o legati alla sicurezza dei lavoratori, senza obbligo di verifica di tali aspetti, il GVI è tenuto ad informare la direzione dell'Organizzazione valutata attraverso apposito documento "riservato" diverso dal rapporto di verifica. Tale aspetto, tranne che in casi eccezionali in cui sarà richiesto all'Organizzazione, da parte della direzione tecnica di RISK CONTROL ADVISORY, di porre rimedio in un tempo stabilito e ragionevolmente breve, sarà oggetto di valutazione nel corso della successiva verifica ispettiva.

In ogni caso i risultati della verifica raggiunti dal GVI sono oggetto di riesame interno e di eventuale ulteriore ratifica formale da parte dell'OdC.

Qualora la valutazione dell'OdC non confermi l'esito raggiunto e già ratificato dal GVI, l'OdC informa l'Organizzazione nel più breve tempo possibile, e comunque non oltre 10 giorni dalla Verifica effettuata, attraverso specifica comunicazione scritta indicando le variazioni al precedente risultato e le motivazioni.

A fronte delle Non Conformità e delle Osservazioni ratificate l'Organizzazione deve inviare all'OdC, nei tempi concordati e sull'apposita modulistica, le rispettive correzioni, le cause e le azioni correttive, indicando la tempistica di attuazione. Le stesse possono essere raccolte dal GVI direttamente al termine della verifica ispettiva. Nel caso in cui la struttura tecnica di RISK CONTROL ADVISORY decida di modificare l'esito della verifica, come sopra specificato, l'Organizzazione può essere invitata ad inoltrare nuovamente correzioni, cause, azioni correttive e tempi di risoluzione.

L'OdC valuta ed approva le azioni correttive proposte e, qualora non le ritenga adeguate, ne informa per iscritto l'Organizzazione per le revisioni necessarie. L'iter di rilascio/mantenimento/rinnovo della certificazione non potrà in ogni caso proseguire finché l'Organizzazione non provveda ad inviare le opportune azioni correttive all'OdC, con la conseguenza che l'Organizzazione non potrà essere sottoposta all'analisi del Comitato Tecnico.

I Commenti devono essere presi in carico per iscritto dall'Organizzazione. RISK CONTROL ADVISORY verificherà le relative considerazioni nel corso della verifica successiva (di sorveglianza/rinnovo/supplementare). I Commenti non presi in carico potranno essere riproposti come Osservazioni.

6.7 – Verifiche ispettive di certificazione

Le VIC sono condotte in due fasi, chiamate audit di stage 1 e audit di stage 2.

6.7.1 Audit di stage 1

Nel corso dell'audit di stage 1 il GVI RISK CONTROL ADVISORY:

- verifica la documentazione del SGSI dell'Organizzazione;
- valuta il sito dell'Organizzazione, comprese eventuali particolarità, ed approfondisce con il personale aziendale il grado di preparazione per l'audit di stage 2;
- esamina il livello di adeguamento e di comprensione rispetto ai requisiti della norma di riferimento, in particolare relativamente agli aspetti più significativi di processi, attività, prestazioni e obiettivi del SGSI;
- raccoglie le informazioni necessarie riguardo al campo di applicazione del SGSI, ai processi e alle apparecchiature utilizzate, ai livelli dei controlli stabiliti, ai siti, ai requisiti legislativi e regolamentari di riferimento;
- riesamina l'adeguatezza del GVI per l'audit di stage 2, di cui definisce i dettagli con l'Organizzazione;
- mette a fuoco la pianificazione dell'audit di stage 2, acquisendo una sufficiente conoscenza dell'SGSI e delle attività aziendali;
- valuta se gli audit interni e il riesame della direzione sono in corso di pianificazione ed esecuzione e che il livello di attuazione del sistema di gestione fornisca l'evidenza che il cliente è pronto per lo stage 2.

L'audit di stage 1 è condotto presso la sede dell'Organizzazione cliente.

Come indicato al punto 6.5 del presente Regolamento, al termine dell'audit di stage 1, l'RGVI formalizza i risultati della verifica di stage 1 e li comunica all'Organizzazione.

Nel caso in cui le anomalie individuate potessero portare all'emissione, in stage 2, di NC o di più di 10 Osservazioni, gli audit di stage 1 e stage 2 saranno separati da un intervallo di tempo sufficiente all'Organizzazione per la risoluzione dei rilievi (non più di 4 mesi, altrimenti sarà necessario ripetere la verifica di stage 1).

In caso contrario, l'audit di stage 2 può iniziare immediatamente dopo l'audit di stage 1. In ogni caso, gli audit di stage 1 e 2 sono solitamente separati per organizzazioni con un numero equivalente di dipendenti superiore a 25; entrambi i casi, la piccola impresa ed eccezionalmente l'organizzazione > 25, ogniqualvolta lo stage 2 abbia inizio alla fine dello stage 1, saranno debitamente giustificati nel rapporto di audit di stage1.

A valle dell'audit di stage 1 può essere rivista la pianificazione dell'audit di stage 2, anche in termini di giorni/uomo ed anche in funzione delle esigenze del cliente per la risoluzione dei problemi identificati in stage 1. In assenza di comunicazioni contrarie, si considera confermata la pianificazione dell'audit di stage 2 già trasmessa all'Organizzazione.

6.7.2 Audit di stage 2

Nel corso dell'audit di stage 2, che è sempre condotto presso la sede del Cliente, il GVI RISK CONTROL ADVISORY verifica almeno:

- le informazioni e le evidenze circa la conformità a tutti i requisiti della norma di sistema di gestione applicabile o di altri documenti normativi;
- il monitoraggio, la misurazione, il reporting e il riesame delle prestazioni, a fronte degli obiettivi e traguardi fondamentali di prestazione (coerentemente alle attese della norma di sistema di gestione applicabile o di altro documento normativo);

la capacità del sistema di gestione del cliente e le relative prestazioni, con riferimento al rispetto dei requisiti cogenti applicabili;

- il controllo operativo dei processi del cliente;
- gli audit interni e il riesame della direzione;
- la responsabilità della direzione rispetto alle politiche del cliente;
- le correlazioni complessive tra: i requisiti della norma, la politica, gli obiettivi, i requisiti cogenti applicabili, la responsabilità e la competenza del personale, le prestazioni e i risultati degli audit interni.

Al termine della verifica, il GVI RISK CONTROL ADVISORY analizza tutte le evidenze emerse nel corso delle verifiche di stage 1 e di stage 2 per riesaminare ogni rilievo e concordare sulle conclusioni dell'audit. Come indicato al punto 6.5 del presente Regolamento, al termine dell'audit di stage 2, l'RGVI formalizza i risultati della verifica e li comunica all'Organizzazione.

L'RGVI trasmette poi il proprio rapporto di verifica alla struttura tecnica di RISK CONTROL ADVISORY.

6.7.3 – Procedura per il Rilascio della Certificazione

La documentazione della pratica viene esaminata dalla Direzione RISK CONTROL ADVISORY prima di essere sottoposta al Comitato Tecnico per la delibera del rilascio della Certificazione. Affinché la pratica di certificazione possa essere portata all'analisi del Comitato Tecnico deve presentarsi almeno la seguente condizione 1:

Condizione 1

- Non Conformità pari a 0 (Zero);
- Osservazioni fino a 10 (Dieci) incluso;
- Commenti nessuna limitazione.

In tal caso l'Organizzazione deve definire per ogni Osservazione rilevata dal GVI il trattamento e le azioni correttive poste in atto. Tale attività deve essere effettuata utilizzando il "File Gestione Rilievi" (modulo M-DCT01-0207).

Tutti i modelli M-DSG01-0207 compilati devono essere trasmessi sempre in originale ad RISK CONTROL ADVISORY appena possibile, anticipandoli a mezzo fax od e-mail. Possono essere ritirati compilati direttamente dall'RGVI alla fine dell'audit.

La pratica di certificazione non può essere sottoposta al comitato se la Direzione Tecnica di RISK CONTROL ADVISORY e l'RGVI non hanno verificato ed accolto su base documentale, e se necessario attraverso una verifica supplementare, la positiva chiusura delle Osservazioni o il programma di superamento. In assenza di una comunicazione contraria da parte di RISK CONTROL ADVISORY entro 10 gg dal ricevimento delle correzioni e delle AC, le stesse si intendono accettate.

In caso di verifica positiva da parte della Direzione Tecnica e dell'RGVI, la pratica viene portata all'attenzione del Comitato Tecnico che può deliberare per il rilascio della certificazione. In relazione al numero e all'importanza delle Osservazioni rilasciate, nonché alle azioni correttive definite, il comitato può deliberare che sia effettuata una verifica di sorveglianza supplementare (VSS), successiva alla certificazione, da effettuarsi in un tempo definito dal comitato ma comunque non superiore a 6 mesi dalla data di rilascio della certificazione.

L'incremento delle verifiche di sorveglianza così stabilito serve a garantire che i provvedimenti messi in atto dall'Organizzazione siano realmente efficaci, in un periodo di tempo definito, nel rispetto del Sistema di Gestione dell'Organizzazione nonché validati ai fini della conformità delle regole generali di certificazione dell'OdC.

Qualora la verifica di sorveglianza supplementare, rilevasse importanti carenze nell'applicazione efficace delle azioni correttive definite, il Comitato Tecnico potrà deliberare la sospensione della certificazione.

Per la revoca della sospensione dovrà essere effettuata nuovamente una verifica supplementare VSS. Tale iter è da intendersi valido anche per le verifiche programmate di sorveglianza VPS.

Le VSS effettuate in tale condizione risultano a carico dell'Organizzazione.

Nei restanti casi la pratica non può essere sottoposta al Comitato Tecnico ed in particolare:

Condizione 2

- Non Conformità 1 (Uno) o più e/o;
- Osservazioni oltre 10 (dieci).

In tal caso l'Organizzazione deve definire per ogni Non Conformità e Osservazione rilevata dal GVI il trattamento e le azioni correttive poste in atto. Tale attività deve essere effettuata utilizzando il "File Gestione Rilievi" (modulo M-DCT01-0207).

La pratica di certificazione non può essere sottoposta al Comitato Tecnico.

RISK CONTROL ADVISORY effettua un'indagine supplementare (in campo o documentale) al fine di verificare il superamento delle NC rilevate ed almeno il programma di superamento delle Osservazioni.

Qualora questa indagine supplementare riporti l'Organizzazione nella "Condizione 1" la pratica può essere sottoposta al Comitato Tecnico.

L'eventuale verifica supplementare in campo risulta a carico dell'Organizzazione.

Se l'implementazione delle correzioni ed azioni correttive relative ad ogni NC non possono essere verificate da RISK CONTROL ADVISORY entro 6 mesi dalla data dell'audit di stage 2, allora l'audit di stage 2 stesso va ripetuto, prima di poter proporre la pratica al Comitato Tecnico per la certificazione.

6.7.4 – Decisioni per la Certificazione

Ad esito favorevole dell'esame del Comitato Tecnico, verificato l'adempimento degli impegni economici da parte dell'Organizzazione, RISK CONTROL ADVISORY emette il Certificato di Conformità.

L'OdC invia all'Organizzazione una lettera per informarla dell'ottenimento della Certificazione, allegando il Certificato di Conformità. In esso sono riportati fra l'altro: la ragione sociale dell'Organizzazione, l'indirizzo delle sue sedi, le norme e/o regolamenti di riferimento, l'oggetto e i limiti di applicazione del Sistema di Gestione per la Sicurezza delle Informazioni certificato, la data e la durata della validità della certificazione.

A seguito del rilascio della certificazione, RISK CONTROL ADVISORY inserisce il nominativo dell'Organizzazione nell'elenco delle Organizzazioni certificate. Tale elenco è aggiornato ad ogni riunione di Comitato Tecnico ed è disponibile a chiunque ne faccia richiesta.

Ad esito non favorevole dell'esame del Comitato Tecnico, RISK CONTROL ADVISORY invia all'Organizzazione una comunicazione in cui vengono spiegate le motivazioni del mancato rilascio della certificazione ed in cui viene specificato se è necessario effettuare una verifica supplementare in campo o sono sufficienti evidenze documentali per riportare l'azienda nella Condizione 1 o nella Condizione 2 di cui sopra, da cui si riprende poi l'iter certificativo.

Il CSI si riunisce periodicamente presso RISK CONTROL ADVISORY ed analizza alcune pratiche di certificazione a campione, per verificare, tra l'altro, la corretta conduzione del processo certificativo da parte di RISK CONTROL ADVISORY dal punto di vista della garanzia dell'imparzialità.

Nel caso in cui durante la verifica del CSI emergano potenziali irregolarità, non imputabili all'Organizzazione, eventuali supplementi di verifica che si rendano necessari non saranno fatturati all'Organizzazione. Viceversa, qualora eventuali mancanze fossero imputabili all'Organizzazione, gli eventuali costi aggiuntivi per supplementi di verifica saranno fatturati all'Organizzazione. Le motivazioni dei supplementi di verifica saranno trasmesse all'Organizzazione con le indicazioni delle relative motivazioni.

La pratica di certificazione viene quindi sottoposta a nuova analisi dello specifico Comitato Tecnico che dovrà definire quali azioni intraprendere per la risoluzione degli eventuali rilievi emersi. RISK CONTROL ADVISORY non porrà in atto provvedimenti di sospensione e/o revoca fino a quando non saranno rilevate evidenze oggettive necessarie a supporto del provvedimento stesso.

Il Comitato Tecnico deve, entro un tempo massimo di 120 giorni, assicurarsi che siano state risolte le problematiche rilevate dal Comitato di Salvaguardia dell'Imparzialità. Trascorso tale periodo RISK CONTROL ADVISORY, nella prima riunione utile del suddetto consiglio, dovrà documentare i risultati ottenuti a seguito degli approfondimenti effettuati.

In ogni caso l'Organizzazione accetta ed autorizza RISK CONTROL ADVISORY a comunicare il provvedimento all'Organismo di accreditamento.

6.8 - Validità, sorveglianza e mantenimento della Certificazione

La certificazione ha validità triennale, decorrente dalla data di emissione riportata sul Certificato (coincidente con la data della riunione del Comitato Tecnico che l'ha deliberato), ed è soggetta a 3 (tre) "verifiche programmate di sorveglianza" (VPS) presso l'Organizzazione, la prima delle (VPS) è svolta entro 12 (dodici) mesi dalla data dell'ultimo giorno di verifica di stage 2, la seconda ad un anno dalla prima e la terza entro un anno dalla seconda.

La terza VPS coincide con la verifica di rinnovo della certificazione VRC.

Con un anticipo di circa 4 mesi rispetto alla data limite per l'effettuazione della verifica di sorveglianza, RISK CONTROL ADVISORY ricorda all'Organizzazione la scadenza ed allega, in genere, la fattura relativa all'audit, insieme all'eventuale modulo relativo ai cantieri attivi in caso di Organizzazioni del settore EA28. La data precisa dell'audit, così come gli eventuali cantieri da visitare, saranno concordati direttamente tra l'Organizzazione e l'RGVI.

Nel caso in cui alla data della verifica di sorveglianza l'Organizzazione non abbia ancora effettuato il pagamento della fattura di cui sopra, comunque trasmessa, la certificazione potrà essere sospesa come previsto dal successivo art. 7.

Le visite di sorveglianza hanno lo scopo di verificare, almeno:

- audit interni e riesame di direzione;
- un riesame delle azioni intraprese a seguito delle non conformità identificate durante il precedente audit;
- il trattamento dei reclami;
- l'efficacia del sistema di gestione in riferimento al conseguimento degli obiettivi del cliente certificato e dei risultati attesi del rispettivo(i) sistema(i) di gestione;
- l'avanzamento delle attività pianificate, finalizzate al miglioramento continuo;
- il controllo operativo su base continua;
- il riesame di ogni modifica;
- l'utilizzo di marchi e/o di ogni altro eventuale riferimento alla certificazione.

Visite di sorveglianza supplementari non programmate, con breve preavviso (generalmente 1 settimana), potranno essere effettuate qualora l'OdC per indagare su reclami o in risposta a modifiche o come azione conseguente nei confronti di clienti cui è stata sospesa la certificazione. In questo caso RISK CONTROL ADVISORY porrà particolare cura nella scelta del Gruppo di Audit in quanto l'Organizzazione non potrà ricusare il Gruppo stesso con l'eventuale presenza dell'Organismo di Accreditamento/Abilitazione. Le motivazioni dell'indagine dovranno essere supportate da evidenze documentali o segnalazioni scritte pervenute all'OdC. Qualora nelle verifiche il GVI confermi la validità delle cause che hanno reso necessario effettuare una Verifica Supplementare i costi di queste ultime saranno addebitati all'Organizzazione nelle modalità definite in sede contrattuale.

Se invece il GVI dovesse concludere la verifica supplementare senza evidenze in merito alle cause che hanno reso necessario effettuare la verifica i costi saranno a carico di RISK CONTROL ADVISORY.

L'Organizzazione certificata deve informare tempestivamente per iscritto l'OdC di modifiche rilevanti che vengano apportate al SGSI. Tali modifiche potrebbero inoltre rendere necessaria, a giudizio dell'OdC, un'apposita VSS.

Il mantenimento della Certificazione per il triennio di validità è soggetto alle prescrizioni riportate al punto 6.7.3. In particolare, il mantenimento della certificazione viene concesso al verificarsi della condizione 1. Tuttavia, la direzione RISK CONTROL ADVISORY può, in relazione al numero ed all'importanza delle Non Conformità/Osservazioni rilevate nelle VPS, effettuare Verifiche di Sorveglianza Supplementare VSS per misurare l'efficacia dei trattamenti posti in essere nonché delle azioni correttive implementate.

Al verificarsi della Condizione 2 definita al punto 6.7.3 RISK CONTROL ADVISORY determina un tempo massimo (in genere non superiore a tre mesi) per il superamento delle non conformità e/o delle osservazioni. Verificato tale superamento con una VSS (documentale o in campo) il Comitato Tecnico decide per il mantenimento della certificazione. In caso di mancato superamento entro il termine stabilito, RISK CONTROL ADVISORY sospende la certificazione all'Organizzazione, così come al successivo art. 7.

Solamente attraverso una VSS (documentale o in campo) che porti nuovamente alla condizione 1, dopo aver sottoposto al Comitato Tecnico la pratica, RISK CONTROL ADVISORY può revocare il provvedimento di sospensione.

I risultati delle verifiche programmate di sorveglianza (VPS) e delle verifiche supplementari di sorveglianza (VSS) sono oggetto di analisi da parte del Comitato Tecnico ai fini del mantenimento della certificazione rilasciata. Il Comitato Tecnico può richiedere eventuali supplementi di verifica o approfondimenti al GVI incaricato.

Altre attività di sorveglianza possono comprendere:

- indagini da parte dell'organismo di certificazione sul cliente certificato relative ad aspetti di certificazione;
- riesame di ogni dichiarazione del cliente certificato rispetto alla proprie attività (per esempio materiale promozionale, sito web);
- richieste al cliente certificato di fornire informazioni documentate (su carta o mezzi elettronici);
- altri mezzi di monitoraggio delle prestazioni del cliente certificato.

Le eventuali anomalie evidenziate da questo ulteriore metodo di indagine, così come la mancata risposta da parte del cliente, saranno gestite come al punto 6.7.3 – condizione 1 o 2 – di cui sopra.

6.9 - Rinnovo della certificazione

La decisione di rinnovo della certificazione è normalmente presa entro la scadenza del triennio di validità del certificato (sempre per le Organizzazione del settore IAF 28). RISK CONTROL ADVISORY può decidere di concedere il rinnovo della certificazione anche quando il processo di ricertificazione si concluda entro un anno dopo la data di scadenza del certificato (in questo caso saranno chiaramente indicate sul certificato le date di inizio e fine validità dell'attuale ciclo di certificazione, e le date di scadenza del precedente ciclo di certificazione e dell'audit di ricertificazione). A seguito della scadenza della certificazione, RISK CONTROL ADVISORY può ripristinare la stessa entro 6 mesi, con una verifica di rinnovo, posto che siano già state completate le attività pendenti di rinnovo della certificazione, oppure dopo 6 mesi ed entro 1 anno, con una verifica della durata almeno di un audit di stage 2 (e non meno della durata di un rinnovo).
In ogni caso, se il certificato dovesse avere una durata inferiore ai 3 anni, per via del rinnovo posticipato, rimane pienamente applicabile il principio per cui nel ciclo di certificazione devono essere coperti tutti i requisiti e tutto lo scopo del certificato, con verifiche di sorveglianza condotte almeno una volta ogni anno. Se le attività di verifica e delibera di rinnovo non vengono completate entro un anno dalla scadenza del certificato, si può procedere soltanto con l'effettuazione di un nuovo audit iniziale (stage 1 + stage 2).
La pianificazione della Verifica di Rinnovo di Certificazione (VRC) viene comunque effettuata a partire dal 4° mese antecedente la data di scadenza del certificato.

Con tale anticipo RISK CONTROL ADVISORY ricorda all'Organizzazione la necessità di effettuare l'audit di rinnovo ed allega, in genere, la fattura relativa, insieme all'eventuale modulo su cui indicare i cantieri attivi in caso di Organizzazioni del settore EA28. La data precisa dell'audit, così come gli eventuali cantieri da visitare, saranno concordati direttamente tra l'Organizzazione e l'RGVI.

Nel caso in cui alla data della verifica di rinnovo l'Organizzazione non abbia ancora effettuato il pagamento della fattura di cui sopra, comunque trasmessa, la certificazione potrà essere sospesa come previsto dal successivo art. 7. In ogni caso il nuovo certificato sarà trasmesso solo a valle del pagamento della fattura.

L'audit di rinnovo è pianificato (anche in considerazione dei risultati delle verifiche precedenti) e condotto per valutare:

- l'efficacia del sistema di gestione nella sua globalità, alla luce di cambiamenti interni ed esterni, e la sua continua pertinenza e applicabilità al campo di applicazione della certificazione;
- l'impegno dimostrato a mantenere l'efficacia ed il miglioramento del sistema di gestione, al fine di rafforzarne le prestazioni complessive;
- l'efficacia del sistema di gestione in riferimento al conseguimento degli obiettivi del cliente ed i risultati attesi del(i) rispettivo(i) sistema(i) di gestione.

L'audit di rinnovo considera le performance del SGSI nel periodo pregresso di certificazione e include il riesame dei rapporti di tutti gli audit di sorveglianza.

Nel caso in cui il SGSI, o la situazione al contorno, abbiano subito significative modifiche (per esempio in caso di sostanziali modifiche legislative), RISK CONTROL ADVISORY può ritenere necessario effettuare un audit di rinnovo suddiviso in stage 1 e stage 2 come ai precedenti punti 6.7.1 e 6.7.2 di questo Regolamento.

In caso di siti multipli (art. 6.12) o di certificazioni emesse a fronte di più norme di sistema di gestione, la pianificazione dell'audit di rinnovo sarà effettuata con particolare attenzione, in modo che la verifica on-site copra tutti i requisiti normativi e tutte le attività aziendali, così da infondere fiducia nella certificazione.

La VRC comporta un nuovo esame della documentazione del SGSI e una visita di rivalutazione sull'intero SGSI secondo le modalità descritte ai precedenti punti 6.7.3 e 6.7.4.

Il rinnovo della Certificazione allo scadere del triennio di validità è soggetto alle prescrizioni riportate al punto 6.7.3. In particolare, la certificazione viene rinnovata al verificarsi della condizione 1. Tuttavia, la direzione RISK CONTROL ADVISORY può, in relazione al numero ed all'importanza delle Non Conformità/Osservazioni rilevate nelle VRC, effettuare Verifiche di Sorveglianza Supplementare VSS per misurare l'efficacia delle trattamenti posti in essere nonché delle azioni correttive implementate.

Al verificarsi della Condizione 2 definita al punto 6.7.3 RISK CONTROL ADVISORY non rinnova la certificazione all'Organizzazione. La pratica di certificazione non può essere sottoposta al Comitato Tecnico.

RISK CONTROL ADVISORY effettua una Verifica di Sorveglianza Supplementare VSS in cui verificare il superamento delle NC rilevate ed almeno il programma di superamento delle Osservazioni.

In casi eccezionali, accoglibili solo dalla Direzione Tecnica RISK CONTROL ADVISORY, il superamento delle NC può essere verificato sulla base di invio di documentazione da parte dell'Organizzazione.

Qualora una o più verifiche documentali e/o di sorveglianza supplementare VSS riportino l'Organizzazione nella "Condizione 1" la pratica può essere sottoposta al Comitato Tecnico.

Le verifiche documentali e le VSS effettuate in tale condizione risultano a carico dell'Organizzazione.

Il Comitato Tecnico può richiedere eventuali supplementi di verifica o approfondimenti al GVI incaricato.

6.10 - Estensione e riduzione del campo di applicazione della certificazione

L'Organizzazione può richiedere all'OdC l'estensione della certificazione ad altre attività, non comprese nel certificato rilasciato.

Analoga richiesta può essere presentata all'OdC nel caso di riduzioni o di esclusioni di attività, fermo quanto indicato nel precedente punto 6.8.

Le suddette estensioni o riduzioni potrebbero rendere necessaria una revisione del certificato di conformità precedentemente rilasciato.

A valle di una richiesta scritta, l'OdC valuterà se, oltre all'esame della documentazione presentata, debba essere svolta una verifica ispettiva supplementare o se questa possa invece essere evitata, integrandola con la prima visita di sorveglianza/rinnovo pianificata.

Modifiche al campo di applicazione della certificazione possono anche essere proposte dall'RGVI al Comitato Tecnico, mediante indicazione nel rapporto di audit, in funzione delle attività rilevate presso la sede (o le sedi) dell'Organizzazione cliente durante la verifica ispettiva.

6.11 – Riconoscimento delle certificazioni rilasciate da altri Organismi di Certificazione – Mantenimento e Rinnovo

Qualora RISK CONTROL ADVISORY riceva richiesta di preventivo da Organizzazione già certificata da altro organismo di certificazione, effettua un riesame analogo a quanto descritto al punto 6.1.

Nel caso in cui l'Organizzazione risulti certificata da un OdC non accreditato per il settore EA da ente firmatario degli accordi EA, PAC, IAAC o IAF MLA o accreditato per il settore EA da ente non firmatario degli accordi EA, PAC, IAAC o IAF MLA, sarà emesso un preventivo per nuova certificazione e l'iter sarà il medesimo di cui ai punti 6.1-6.7.4.

Non sono previste variazioni rispetto alle normali regole RISK CONTROL ADVISORY per il rilascio di nuove certificazioni di conformità.

Nel caso in cui invece l'Organizzazione sia certificata da un OdC accreditato per il settore EA da ente firmatario degli accordi EA, PAC, IAAC o IAF MLA, potrà essere emesso un preventivo di mantenimento della certificazione, comportante comunque una verifica documentale pre-transfer (con conseguente decisione del Comitato Tecnico) con analisi dei seguenti aspetti:

- Congruenza tra settore di attività effettivo e settore EA di certificazione;
- Motivazioni per il cambiamento di OdC;
- Stato di accreditamento dell'OdC certificatore:
  - Accreditamento dell'OdC in corso di validità per lo specifico settore;
  - Analisi di eventuali sospensioni/revoche comminate all'OdC da parte dell'Ente di accreditamento;
- Stato della certificazione rilasciata all'Organizzazione:
  - Certificazione in corso di validità;
  - Congruenza tra attività coperte dal Sistema di Gestione e certificazione emessa;
  - Ammissibilità di eventuali requisiti non applicati;
- Analisi della documentazione di verifica rilasciata dall'OdC certificatore nelle ultime verifiche effettuate fino alla più recente verifica di rinnovo o certificazione e delle azioni correttive definite dall'Organizzazione;
- Eventuali reclami ricevuti dall'Organizzazione e relative azioni intraprese;
- Eventuali implicazioni dell'Organizzazione con Organismi di Regolazione relativamente al rispetto di prescrizioni legislative e/o regolamentari.

A valle dell'esito positivo delle verifiche di cui sopra, il Comitato Tecnico potrà esprimersi favorevolmente in merito al transfer della certificazione e potrà essere ripristinata la periodicità già in essere relativamente alle successive verifiche di sorveglianza e/o rinnovo.

Qualora:

- non sia possibile un qualsiasi contatto con l'OdC cedente, oppure
- non si possieda una qualsiasi conferma sulla validità del certificato da parte dell'OdC cedente, oppure
- non si possieda tutta la documentazione di verifica (comprese le checklist) del ciclo in corso

la verifica documentale pre-transfer sarà condotta parzialmente o totalmente in campo (al limite sarà condotta una nuova certificazione nel caso in cui non vi siano registrazioni disponibili relativamente alla documentazione delle verifiche del ciclo in corso).

A valle dell'esito positivo della verifica documentale pre-transfer in campo, il Comitato Tecnico potrà esprimersi favorevolmente in merito al transfer della certificazione e potrà essere ripristinata la periodicità già in essere relativamente alle successive verifiche di sorveglianza e/o rinnovo.

Nel caso in cui l'accreditamento dell'OdC cedente risulti sospeso, è obbligatorio effettuare una verifica in campo di almeno 1 gg/uomo prima di poter trasferire il certificato.

Nel caso in cui l'accreditamento dell'OdC cedente risulti revocato, è obbligatorio effettuare una verifica in campo della durata almeno pari ad un audit di stage 2, se entro 6 mesi dal provvedimento di revoca, prima di poter trasferire il certificato. Se sono passati più di 6 mesi dal provvedimento di revoca, occorre procedere con una verifica inziale.

Ai fini della determinazione del numero di giornate necessarie per l'effettuazione degli audit, RISK CONTROL ADVISORY tiene conto di quanto previsto dalla guida IAF MD5.

In ogni caso la Direzione RISK CONTROL ADVISORY, a fronte di particolari esigenze tecniche, può incrementare il numero di giornate rispetto a quanto previsto.

La prosecuzione dell'iter di certificazione procede quindi attraverso le stesse modalità definite dal punto 6.2. e successivi. A valle dell'emissione del certificato, RISK CONTROL ADVISORY informerà il precedente OdC.

6.12 – Certificazione di Organizzazioni "Multisite" basata sul campionamento

Il presente paragrafo è applicabile per Organizzazioni che svolgono attività simili in siti diversi, che hanno una sede centrale definita, in cui le attività sono pianificate, controllate e gestite e una rete di uffici o sedi locali, in cui le attività sono completamente o parzialmente svolte. I processi in tutti i siti devono essere dello stesso tipo ed essere svolti secondo metodi e procedure analoghi. Il SGSI deve essere gestito centralmente ed essere soggetto a riesame della direzione centrale.

Tutti i pertinenti siti (inclusa la funzione amministrativa centrale) devono essere soggetti al programma di audit interno e devono essere stati auditati prima dell'inizio del processo certificativo. L'Organizzazione deve dimostrare la sua abilità nel ricavare ed analizzare dati da tutti i siti (compresa la sede centrale) e deve inoltre dimostrare di avere autorità e capacità di attuare le necessarie modifiche, se del caso (p.e. dati provenienti da documentazione e modifiche di sistema, riesame della direzione, reclami, AC, audit interni e valutazione degli esiti, modifiche intervenute nei requisiti legislativi di riferimento).

Le dimensioni del campione da sottoporre ad audit di certificazione, sorveglianza e rinnovo sono determinate da RISK CONTROL ADVISORY, anche in funzione, per esempio, della complessità dell'attività svolta, della dimensione dei siti da sottoporre ad audit e dell'entità delle differenze che intervengono tra i diversi siti. Prima dell'emissione dell'offerta l'Organizzazione deve fornire ad RISK CONTROL ADVISORY tutte le informazioni necessarie per identificare le attività coperte dal SGSI e la loro complessità, comprese le peculiarità di ogni sito, in modo da permettere una puntuale identificazione del campione.

L'Organizzazione deve comunicare a RISK CONTROL ADVISORY, in fase di richiesta d'offerta, quali siti sono da includere nella certificazione e quali invece da escludere. Nel caso in cui emergano Non Conformità, in qualsiasi sito, anche durante un audit interno o un audit RISK CONTROL ADVISORY, l'Organizzazione deve effettuare opportune indagini per verificare se la stessa anomalia possa verificarsi anche in altri siti. Eventuali Azioni Correttive devono essere intraprese sia a livello centrale sia a livello locale e, comunque, deve essere dimostrata a RISK CONTROL ADVISORY l'effettuazione di opportune indagini in merito. RISK CONTROL ADVISORY chiede l'evidenza delle azioni intraprese dall'Organizzazione e può aumentare la frequenza e/o le dimensioni del campione per avere la certezza che il controllo sia stato ristabilito.

Nel caso in cui vi siano Non Conformità non risolte, la certificazione non sarà rilasciata ad alcun sito. Non sarà ammissibile escludere un sito in process, nel caso in cui nel sito siano state rilevate Non Conformità, come soluzione al problema.

I documenti relativi alla certificazione faranno esplicito riferimento alle attività svolte e ai siti certificati. Nel caso in cui si rilasci un singolo certificato per sito, lo stesso farà chiaro riferimento alla certificazione "multisite". Tutti i certificati saranno revocati nel caso in cui un sito qualsiasi non rispetti i requisiti necessari per il mantenimento della certificazione. L'Organizzazione si impegna a informare RISK CONTROL ADVISORY relativamente alla chiusura di un sito compreso nella certificazione. Nuovi siti possono essere aggiunti alla certificazione, in genere durante gli audit di sorveglianza o rinnovo, sempre nel rispetto delle regole sopra elencate. Il sito/gruppo di siti da aggiungere saranno considerati in modo analogo ad una certificazione iniziale.

I criteri per effettuare il campionamento saranno in parte selettivi e in parte casuali. Almeno il 25% del campione sarà scelto a caso. Si cercherà di scegliere un campione che possa comprendere le maggiori differenze possibili tra i vari siti nell'arco del periodo di validità della certificazione. La selezione dei siti terrà conto, ad esempio, dei risultati degli audit interni e dei riesami della direzione, di reclami, azioni correttive e preventive, variazioni significative delle dimensioni dei siti, modifiche nei turni di lavoro e nelle procedure, complessità del SGSI e dei processi, modifiche rispetto agli audit precedenti, maturità dell'SGSI e livello di conoscenza dell'Organizzazione, differenze culturali, di lingua e nei requisiti legislativi di riferimento, dispersione geografica. Il campione potrà essere individuato anche a valle dell'audit iniziale presso la sede centrale. In ogni caso alla sede centrale sarà comunicato il campione da sottoporre ad audit.

In generale, sempre nel rispetto delle regole sopra indicate, il numero minimo di siti da sottoporre ad audit è n½ (n=numero di siti) per la VIC, 0.6 n½ per la VPS e 0.8 n½ per la VRC. La sede centrale è sempre oggetto di audit. Il campione potrà essere comunque aumentato da RISK CONTROL ADVISORY in caso di siti di notevoli dimensioni, attività complesse, presenza di turni di lavoro, modifiche nelle attività, reclami, risultati di audit interni e riesami della direzione ed in ogni altro caso in cui RISK CONTROL ADVISORY ritenga possa esserci il rischio che la propria valutazione sulla conformità del SGSI non sia sufficiente valutando un numero di siti secondo la regola di cui sopra. Il numero di gg/uomo destinati alla verifica per ogni singolo sito sarà determinato in base a quanto previsto dal documento IAF MD5 in relazione al numero di addetti. Il numero totale di gg/uomo non potrà essere inferiore a quello calcolato sulla base del documento IAF MD5 nell'ipotesi in cui tutti gli addetti lavorassero in un singolo sito. Nel caso in cui l'Organizzazione intenda aggiungere un gruppo di siti alla certificazione, il gruppo stesso sarà considerato come un'Organizzazione "multisite" indipendente, per la determinazione del campione. A valle della certificazione del nuovo gruppo, lo stesso sarà cumulato al precedente per il calcolo del campione relativo a VPS e VRC.

Art. 7 - Sospensione della Certificazione

L'OdC può sospendere la validità della certificazione per un periodo di tempo determinato, quando si verificano situazioni indebite tra cui ad esempio:

- l'Organizzazione ha sospeso temporaneamente l'applicazione del SGSI;
- l'Organizzazione non consente l'esecuzione delle VPS o delle VSS o delle VRC;
- l'Organizzazione non si rende disponibile all'effettuazione di verifiche in accompagnamento con ispettori dell'Organismo di Accreditamento;

- non vengono attuate le azioni correttive a fronte delle non conformità rilevate;
- si verificano irregolarità nell'uso del Marchio e/o del Certificato dell'OdC o del marchio dell'Ente di Accreditamento dell'OdC;
- il Sistema di Gestione non garantisce il rispetto dei requisiti cogenti di prodotto e/o servizio;
- l'esistenza di problematiche aventi per oggetto i requisiti cogenti del prodotto / servizio erogato o del sistema di gestione interessato;
- la mancata comunicazione all'OdC di modifiche al proprio sistema di gestione;
- la mancata comunicazione all'OdC circa procedimenti giudiziari e/o amministrativi;
- la condanna dell'Organizzazione per fatti aventi ad oggetto il mancato rispetto dei requisiti cogenti pertinenti al sistema di gestione oggetto di certificazione;
- la mancata gestione di reclami o segnalazioni direttamente connesse con carenze del sistema di gestione certificato.
- l'Organizzazione non rispetti gli impegni finanziari assunti nei confronti dell'OdC.

Nel caso in cui l'Organizzazione chieda la sospensione della certificazione (per un periodo che non dovrebbe superare i 6 mesi), la Direzione RISK CONTROL ADVISORY, dopo avere approfondito le motivazioni, notifica all'Organizzazione mediante lettera raccomandata con R.R., anticipata via fax, ovvero tramite posta certificata (PEC), l'accettazione della richiesta e le condizioni alle quali la sospensione può esser revocata. Il provvedimento viene poi comunicato al Comitato Tecnico nella prima riunione utile.

Qualora si realizzi una delle condizioni a carattere amministrativo/gestionale di cui all'elenco sopra riportato, il provvedimento di sospensione viene deliberato dalla Direzione RISK CONTROL ADVISORY, sentito eventualmente il Comitato Tecnico qualificato con riferimento alle aree tecniche, anche convocato in riunione straordinaria.

Qualora si realizzi una delle condizioni a carattere tecnico di cui all'elenco sopra riportato, il provvedimento di sospensione viene deliberato dal Comitato Tecnico qualificato con riferimento alle aree tecniche, nella prima riunione utile, oppure convocato in riunione straordinaria.

In ogni caso la Direzione RISK CONTROL ADVISORY notifica all'Organizzazione mediante lettera raccomandata con R.R., anticipata via fax, ovvero tramite posta elettronica certificata (PEC), i motivi del provvedimento assunto, la durata della sospensione (anche in questo caso generalmente non superiore a 6 mesi) e le condizioni alle quali può esser revocata. In alcuni casi può essere mandato un telegramma.

Il provvedimento di sospensione entra in vigore alla data della raccomandata (o PEC).

La certificazione rilasciata e successivamente sospesa non può essere utilizzata in nessun caso (ad esempio partecipazione ad appalti pubblici) a partire dal giorno di avvenuta ricezione da parte dell'Organizzazione della Raccomandata con R.R., ovvero della posta certificata (PEC), inviata da RISK CONTROL ADVISORY.

L'Organizzazione accetta ed autorizza RISK CONTROL ADVISORY a rendere pubblico, attraverso il proprio sito web, l'eventuale provvedimento di sospensione comminato.

La sospensione sarà revocata soltanto dopo che l'OdC avrà accertato il soddisfacente ripristino della conformità ai requisiti specificati attraverso una VSS.

Il provvedimento di revoca della sospensione viene deliberato dalla Direzione RISK CONTROL ADVISORY nei casi a carattere amministrativo/gestionale oppure, per le casistiche tecniche sopra definite, dal Comitato Tecnico qualificato con riferimento alle aree tecniche, eventualmente convocato in riunione straordinaria. La revoca della sospensione ha decorrenza dalla data della comunicazione inviata via R.R. o tramite posta certificata (PEC).

Le spese relative alle verifiche supplementari conseguenti, presso la sede RISK CONTROL ADVISORY e/o presso la sede aziendale, sono a carico dell'Organizzazione.

Art. 8 – Revoca della certificazione

L'OdC revoca la certificazione nei casi in cui l'Organizzazione:

1. non abbia eliminato, nei modi e nei tempi stabiliti, le condizioni che hanno portato alla sospensione della certificazione;
2. sia inadempiente rispetto alle norme cogenti dei prodotti/servizi coperti da certificazione;
3. cessi le attività per le quali aveva ottenuto la certificazione del proprio SGSI;
4. sia messa in liquidazione o in amministrazione giudiziale o in amministrazione straordinaria o sia aperta a suo carico una procedura fallimentare;
5. abbia, a carico dei propri rappresentanti, sentenze definitive di condanna, passate in giudicato, per fatti aventi ad oggetto il mancato rispetto dei requisiti cogenti del sistema di gestione oggetto di certificazione;
6. non rispetti, dopo sollecito, gli impegni finanziari assunti nei confronti dell'OdC, nei termini indicati.

La decisione per la revoca della certificazione è presa dalla Direzione di RISK CONTROL ADVISORY oppure dal Comitato Tecnico qualificato con riferimento alle aree tecniche, eventualmente convocato in riunione straordinaria, in genere a seconda che le motivazioni siano di carattere amministrativo/legale oppure tecnico. Con la revoca della certificazione il contratto tra l'Organizzazione e RISK CONTROL ADVISORY si intende risolto.

La revoca della certificazione ha effetto dalla data di trasmissione della comunicazione, anticipata a mezzo fax, invita a mezzo raccomandata con R.R., ovvero tramite posta certificata (PEC), da parte della Direzione RISK CONTROL ADVISORY all'Organizzazione certificata.

La Direzione RISK CONTROL ADVISORY notifica all'Organizzazione nella comunicazione inviata, i motivi del provvedimento.

Alla revoca della certificazione l'Organizzazione deve pagare una penale pari all'80% dell'importo previsto per le attività del triennio in corso di validità del certificato.

La revoca della certificazione implica la cancellazione dell'Organizzazione dall'elenco delle società certificate; l'Organizzazione deve restituire all'OdC l'originale del certificato di conformità in suo possesso ed eliminare eventuali copie dello stesso, nonché cessare l'uso del marchio di certificazione, in ogni forma e modo.

L'Organizzazione accetta ed autorizza RISK CONTROL ADVISORY a rendere pubblico attraverso il proprio sito web, ed a trasmettere all'Organismo di Accreditamento, nonché ad altri Enti, se applicabile - ad esempio l'Autorità Nazionale Anticorruzione ANAC e le Società Organismo di Attestazione - l'eventuale provvedimento di revoca comminato.

L'OdC si riserva di richiedere risarcimento per eventuali danni subiti.

Art. 9 – Rinuncia

L'Organizzazione può rinunciare alla certificazione in proprio possesso, con raccomandata con R.R.:

- alla scadenza del periodo di validità del certificato, ante suo rinnovo e post seconda verifica di sorveglianza, dando formale disdetta del contratto entro i 30 gg solari successivi alla seconda verifica di sorveglianza del triennio;
- nei casi di variazioni contemplate all'art. 10;
- in qualsiasi altro momento, con il pagamento di una penale di recesso che è pari all'80% dell'importo previsto per le attività del triennio in corso di validità del certificato, previste dal contratto in corso di validità.

La certificazione rilasciata cessa la sua validità il giorno della scadenza riportato sul certificato, nel caso in cui la rinuncia avvenga dopo la seconda verifica di sorveglianza, oppure, negli altri casi, alla data prevista per l'effettuazione dell'audit di sorveglianza per il quale l'Organizzazione non risulta più disponibile.

L'Organizzazione accetta ed autorizza RISK CONTROL ADVISORY a rendere pubblico attraverso il proprio sito web, ed a trasmettere all'Organismo di Accreditamento, nonché ad altri Enti, se applicabile - ad esempio l'Autorità Nazionale Anticorruzione ANAC e le Società Organismo di Attestazione – l'avvenuta cessazione della validità del certificato.

Art. 10 – Modifiche ai requisiti per la certificazione

In caso di variazioni ai requisiti RISK CONTROL ADVISORY per la certificazione e/o al presente Regolamento, salvo quelle necessarie o relative agli aggiornamenti normativi o regolamentari, tra i quali in via non esaustiva quelli dei documenti di riferimento indicati all'art. 2, o correlate o conseguenti agli stessi, o le variazioni necessarie o relative al rispetto di regolamenti, direttive o adempimenti necessari e/od opportuni all'ottenimento o mantenimento dell'accreditamento da parte di RISK CONTROL ADVISORY, l'OdC ne darà comunicazione all'Organizzazione, indicando il tipo di variazione e la data entro la quale l'Organizzazione dovrà uniformarsi.

L'Organizzazione, in caso di non accettazione delle variazioni proposte potrà rinunciare alla certificazione, dandone comunicazione scritta all'OdC secondo le modalità previste all'art. 9, ossia con raccomandata con R.R. e con effetto dal giorno dell'avvenuta ricezione da parte di RISK CONTROL ADVISORY, alla sola condizione che tali variazioni siano sostanziali e rilevanti nel modificare lo schema di certificazione dell'OdC e/o il presente Regolamento e risultino per l'Organizzazione sostanziali ed eccessivamente onerose comportando modifiche rilevanti nel sistema di gestione e nell'operatività ordinaria dell'azienda.

Eventuali costi per attività di valutazione derivanti dalle sopraccitate variazioni saranno a carico dell'Organizzazione valutata.

RISK CONTROL ADVISORY verifica che ogni cliente si conformi ai nuovi requisiti, in genere nel corso della successiva verifica ispettiva, in altri casi mediante richiesta di trasmissione di evidenze documentale e/o verifiche ispettive supplementari.

Art. 11 – Responsabilità ed Obblighi

11.1 - Requisiti cogenti connessi al sistema di gestione e limiti dei relativi controlli.

La certificazione del SGSI non solleva l'Organizzazione dalle proprie responsabilità verso i clienti ed i terzi in generale né dall'osservanza, per l'espletamento delle sue attività per la conformità dei beni e servizi forniti, dalle disposizioni che derivano da Leggi o altri atti aventi forza di legge (quali Direttive e Regolamenti), o da norme tecniche, vincoli e/o accordi contrattuali applicabili.

La certificazione riguarda solo la conformità del sistema di gestione dell'Organizzazione alla norma di riferimento e non costituisce pertanto un attestato del rispetto dei predetti requisiti cogenti.

L'Odc ha la responsabilità di verificare, sulla base di un campionamento commisurato ai tempi di audit, che l'Organizzazione conosca e sia in grado di gestire tutti gli aspetti cogenti connessi al sistema dì gestione oggetto della certificazione.

L'Organizzazione rimane pertanto l'unica responsabile dell'osservanza delle disposizioni legislative in vigore relative all'Organizzazione stessa e/o ai prodotti / servizi erogati, con esclusione di qualsiasi responsabilità od obbligo di garanzia da parte dell'OdC.

11.2 – Obbligo di informazione su eventuali procedimenti giudiziari e/o amministrativi in corso

Nel caso giungano ad RISK CONTROL ADVISORY informazioni ufficiali circa coinvolgimenti in procedimenti giudiziari conseguenti alle leggi sulle responsabilità da prodotto o violazioni di leggi concernenti i prodotti forniti e/o servizi erogati e comunque afferenti al sistema oggetto di certificazione, la Direzione provvederà a trasmettere in via ufficiale tale informazione al Comitato Tecnico nonché all'Ente di accreditamento per quanto di competenza.

L'Organizzazione si impegna inoltre a comunicare tempestivamente all'OdC tutte le situazioni difformi rilevate dall'Autorità di Controllo, nonché eventuali sospensioni o revoche di autorizzazioni, concessioni, ecc, relative alla produzione/ erogazione di prodotti/ servizi connessi alla certificazione.

Inoltre, deve comunicare immediatamente all'OdC eventuali procedimenti giudiziari e/o amministrativi in corso, riguardanti l'oggetto della certificazione, fatti salvi i limiti imposti dalla Legge. L'Organizzazione deve costantemente informare l'OdC sull'evolversi di tali situazioni.

11.3 – Clausola di limitazione di responsabilità

L'Organizzazione si impegna a garantire la completezza e veridicità dei documenti e delle informazioni messe a disposizione del GVI incaricato.

L'OdC è espressamente esonerato da ogni responsabilità in caso di mancata o incompleta comunicazione di dati, come pure nel caso gli stessi non corrispondano alla reale situazione aziendale.

Nel caso in cui venissero meno i requisiti in capo ad RISK CONTROL ADVISORY per il rilascio delle certificazioni, RISK CONTROL ADVISORY darà pronta comunicazione alle Organizzazioni clienti. Le Parti concordano espressamente che RISK CONTROL ADVISORY risponderà per l'eventuale risarcimento dei danni in favore dell'Organizzazione cliente, e solo a seguito di pronuncia ai sensi dell'art. 16, nel limite delle somme previste, a carico del cliente, per le annuali verifiche di sorveglianza.

11.4 – Obbligo di mantenimento della conformità ai requisiti del Sistema di Gestione ed eventuali modifiche

L'organizzazione certificata si impegna a mantenere la propria struttura conforme ai requisiti richiesti dalle norme precisate nel certificato, durante l'intero periodo di validità della certificazione.

In caso di modifiche relative a:

- aspetti legali, commerciali, organizzativi o relativi alla proprietà;
- organizzazione e direzione (per esempio dirigenti con ruoli chiave, personale con potere decisionale o personale tecnico);
- indirizzi di contatto e siti;
- campo di applicazione delle attività dell'organizzazione comprese nel sistema di gestione certificato;
- modifiche significative del sistema di gestione e dei processi;

dovrà esserne data preventiva comunicazione scritta ad RISK CONTROL ADVISORY, che può accettare le variazioni o predisporre l'effettuazione di una verifica di sorveglianza supplementare.

In particolare, nel caso in cui l'Organizzazione intenda modificare il campo di validità della certificazione (scopo di certificazione), deve farne richiesta scritta all'OdC; in relazione alle variazioni richieste RISK CONTROL ADVISORY valuterà la necessità di effettuare una Verifica di Sorveglianza Supplementare.

Art. 12 - Gestione del marchio di certificazione, del certificato di conformità e delle informazioni relative alla certificazione

12.1 – Autorizzazione

In riferimento alla comunicazione di rilascio della certificazione di conformità alla Norma ISO 27001 e nel corso del periodo di validità della stessa certificazione, l'Organizzazione è autorizzata ad utilizzare il marchio di certificazione, il certificato di conformità di proprietà dell'OdC e le informazioni relative alla certificazione nei modi e alle condizioni descritte nei punti che seguono. Il certificato ed il file contenente il marchio di certificazione da utilizzare sono inviati all'Organizzazione a valle della decisione positiva del Comitato Tecnico RISK CONTROL ADVISORY e nel caso in cui non vi siano fatture amministrative in sospeso.

12.2 – Caratteristiche del marchio di certificazione

L'utilizzo del marchio è facoltativo; tuttavia, qualora l'Organizzazione certificata desideri avvalersi di tale facoltà, essa dovrà utilizzare il marchio secondo specifiche che seguono.

Il marchio di certificazione, richiama il logo Aziendale di RISK CONTROL ADVISORY, che può essere usato solamente da RISK CONTROL ADVISORY.

Il logo aziendale RISK CONTROL ADVISORY è costituito dai seguenti elementi:

il Logo (scritta RCA in forma circolare), i cerchi, il nome nel cerchio esterno "Risk Control Advisory" sul lato superiore e "Inspection and Certification" sul lato inferiore con 2 punti in mezzo.

Logo RISK CONTROL ADVISORY

La successiva figura 1 rappresenta il Marchio RISK CONTROL ADVISORY per le Organizzazioni certificate ISO/IEC 27001.

Figura 1

RISK CONTROL ADVISORY
ISO/IEC 27001
INFORMATION SECURITY MANAGEMENT SYSTEM

Per il dettaglio relativo all'abbinamento tra il marchio di certificazione RISK CONTROL ADVISORY e il marchio dell'Organismo di Accreditamento, che l'Organizzazione può utilizzare nel caso in cui RISK CONTROL ADVISORY abbia l'accreditamento nello specifico settore IAF, deve essere rispettato quanto definito nel regolamento di utilizzo del marchio presente nel sito dell'Organismo di Accreditamento, in ogni momento nella versione aggiornata, oltre a quanto definito nel presente articolo.

Per applicazioni di carattere documentale e su web può essere utilizzato soltanto il Marchio contenuto nell'apposito file trasmesso da RISK CONTROL ADVISORY a valle della certificazione all'Organizzazione certificata: il Marchio può essere ridotto, nel rispetto delle esigenze di leggibilità e mantenendo il rapporto delle dimensioni. Parimenti, per applicazioni su "oggetti" di grandi dimensioni, il Marchio può essere ingrandito, sempre mantenendo il rapporto delle dimensioni.

La sorveglianza sulla corretta conformazione del marchio di certificazione RISK CONTROL ADVISORY e del marchio dell'Ente di accreditamento nonché sul loro corretto utilizzo viene effettuata da RISK CONTROL ADVISORY sia attraverso le verifiche di sorveglianza sia attraverso documenti e/o informazioni documentali reperite sul mercato.

12.3 – Utilizzo del marchio di certificazione, del certificato e delle informazioni relative alla certificazione

Il marchio può essere utilizzato, abbinato alla Ragione Sociale/marchio dell'Organizzazione certificata su carta intestata, cancelleria, materiale pubblicitario e promozionale, ma non può essere utilizzato su prodotti o sugli imballaggi dei prodotti, né applicato in modo tale che possa essere scambiato per una certificazione di prodotto o che possa intendersi esteso ad altri schemi o sistemi non rientranti nella certificazione di conformità rilasciata da RISK CONTROL ADVISORY. Il marchio RISK CONTROL ADVISORY non può essere apposto su rapporti o certificati di prova, taratura o ispezione.

E' fondamentale che la certificazione di sistema non sia confusa con una certificazione di prodotto, e che non sia estesa ad altri siti che non rientrano nello scopo della certificazione rilasciata. Non ci devono essere ambiguità nei marchi e nei testi che li accompagnano, relativamente o cosa è stato certificato e quale organismo abbia rilasciato la certificazione.

Il Certificato di Conformità può essere utilizzato dall'Organizzazione certificata con finalità informative, purché riprodotto fedelmente in tutte le sue parti; può essere ingrandito o ridotto in modo uniforme purché il contenuto rimanga leggibile e non risultino alterati i contorni e i contenuti.

L'Organizzazione certificata deve assicurare che l'utilizzo del marchio e del certificato sia sufficiente per una corretta informativa verso terzi inerente le proprie attività realmente coperte dalla certificazione ottenuta.

Revisioni del certificato di conformità, originate da qualsiasi tipo di modifica – p.e. della revisione della norma di riferimento, della ragione sociale, ecc. – saranno fatturate in ragione di 100 € + IVA o come diversamente specificato nell'offerta RISK CONTROL ADVISORY o in altro documento. Anche eventuali comunicazioni riguardanti la validità del certificato o lo status dell'iter certificativo saranno fatturate in egual misura.

L'Organizzazione certificata non deve inoltre fare, né consentire, affermazioni che possano trarre in inganno riguardo la propria certificazione.

Le dichiarazioni apposte sull'imballaggio di un prodotto (ciò che può essere rimosso senza che il prodotto venga danneggiato o disintegrato) o all'interno delle informazioni di accompagnamento (ciò che è disponibile separatamente ovvero facilmente separabile) non devono sottintendere in alcun modo che il prodotto, processo o servizio sia certificato, e devono comprendere riferimenti a: identificazione del cliente certificato, tipo di sistema di gestione certificato e norma applicabile, organismo di certificazione che ha emesso il certificato.

12.4 – Uso non corretto del marchio di certificazione e/o del certificato di conformità ed informazioni fornite

Nel caso si verifichi un uso non corretto del marchio di certificazione, del marchio dell'Ente di accreditamento e/o del certificato di conformità e si forniscano informazioni non corrette, cioè qualora il cliente certificato:

- non si conformi ai requisiti RISK CONTROL ADVISORY nel fare riferimento allo stato della propria certificazione nei mezzi di comunicazione quali Internet, opuscoli o materiale pubblicitario o altri documenti;
- faccia, o consenta, affermazioni che possano trarre in inganno riguardo la propria certificazione;
- utilizzi, o consenta l'utilizzo ingannevole, di un documento di certificazione, di qualche sua parte, o dei rapporti di audit;
- non interrompa l'utilizzo di tutti i materiali pubblicitari che fanno riferimento alla certificazione, nel caso di revoca della certificazione;
- non rettifichi tutti i materiali pubblicitari qualora il campo di applicazione della certificazione sia stato ridotto;
- consenta che i riferimenti alla certificazione del suo sistema di gestione siano utilizzati in modo tale da far intendere che RISK CONTROL ADVISORY certifichi un prodotto (compreso un servizio) o un processo;

- lasci intendere che la certificazione si applichi ad attività e siti che siano al di fuori del campo di applicazione della certificazione;
- utilizzi la propria certificazione in modo tale da poter discreditare l'organismo di certificazione e/o il sistema di certificazione e compromettere la fiducia del pubblico;

oppure qualora il marchio sia utilizzato sui prodotti, sugli imballi, sul nastro adesivo, su schede tecniche di prodotto, su certificati di laboratorio ecc., RISK CONTROL ADVISORY dovrà adottare nei confronti dell'Organizzazione certificata i provvedimenti ritenuti idonei per proteggere l'integrità della propria immagine nonché salvaguardare le organizzazioni e/o le persone che possono essere indotte in errore a causa dell'impiego non corretto dei documenti di cui sopra o delle informazioni non corrette fornite.

12.5 – Azioni correttive in caso di uso non corretto del marchio e/o del certificato e/o in caso di relative informazioni non corrette

In seguito ad uso non corretto del marchio di certificazione, del marchio dell'Ente di accreditamento e/o del certificato di conformità, RISK CONTROL ADVISORY richiede all'Organizzazione adeguate azioni correttive che consentano il ripristino di un uso conforme degli stessi.

In ogni caso, le azioni correttive saranno definite avuto riguardo al tipo di impiego non corretto ed alle sue conseguenze; azioni legali potranno essere intraprese qualora il marchio e/o il certificato siano utilizzati non conformemente agli accordi contrattuali.

Le azioni correttive richieste da RISK CONTROL ADVISORY dovranno essere immediatamente attuate dall'Organizzazione.

12.6 – Sospensione della certificazione in caso di uso non corretto del marchio e/o del certificato e/o in caso di relative informazioni non corrette

Nel caso in cui l'uso non corretto del marchio di certificazione e/o del certificato di conformità abbia portato discredito all'immagine dell'OdC, RISK CONTROL ADVISORY può sospendere la certificazione rilasciata all'Organizzazione e richiedere il risarcimento di eventuali danni. La notifica della sospensione sarà inviata all'Organizzazione certificata a mezzo di lettera raccomandata ed in copia all'Organismo di Accreditamento, se il certificato rilasciato è sotto accreditamento.

La sospensione della certificazione potrà essere decisa dall'OdC anche nel caso in cui l'Organizzazione rifiuti di attuare le azioni correttive richieste a seguito di un uso improprio o non corretto del marchio di certificazione e/o del certificato di conformità.

Art. 13 – Protezione dei dati personali

In ottemperanza alla legislazione applicabile in materia di protezione dei dati personali, il "preventivo consenso informato" da parte dell'Organizzazione è condizione essenziale per l'OdC al fine di dare esecuzione al rapporto contrattuale ed alle correlate attività valutative e certificative. RISK CONTROL ADVISORY garantisce la più completa riservatezza e cura dei dati cui verrà in possesso, che saranno trattati secondo la vigente normativa sulla privacy.

In particolare, RISK CONTROL ADVISORY garantisce al cliente che:

- Titolare dei dati è RISK CONTROL ADVISORY.
- Nell'espletamento del servizio, possono venire a conoscenza dei dati dipendenti e/o collaboratori di volta in volta interessati o coinvolti nell'ambito delle rispettive mansioni, conformemente alle istruzioni ricevute. La lista dei Responsabili in essere è costantemente aggiornata, che potrà essere comunicata, unitamente ad informazioni più dettagliate, sui soggetti che possono venire a conoscenza dei dati, in qualità di incaricati, su specifica richiesta alla sede RISK CONTROL ADVISORY.
- I dati affidati non saranno ceduti o comunicati a terzi, ovvero Organizzazioni, entità giuridiche, persone fisiche che non collaborano con RISK CONTROL ADVISORY e che quindi non abbiano firmato con la stessa un contratto per la riservatezza delle informazioni dei Clienti. Il trattamento dei dati sarà pertanto affidato esclusivamente a personale interno o esterno che abbia sottoscritto con la direzione di RISK CONTROL ADVISORY impegno per garantirne la riservatezza (gentlemen's agreement).

- I sistemi informativi di RISK CONTROL ADVISORY sono adeguatamente protetti da intrusioni esterne nonché da quelle interne. Tutti i sistemi sono a norma di legge per quanto concerne l'adeguamento al testo unico sulla privacy.
- È data piena e completa facoltà al Cliente di richiedere l'immediata cancellazione e/o distruzione dei dati personali ad eccezione di quelli che RISK CONTROL ADVISORY è obbligata a mantenere per legge (documentazione fiscale – cartacea ed elettronica). In caso di cancellazione, RISK CONTROL ADVISORY sarà impossibilitata ad espletare qualsiasi attività, qualora questa richiesta avvenga durante l'erogazione del servizio, RISK CONTROL ADVISORY interromperà le attività in corso, riservandosi la possibilità di richiedere all'Organizzazione l'intera somma pattuita nel contratto/offerta.
- L'utilizzo dei dati personali per l'invio di documentazione commerciale sarà effettuato solo ed esclusivamente senza l'ausilio di sistemi automatici, con la possibilità immediata che tali invii siano immediatamente sospesi.
- È disponibile a richiesta l'informativa completa ed estesa sui dati personali. Tale informativa verrà rilasciata in caso di firma del contratto per la fornitura dei servizi o dietro semplice richiesta da parte del Cliente o potenziale Cliente.

L'Organizzazione, informata di cui sopra, con la sottoscrizione del presente Regolamento, autorizza RISK CONTROL ADVISORY a trattare i dati di cui al successivo elenco puntato come informazioni riservate, in conformità alla propria politica di protezione dei dati, ed in particolare a:

1. Trattare i dati personali ed eventualmente i dati sensibili o giudiziari che saranno necessari per l'erogazione del servizio;
2. Trattare i dati personali ed eventualmente i dati sensibili o giudiziari mediante l'ausilio di tecnologie informatiche protette;
3. Utilizzare sistemi di comunicazione con il cliente per l'invio di informative anche a carattere commerciale;
4. Rendere pubblici i provvedimenti di certificazione e gli eventuali provvedimenti di sospensione e/o revoca della certificazione stessa;
5. Comunicare, quando previsto, ad altri Enti istituzionali gli eventuali provvedimenti di revoca della certificazione;
6. Informare chiunque lo richieda relativamente allo stato di validità della certificazione (per esempio se la certificazione è sospesa, revocata o ridotta);
7. Fornire, su richiesta, informazioni sul nome, sui documenti normativi correlati, sul campo di applicazione e sulla posizione geografica (città e Paese) relativamente alla certificazione dell'Organizzazione stessa;
8. Trattare le informazioni riguardanti il cliente provenienti da fonti diverse dal cliente stesso (p.e. da chi presenta un reclamo, da autorità in ambito legislativo).

Art. 14 – Reclami

L'Organizzazione può presentare reclamo, in forma verbale o scritta, avente per oggetto i suoi rapporti contrattuali con l'OdC. Tale reclamo può scaturire da inconvenienti verificatisi nel corso dell'iter di certificazione, quali, ad esempio, ritardi nell'espletamento delle varie fasi o comportamenti ritenuti non corretti da parte di ispettori o del personale dell'OdC. Reclami possono essere presentati ad RISK CONTROL ADVISORY anche da clienti di Organizzazioni certificate RISK CONTROL ADVISORY o da terze parti nei confronti delle Organizzazioni stesse.

L'OdC provvede a registrare i reclami (confermandone al reclamante la ricezione, entro 5 gg lavorativi dalla stessa), ad analizzarli e ad informare il reclamante entro 30 (trenta) giorni, in merito alle azioni scaturite.

La presentazione dei reclami, il loro esame e le relative decisioni non danno luogo ad alcuna azione di natura discriminatoria nei confronti di chi ha presentato il reclamo.

Art. 15 – Ricorsi

Il ricorso scaturisce dal dissenso dell'Organizzazione nei confronti di una decisione presa dall'OdC nell'ambito dell'iter certificativo.

Il ricorso deve pervenire all'OdC in forma scritta entro 30 giorni dalla data del documento a cui è riferito e deve contenere gli estremi del ricorrente, l'indicazione dell'atto contro cui viene presentato e la motivazione, supportata da evidenze documentali se esistenti. RISK CONTROL ADVISORY conferma per iscritto la ricezione del ricorso entro 5 gg lavorativi, entro 30 giorni fornisce rapporti sui risultati e, quando applicabile, sullo stato di avanzamento.

Le decisioni relative al ricorso sono prese, riesaminate e approvate dalla direzione RISK CONTROL ADVISORY e comunque non da soggetti coinvolti nei contenuti del ricorso, i quali sono comunque consultati. Qualora l'esito del ricorso non sia accettato dall'Organizzazione, la controversia sarà trattata da una Commissione costituita da un rappresentante dell'OdC, da un rappresentante dell'Organizzazione e da un terzo soggetto, con funzione di Presidente, nominato di comune accordo dai precedenti due al fine di riesaminare il ricorso e di pervenire ad una soluzione amichevole della controversia stessa.

La presentazione dei ricorsi, il loro riesame e le relative decisioni, non daranno luogo, da parte di RISK CONTROL ADVISORY, a qualsiasi azione di natura discriminatoria nei confronti di chi ha presentato ricorso.

Art. 16 – Contenziosi

Tutte le controversie non risolte con l'applicazione dell'art. 15 potranno essere deferite alla decisione di un Arbitro Unico da nominarsi in conformità al Regolamento della Camera Arbitrale Nazionale di Milano - Italia.

Le Parti espressamente dichiarano di conoscere ed accettare il citato Regolamento Arbitrale Nazionale. L'Arbitro Unico decide in via rituale secondo equità, nel rispetto delle norme inderogabili del Codice di Procedura Civile (art. 816 e seguenti CPC).

Le spese sono a carico della Parte soccombente nella misura dell'80%.

Per accettazione, del presente Regolamento e delle sue modifiche e/o integrazioni, per il reperimento delle quali l'Organizzazione si impegna a consultare periodicamente il sito www.rcacert.com:

*Data:*_____*Timbro e Firma del Legale Rappresentante:* _____