VERIFICA: GIOVANNI ZANVETTOR **APPROVA**: CARMINE CERRUTI

REV	NOTE DI MODIFICA	DATA
0	Prima emissione	30.08.2021
1	Correzioni/integrazioni audit ACCREDIA agosto 2021 per gli schemi ISO 37001 e ISO 22301 Modificati i Par. 4 -5.1 – 5.5 – 7.1	16.12.2021

QUESTO DOCUMENTO È DISTRIBUITO			
	COPIA CONTROLLATA		COPIA NON CONTROLLATA
DESTINATARIO			

INDICE

1. Scopo e Validità

Scopo del presente Regolamento Tecnico è definire e stabilire l'iter e le regole per la gestione, il rilascio, la sorveglianza della Certificazione dei Sistemi di Gestione per la Prevenzione della Corruzione" (SGPC).

Il presente documento è da considerarsi supplementare, e quindi non sostitutivo, a quanto definito nel "Regolamento Certificazione Sistemi di Gestione SGSI, SMS, SGPC e SGCO (ISO 27001, ISO 20000, ISO 37001 e ISO 22301) Parte 1 – Requisiti Generali".

Ai fini dell'accettazione del presente Regolamento è necessario che il Legale Rappresentante dell'Organizzazione firmi l'apposita parte prevista sull'offerta economica e, nel caso di offerta emessa dal Business Partner, sul contratto, anche mediante l'utilizzo della propria firma elettronica.

2. Modifiche del presente Regolamento

Eventuali variazioni delle norme di riferimento, delle prescrizioni degli Organismi di Accreditamento, del presente Regolamento, saranno comunicate da SI Cert all'Organizzazione certificata, che avrà la facoltà di adeguarsi alle nuove prescrizioni entro i tempi e con le modalità definiti nella comunicazione o di rinunciare alla Certificazione in accordo con quanto previsto nel "Regolamento Certificazione Sistemi di Gestione SGSI, SMS, SGPC e SGCO (ISO 27001, ISO 20000, ISO 37001 e ISO 22301) Parte 1 – Requisiti Generali".

Qualora l'Organizzazione certificata non rifiuti formalmente di adeguarsi, le nuove prescrizioni si intenderanno accettate. L'eventuale rifiuto deve essere comunicato ed inviato per iscritto con conferma di ricezione (o a mezzo PEC) entro quindici giorni dal ricevimento della comunicazione delle variazioni.

Eventuali variazioni del presente regolamento entreranno in vigore secondo una procedura che preveda tempi e modalità tali da garantire l'imparzialità.

SI Cert, nel caso di variazioni delle norme di riferimento, si riserva il diritto di verificare la conformità dell'adeguatezza dell'Organizzazione alle nuove prescrizioni della normativa attraverso un Audit.

3. Definizioni, Acronimi e Sinonimi

Le definizioni utilizzate dal presente Regolamento sono quelle riportate nelle norme di riferimento.

In generale nel proseguo del presente documento saranno usati questi Acronimi e Sigle:

- SGPC (ABMS): acronimo di Sistema di Gestione per la Prevenzione della Corruzione (Anti-bribery management systems)
- SI Cert: sinonimo di SI CERT ITALI srl
- OdA: acronimo di Organismi di Accreditamento o Organismo di Accreditamento
- Sistema di Certificazione: sinonimo di certificazione del sistema di gestione, certificazione di prodotto/Servizio, certificazione di Processo
- EA: Acronimo di European co-operation for Accreditation, è un'associazione senza scopo di lucro, registrata nei Paesi Bassi. È formalmente nominato dalla Commissione europea nel regolamento (CE) n. 765/2008 per sviluppare e mantenere un accordo multilaterale di riconoscimento reciproco, l'EA MLA, basato su un'infrastruttura di accreditamento armonizzata.
- IAF: acronimo di International Accreditation Forum è l'associazione mondiale che raggruppa gli organismi che svolgono l'accreditamento della valutazione di conformità e altri organismi interessati alla valutazione di conformità per quanto riguarda sistemi di gestione, prodotti, servizi, risorse umane ed altri ambiti similari.

Laddove necessario, ai fini di una migliore comprensione del presente Regolamento, talune altre definizioni o significati di alcuni termini e/o locuzione, sono riportate contestualmente all'utilizzo del termine o della locuzione stessa.

4. Campo di Applicazione

Il campo di applicazione del presente Regolamento si riferisce alla certificazione dei Sistemi di Gestione per la Prevenzione della Corruzione secondo la norma:

UNI ISO 37001 Sistema di Gestione per la Prevenzione della Corruzione

e la relativa Circolare Accredia:

Circolare Tecnica n. 28/2017 - Dipartimento Certificazione e Ispezione Informativa in merito all'accreditamento per lo schema di certificazione ISO 37001

UNI CEI EN ISO/IEC 17021-1 "Valutazione della conformità – Requisiti per gli organismi che forniscono Audit e certificazione di sistemi di gestione – Parte 1: Requisiti"

Linee Guide IAF MD 05

nelle edizioni correnti e descrive le procedure applicate da SI Cert per la Certificazione dei SGPC.

La certificazione ISO 37001 può essere richiesta da qualunque tipo di organizzazione, di qualsiasi dimensione e/o natura. Non sono ammesse esclusioni di processi/funzioni svolti in una stessa nazione.

La certificazione è rilasciata ad una sola entità giuridica e comprende tutti i siti, filiali, sedi secondarie, attività e processi effettivamente svolti dall'organizzazione.

È possibile però limitare l'applicazione a specifiche Nazioni, ma il campo di applicazione deve sempre includere processi ed attività sensibili svolti all'estero sotto la responsabilità ed il diretto controllo dell'organizzazione (elenco non esaustivo di attività e processi sensibili: finanza e controllo, commerciale, agenti e rete vendita, approvvigionamento, figure istituzionali ed organi sociali, uffici di direzione e CdA, internal auditing, gestione licenze, gare e autorizzazioni, gestione risorse umane - compreso gestione, selezione, assunzioni e avanzamenti di carriera - amministrazione e gestione cassa, acquisti, gestione omaggi e liberalità, relazioni con autorità istituzionali ed enti di controllo, gestione patrocini e sponsor, gestione contenziosi e reclami, servizi informatici, gestione security, attività di controllo e collaudi). Questo aspetto dovrà essere ben esplicitato nel certificato.

Nel caso di gruppi di società, quando attività/processi sensibili siano svolti da altre società del gruppo (capogruppo e/o controllate), anche all'estero, si applica il paragrafo 8.5. della UNI ISO 37001.

I criteri per la formulazione dello scopo del certificato sono gli stessi già applicati per la ISO 9001, con particolare attenzione alle attività svolte.

Poichè i tempi di audit sono influenzati dal livello di rischio dell'organizzazione, ai fini della sua identificazione, è necessario che l'Organizzazione fornisca puntuali informazioni attraverso l'utilizzo del Modulo Richiesta di Offerta Generale.

5. GENERALITA'

5.1. REQUISITI PER LA CERTIFICAZIONE

La certificazione ISO 37001 può essere richiesta da qualunque tipo di organizzazione, di qualsiasi dimensione o natura.

La certificazione viene rilasciata ad una sola entità giuridica e comprende tutti i siti, filiali, sedi secondarie, attività e processi effettivamente svolti dall'organizzazione.

Non sono ammesse esclusioni a processi / funzioni svolte in una stessa Nazione.

È possibile però limitare l'applicazione a specifiche Nazioni, ma il campo di applicazione deve sempre includere processi e attività sensibili1 svolti all'estero quando svolti sotto la responsabilità e il diretto controllo dell'organizzazione (es. uffici di rappresentanza o sedi secondarie agenti o mediatori). Questo aspetto deve essere ben esplicitato nel certificato. Nel caso di gruppi di società, quando attività/processi sensibili siano svolti da altre società del gruppo (capogruppo e/o controllate), anche all'estero, si applica il paragrafo 8.5.della UNI ISO 37001.

La conformità ai requisiti di modelli e sistemi di prevenzione previsti da norme di legge (es. Modelli Organizzativi ai sensi del D.Lgs. 231/2001, PTPC ai sensi della L. 190/2012 e simili) non è certificabile sotto accreditamento.

L'Organizzazione richiedente la Certificazione deve:

a) avere un Sistema di Gestione per la Prevenzione della Corruzione attivo da almeno tre mesi che rispetti i requisiti della normativa di riferimento e delle eventuali prescrizioni particolari stabilite di legge per tipologia di prodotto/processo/servizio incluso nel campo di applicazione;
b) Dare informazioni complete e dettagliate nel Modello Richiesta di offerta in modo da poter avere un contesto attendibile del richiedente Elenco di attività e processi sensibili e il personale a rischio corruzione, comunicazioni eventuali reati, ecc.
c) avere effettuato un ciclo completo di Verifiche Ispettive Interne ed un Riesame di Direzione;
d) mantenere a disposizione di SI Cert le registrazioni di tutti i reclami ricevuti e delle relative azioni conseguenti;
e) mantenere aggiornata la raccolta delle norme, leggi e regolamenti cogenti applicabili all'attività, processo, servizio, prodotto incluso nel campo di applicazione della Certificazione.

SI Cert Italy emetterà l'offerta commerciale in base ai dati comunicati dall'organizzazione riportati nel modello Richiesta di certificazione in conformità alle normative vigenti richiamate al paragrafo 4. Nel corso delle attività di verifica, il Gruppo di Audit verificherà la congruenza dei dati comunicati dall'organizzazione (addetti corruzione, equivalenti, eventuali reati, ecc.) se dovesse emergere una difformità, SI Cert Italy procederà con il riesame dell'offerta ed eventualmente con una modifica contrattuale.

5.2. EMISSIONE E VALIDITÀ DEL CERTIFICATO

Il Certificato è emesso a fronte del completamento, con esito positivo, dell'Audit Iniziale; il mantenimento della sua validità è subordinato al superamento degli Audit di Sorveglianza periodici annuali e ad una completa rivalutazione (Audit di Rinnovo) ogni 3 anni entro il termine della scadenza.

5.3. OBBLIGHI DELL'ORGANIZZAZIONE (ALTRE INFORMAZIONI)

Un'organizzazione certificata o in certificazione deve informare tempestivamente SI Cert nel momento in cui fosse coinvolta in qualche situazione critica tale da compromettere la garanzia della certificazione del sistema (esempio notizie di pubblico interesse, crisi o coinvolgimento in qualche procedimento giudiziario per fenomeni corruttivi o simili).

Altrettanto l'organizzazione dovrà fare in caso di qualunque evento relativo a fenomeni di corruzione che possa aver coinvolto una o più delle proprie Risorse Umane, e le conseguenti azioni adottate per il contenimento degli effetti di tale evento, l'analisi delle cause radice, le relative azioni correttive.

Nel caso in cui SI Cert venisse a sapere, direttamente dall'organizzazione o da altre fonti, che la stessa organizzazione è implicata con dei profili di responsabilità in qualche scandalo o in qualche procedimento giudiziario per fenomeni corruttivi, condurrà tempestivamente delle valutazioni / approfondimenti specifici, valutando l'opportunità di dare notizia al mercato del fatto che tale organizzazione è "soggetta a valutazione per gli specifici eventi" (fatti salvi gli obblighi di legge e dei mercati regolamentati – per esempio borsa).

Finita l'analisi, saranno adottati i consueti provvedimenti del caso (per esempio chiusura della valutazione con archiviazione, adozione dei provvedimenti previsti dai regolamenti di certificazione, rafforzamento della attività ispettive), definiti in funzione dell'adeguatezza della risposta e delle strategie adottate dall'organizzazione.

5.4. SUBENTRO AD ALTRO ENTE

Qualora la richiesta di Certificazione provenga da Organizzazioni già certificate e con Certificato in corso di validità, SI Cert subentra nelle attività in accordo con quanto previsto nel Regolamento Certificazione Sistemi di Gestione SGSI, SMS, SGPC e SGCO (ISO 27001, ISO 20000, ISO 37001 e ISO 22301) Parte 1 – Requisiti Generali.

5.5. MODALITÀ DI CONDUZIONE DEGLI AUDIT

Gli Audit preferibilmente debbono essere condotti "in campo" (ossia presso la sede dell'Organizzazione), ma, se la situazione lo richiede, possono essere eseguiti in toto o in parte da remoto in accordo con quanto già previsto nel relativo paragrafo del Regolamento Certificazione Sistemi di Gestione SGSI, SMS, SGPC e SGCO (ISO 27001, ISO 20000, ISO 37001 e ISO 22301) Parte 1 – Requisiti Generali.

Prima dell'esecuzione di ogni Audit, SI Cert comunica all'Organizzazione i nomi del Gruppo di Audit che condurrà la valutazione e nello stesso momento indica l'eventuale documentazione che dovrà essere resa disponibile al Gruppo.

L'Organizzazione per la corretta esecuzione dell'Audit deve assicurare la presenza del Personale avente responsabilità per le Aree/Funzioni oggetto di Audit che hanno rilevanza nell'efficace funzionamento dei processi e delle attività rilevanti del Sistema stesso.

Per ogni Audit sono previste:

- una riunione iniziale tra il Gruppo di Audit e l'Organizzazione finalizzata alla presentazione delle parti ed all'illustrazione delle procedure di Audit;
- l'Audit in campo ed a campione della conformità del Sistema di Gestione dell'Organizzazione 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 di chiusura tra il Gruppo di Audit e l'Organizzazione per illustrare l'esito della verifica e consegnare l'Audit Report.

Durante la riunione di chiusura, ove lo ritenesse necessario, l'Organizzazione può confrontarsi con il GA sui contenuti del documento, sul prosieguo delle attività e sulle azioni da intraprendere. Alla riunione di chiusura per conto dell'Organizzazione deve essere sempre presente la Direzione e tutti i Responsabili di Area/Funzione/Processo che hanno rilevanza nell'efficace funzionamento dei processi e delle attività rilevanti del Sistema stesso.

Il contenuto della registrazione dell'Audit lasciata dal GA è da considerarsi come comunicazione ufficiale dei risultati dell'Audit da parte della Direzione di SI Cert (a meno che la stessa non faccia pervenire comunicazioni contrarie entro il termine temporale indicato sul documento stesso).

L'Organizzazione, entro il giorno successivo al termine delle attività di Audit, deve inoltrare via fax o e-mail a SI Cert, la registrazione dell'Audit lasciata dal GA al termine della riunione di chiusura dell'Audit, allegando, qualora previsto, la documentazione richiesta.

Eventuali Rilievi che dovessero emergere al termine dell'Audit devono essere presi in carico dall'Organizzazione e la loro gestione comunicata a SI Cert (tramite le modalità indicate nell'Audit Report in funzione della tipologia del Rilievo).

Quest'ultimo deve essere approvato dal Responsabile del Gruppo di Audit prima di proseguire con le successive fasi del processo di Certificazione.

Nell'eventualità l'Organizzazione intenda avvalersi della possibilità di formulare proprie riserve, l'iter di certificazione si sospende fino alla ricezione delle riserve ed alla risoluzione positiva o negativa delle stesse.

L'intenzione di formulare riserve sull'operato del GA o sui contenuti dei documenti dallo stesso redatti e letti all'Organizzazione (Rapporto di Audit), deve essere comunicata al RGA al termine della lettura del documento. L'Organizzazione può formulare le proprie riserve entro 15 giorni dalla fine delle attività di Audit o dalla ricezione di eventuali comunicazioni da parte di SI Cert.

L'iter di certificazione si chiude negativamente nel caso l'esito delle attività di Audit sia negativo, o nel caso di "risoluzione negativa" delle riserve esposte dall'Organizzazione.

Nel corso dell'Audit sono anche verificati l'uso del Marchio SI Cert e degli OdA, qualora fossero già nelle disponibilità dell'Organizzazione in accordo a quanto previsto nel Regolamento uso del Marchio.

Oltre ai criteri generali di conduzione degli audit, la valutazione in campo è condotta con il supporto del Modello Diario di Verifica ISO 37001.

In tale documento il team di audit deve indicare:

- perimetro e l'applicabilità del Sistema di Gestione (4.3 della ISO 37001);
- definizione di corruzione prevista per l'organizzazione, sviluppata sulla base dell'analisi di contesto, che non può essere meno restrittiva di quella che è prevista per legge;
- specifici dettagli in merito alle attività a rischio (riportando in dettaglio processi a rischio ed attività sensibili);
- mappatura dei soggetti (interni ed esterni) che sono coinvolti in attività a maggior rischio;
- indicazione dei Partner in Affari e tipo di monitoraggio sugli stessi (tipo di gestione da questi adottata in ottica anticorruzione);
- le relazioni societarie;
- i riferimenti legislativi specifici;
- specifiche indicazioni sulla formazione svolta;
- l'elenco delle commesse valutate;
- analisi degli episodi di corruzione verificatisi e le contromisure adottate.

Saranno sottoposti a verifica con maggiore frequenza, impegno e profondità i processi/funzioni identificati dalla stessa organizzazione e/o dal Team di verifica come a maggior rischio, riportandone una spiegazione nella documentazione di verifica, oltre a quelli sensibili riportati alla nota 1 del § 4.1.

Sarà valutata la completezza ed esaustività dell'analisi dei rischi di corruzione, con riferimento ai requisiti applicabili della norma ISO 37001, e la robustezza del processo di internal auditing per la fattispecie della corruzione, che dovrà essere basato sui risultati della valutazione dei rischi e della mitigazione adottata, sulle valutazioni di rischio residuo e sul testing dei controlli operativi (il test dei controlli operativi deve essere valutando un adeguato campione selezionato in base al livello del rischio connesso alle attività soggette al controllo ed alla numerosità di quest'ultime; il criterio di campionamento, sia che si proceda per processi o requisiti, sarà indicato nella check list in modo tale che la sua fondatezza possa essere valutata in sede di riesame del report).

Si precisa che se durante l'audit il team di audit venisse a conoscenza, direttamente dall'organizzazione o da altre fonti, che la stessa organizzazione è implicata con dei profili di responsabilità in qualche scandalo o in qualche procedimento giudiziario per fenomeni corruttivi, qualora questa non abbia informato preventivamente l'organismo, l'audit dovrà essere interrotto dandone comunicazione all'organismo e procedendo, laddove possibile, ai conseguenti approfondimenti per valutare le azioni da adottare.

6. AUDIT PRELIMINARE

Prima dell'Audit Iniziale è possibile effettuare un Audit preliminare (Pre-Audit), indipendente dall'iter di certificazione.

Questo tipo di Audit è facoltativo e mira a verificare il grado di implementazione del Sistema di Gestione dell'Organizzazione prima dell'Audit di Certificazione dello stesso, in relazione ai requisiti della norma e di identificare quelle situazioni che potrebbero compromettere il buon esito dell'Initial Audit. È effettuato soltanto dopo espressa richiesta dell'Organizzazione alle condizioni riportate nell'offerta appositamente emessa, ed è sempre erogato/eseguito a titolo oneroso.

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

7. AUDIT INIZIALE

L'audit Iniziale 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 (così come previsto dai requisiti degli OdA):

- Stage 1 Audit finalizzato alla verifica della documentazione e della pianificazione del Sistema di Gestione nonché alla programmazione dello Stage 2
- Stage 2 Audit avente come scopo la valutazione dell'adeguatezza e conformità del Sistema di Gestione.

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

7.1. AUDIT DI PRIMO STAGE (S1)

Questo Audit deve essere effettuato sempre c/o l'Organizzazione anche nel caso di realtà di piccole dimensioni, secondo la comunicazione inviata da SI Cert e ha lo scopo di verificare la correttezza dei dati forniti dall'Organizzazione, predisporre in sintonia con l'Organizzazione il successivo Audit di Certificazione (Audit di Secondo Stage S2) e fornire al Gruppo di Audit un'esatta situazione delle attività e dei siti da sottoporre a certificazione con particolare attenzione a verificare:

- campo di applicazione del sistema di gestione e sua complessità (attività, esistenza di più sedi, numerosità del personale coinvolto in attività con rischio rilevante, ecc.);
- corretta stesura del sistema di gestione in conformità alla norma e alle eventuali relative linee guida che l'Organizzazione intende adottare;
- livello di coinvolgimento e impegno della leadership;
- modalità utilizzate dall'organizzazione per comprendere il contesto in cui opera, comprese le esigenze/aspettative degli stakeholder, e per valutare il rischio di corruzione al fine di determinare il campo di applicazione del sistema di gestione;
- Politica ed Obiettivi definiti, che siano appropriati all'organizzazione ed ai suoi traguardi di business, sia legali sia contrattuali; Politica ed Obiettivi siano approvati dalla Direzione ed inoltre siano definiti opportuni meccanismi per il loro riesame ed aggiornamento;
- procedura di valutazione e gestione dei rischi, così come previsto dallo standard di riferimento;
- responsabilità ed interfacce tra i processi interni ed esterni al campo di applicazione (compresi quelli messi in atto da eventuali fornitori) nonché gli accordi sui livelli di servizio garantiti;
- che siano elencate e prese in carico dall'organizzazione norme, leggi e regolamenti applicabili (comprese autorizzazioni, implicazioni normative o regolamenti aggiuntivi/inusuali per il settore, siano essi volontari ovvero imposti dai propri clienti);
- che Audit interni e Riesame da parte della Direzione siano stati pianificati ed eseguiti;
- procedura per l'analisi delle Non Conformità, degli eventi e delle azioni che potrebbero avere un impatto sull'efficacia e/o sulle prestazioni del sistema di gestione e che tale procedura sia idonea a determinare le cause degli stessi eventi, al fine di predisporre, ove necessario, le opportune Azioni Correttive;
- grado di implementazione del sistema di gestione e di preparazione per lo Stage 2, anche attraverso uno scambio di informazioni con il personale delegato e/o maggiormente coinvolto nei controlli operativi;
- conferma delle informazioni che hanno determinato la quantificazione del tempo di audit;
- esigenza di eseguire audit presso eventuali outsourcer dell'Organizzazione, qualora i processi a questi affidati possano influenzare significativamente la conformità del sistema di gestione dell'Organizzazione.

Si precisa che l'organizzazione deve fornire evidenza di aver effettuato la valutazione dei rischi su tutti i processi/attività.

Al termine dello Stage 1 deve essere formulato il Piano dello Stage 2 tenendo in considerazione:

- il perimetro dell'ABMS (esistenza di più sedi, numerosità del personale coinvolto in attività con rischio rilevante, ecc);
- i processi/funzioni identificati dalla stessa organizzazione e/o dal Team stesso come a maggior rischio;
- la normativa per la prevenzione della corruzione applicabile all'organizzazione;
- l'esistenza di più sedi, la loro distribuzione territoriale, la rilevanza delle attività svolte in relazione all'ABMS ed il tipo di controllo esercitato dalla sede centrale (si ricorda che non possono essere escluse sedi nell'ambito della stessa nazione, v. § 4);
- l'esistenza di siti temporanei rilevanti per la ABMS (v. § 4.2.7);
- l'esistenza di organizzazioni controllate;
- la rilevanza dei rischi connessi alle attività dei soci in affari non controllati dall'organizzazione;
- i risultati della valutazione del rischio corruzione.

Inoltre, anche in base agli aspetti di cui sopra, il Team dovrà confermare, o meno, l'adeguatezza del tempo previsto per la conduzione dello Stage 2, attraverso opportuna annotazione sul Rapporto. In ogni caso, al termine dello Stage 1, la funzione Resp. Commerciale dovrà verificare che le informazioni acquisite in fase di emissione di offerta siano confermate e, in caso contrario, procedere al riesame dei tempi di audit con il supporto del Lead Auditor.

Il Piano dello Stage 2 potrà essere elaborato con riferimento ai processi o ai requisiti della norma, in base a ciò che il Lead Auditor riterrà più opportuno, garantendo, comunque, un maggior approfondimento dei controlli relativi ai processi valutati con maggior rischio residuo. Pertanto:

a) nel Piano dello Stage 2, con riferimento alle attività operative (§ 8 della norma), dovranno essere elencati i processi/aree valutati dall'organizzazione con un rischio alto, al fine di una loro puntuale verifica che consenta di accertare l'adozione, laddove applicabili, di tutti i controlli specifici previsti dal § 8.2 al § 8.10 della norma (ovviamente, nell'ambito della verifica del processo, i controlli potranno essere campionati in base alla loro significatività ed alla numerosità delle attività oggetto del controllo); i processi/aree con un livello di rischio medio/basso potranno essere identificati in maniera generica (es. processi/aree con livello di rischio medio) e potranno essere campionati già in fase di Stage 2 in base ad opportune considerazioni dell'audit team (e nell'ambito del processo campionato, ovviamente, si procederà alla verifica dei controlli campionandoli in base alla loro significatività ed alla numerosità delle attività oggetto del controllo);
b) in alternativa, il piano dello Stage 2 potrà essere formulato elencando tutti i requisiti di cui al § 8 della ISO 37001, al fine di valutarne la loro applicazione attraverso un adeguato campionamento, nell'ambito di tutti processi interessati allo specifico controllo (es. i controlli finanziari

saranno valutati con riferimento ai rischi di corruzione relativi alle transazioni finanziarie dell'organizzazione, verificandone la pertinenza e la completezza), garantendo, come detto, un maggior approfondimento dei controlli relativi ai processi valutati con maggior rischio.

Nei casi in cui l'organizzazione svolga attività significative nell'ambito dell'ABMS presso un sito temporaneo, questo deve essere considerato ed incluso nel piano di audit; nel caso in cui ve ne siano più di uno è possibile campionarli per tipologia, tenendo conto della loro significatività.

Le risultanze dello Stage 1 Audit saranno documentate nell'Audit Report e comunicate all'Organizzazione dal Gruppo di Audit, compresa l'identificazione di ogni rilievo che nello Stage 2 Audit potrebbe essere classificato come Non Conformità e quindi, concordare/pianificare con l'Organizzazione il prosieguo delle attività, definendo in particolare la data per l'esecuzione dell'Audit S2 ed individuando i turni di lavoro, le eventuali sedi coinvolti dall'Audit S2 e scelti tra quelli comunicati dall'Organizzazione in fase di richiesta/accettazione offerta economica.

7.2. AUDIT DI SECONDO STAGE (S2) O DI CERTIFICAZIONE

L'Audit di Secondo Stage (S2) è eseguito soltanto in caso di esito positivo dell'Audit S1 ed è effettuato secondo la pianificazione concordata con l'Organizzazione alla fine dell'Audit S1 ed ha lo scopo di valutare il grado di adeguatezza ed applicazione dell'intero SGPC implementato dall'Organizzazione.

Durante lo Stage 2 Audit è prevista la valutazione che:

- siano stati presi in carico e risolti i Rilievi emersi durante l'Audit Stage 1;
- l'Organizzazione attui le proprie politiche, obiettivi e procedure;
- il Sistema di Gestione sia conforme a tutti i requisiti dello standard di riferimento (ed alle eventuali linee guida che si è deciso di integrare), agisca nel rispetto delle prescrizioni legali applicabili e stia raggiungendo gli obiettivi di politica dell'Organizzazione;
- il comportamento dell'Organizzazione, nell'ambito di eventuali iter autorizzativi o prescrizioni che non siano risultati completati al momento dell'Audit Stage 1;
- le informazioni che consentano di confermare il campo di applicazione;
- l'Organizzazione tenga sotto controllo i processi compresi nel campo di applicazione ed applichi i controlli selezionati;
- gli Audit interni ed il Riesame di Direzione siano stati effettuati.

A seguito dello Stage 2 dovrà essere elaborato il Programma delle sorveglianze, con riferimento ai processi o ai requisiti della norma, in base a ciò che il Lead Auditor riterrà più opportuno, garantendo, comunque, un maggior approfondimento dei controlli relativi ai processi valutati con maggior rischio residuo nel Rapporto di Audit.

a) **Programma per processi -** I processi con livello di rischio alto dovranno essere identificati puntualmente in modo tale da garantire che siano verificati almeno una volta nell'arco delle sorveglianze; i processi con livello di rischio medio e basso non dovranno essere identificati puntualmente (è possibile, ad esempio, indicarli nel programma utilizzando la formula generica "Processi con livello di rischio medio", "Processi con livello di rischio basso"), ma, comunque, dovranno essere verificati almeno una volta nell'arco delle sorveglianze (il campionamento dei processi nell'ambito del livello medio o basso dovrà avvenire tenendo in considerazione le registrazioni degli audit precedenti disponibili nella check list);
b) **Programma per requisiti -** In alternativa, il programma delle sorveglianze potrà essere formulato elencando i requisiti di cui al § 8 della ISO 37001, garantendo che ciascuno di essi sia verificato almeno una volta nell'arco delle sorveglianze.

Nei casi in cui l'organizzazione svolga attività significative nell'ambito dell'ABMS presso un sito temporaneo, questo deve essere considerato ed incluso nel programma di audit, garantendo che sia verificato almeno una volta nell'arco delle sorveglianze; nel caso in cui ve ne siano più di uno, è possibile campionarli per tipologia, tenendo conto della loro significatività (v. § 4.2.7).

La pratica è sottoposta all'analisi della Funzione Deliberante per la decisione sulla certificabilità o meno del Sistema di Gestione dell'Organizzazione in accordo con quanto previsto nel Regolamento Certificazione Sistemi di Gestione SGSI, SMS, SGPC e SGCO (ISO 27001, ISO 20000, ISO 37001 e ISO 22301) Parte 1 – Requisiti Generali, soltanto dopo che eventuali NC (maggiori o minori) siano gestite correttamente (vedi § 12) ed in seguito alla comunicazione/conferma all'Organizzazione dell'accettazione dei contenuti riportati sui documenti di Audit da parte della Direzione Tecnica o suo incaricato.

8. CERTIFICATO

Il certificato ha valdità triennale a partire dalla data della decisione per la certificazione e durante il periodo di validità è sottoposto, secondo le modalità di seguito riportate, a 2 verifiche, denominate Audit di Sorveglianza, sulle condizioni di mantenimento della relativa validità.

Alla scadenza è eseguito uno specifico Audit (audit di rinnovo) per rinnovare la certificazione per un ulteriore triennio. Tale Audit di Rinnovo è effettuato se l'Organizzazione intende rinnovare con SI CERT ITALY srl la propria certificazione per un ulteriore trienno, fatto salvo previsto dal presente Regolamente in materia di recesso contrattuale.

9. AUDIT DI SORVEGLIANZA

Gli Audit di Sorveglianza consistono:

- 1° Audit, successivo alla certificazione iniziale o Rinnovo, entro 12 mesi dalla data decisione sulla certificazione;
- 2° Audit di Sorveglianza entro 24 mesi dalla data decisione della certificazione, salvo casi particolari di volta in volta esaminati da SI CERT ITALY srl come di seguito riportato.

Il 1° Audit di sorveglianza successivo alla certificazione iniziale deve essere effettuato tassativamente entro massimo 12 mesi dalla data decisione sulla certificazione.

La modifica delle frequenze, della numerosità e dell'estensione degli Audit di Sorveglianza può essere dovuta a richieste, opportunamente motivate, da parte dell'Organizzazione (le quali sono esaminate dalla Direzione Tecnica ed eventualmente dalla Funzione Deliberante di SI Cert per approvazione) oppure richieste da SI Cert.

In entrambi i casi SI Cert da comunicazione formale delle decisioni prese all'Organizzazione. Nel caso quest'ultima non sia concorde con la decisione presa, può fare ricorso, rinunciare alla certificazione o vedersi il certificato sospeso/revocato d'ufficio (si vedano paragrafi specifici nel Regolamento Certificazione Sistemi di Gestione SGSI, SMS, SGPC e SGCO (ISO 27001, ISO 20000, ISO 37001 e ISO 22301) Parte 1 – Requisiti Generali).

Per le casistiche, modalità e costi si faccia riferimento al Regolamento Certificazione Sistemi di Gestione SGSI, SMS, SGPC e SGCO (ISO 27001, ISO 20000, ISO 37001 e ISO 22301) Parte 1 – Requisiti Generali paragrafi "Audit Supplementari" e "Reclami, Ricorsi e Contenziosi".

Ciascun Audit di Sorveglianza riguarda una parte del Sistema di Gestione interessato, ed i 2 Audit di Sorveglianza nel loro insieme assicurano il riesame completo del Sistema di Gestione nel triennio successivo alla certificazione.

L'Audit di Sorveglianza è eseguito secondo la pianificazione in precedenza comunicata all'Organizzazione, che tiene conto della necessità di verificare la risoluzione delle NC minori rilevate durante l'Audit precedente e l'efficacia delle relative azioni correttive, a cui si aggiunge la verifica degli elementi necessari per il mantenimento della certificazione secondo il piano già in possesso dell'Organizzazione:

Nell'eventualità lo ritenga necessario, il GA durante lo svolgimento della Audit di Sorveglianza può andare a verificare anche requisiti e/o aspetti non previsti nel programma iniziale o nella pianificazione comunicata all'Organizzazione.

10. Audit di Rinnovo

La validità del Certificato è confermata a seguito dell'esito positivo di una verifica completa (Audit di Rinnovo o Re-Audit) condotta con gli stessi criteri dello Stage 2 Audit.

La verifica di rinnovo può non prevedere l'esecuzione dello Stage 1 Audit salvo che non siano intervenute modifiche importanti all'Organizzazione o al suo Sistema di Gestione tali da richiederne l'effettuazione.

L'audit di Rinnovo deve essere effettuato entro la data di scadenza del certificato in vigore e con anticipo sufficiente per poter gestire anche la possibilità che, in caso di Non Conformità Maggiori, si disponga del tempo necessario per valutare l'efficacia del trattamento e deliberarne il rinnovo.

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 nuovo Audit Iniziale.

Eventuali eccezioni a quanto sopra riportato saranno gestite da SI Cert in rispetto delle disposizioni e direttive degli Organismi di Accreditamento ed in conformità ai documenti EA/IAF applicabili al presente schema di certificazione.

11. Audit Supplementari

Gli Audit Supplementari (così come già definiti all'omonimo paragrafo del Regolamento Certificazione Sistemi di Gestione SGSI, SMS, SGPC e SGCO (ISO 27001, ISO 20000, ISO 37001 e ISO 22301) Parte 1 – Requisiti Generali) è eseguito con le stesse modalità dello Stage 2 Audit. Qualora l'Audit Supplementare effettuato per la verifica dell'efficacia del trattamento delle Non Conformità Maggiori abbia esito negativo, la Certificazione sarà 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 (Regolamento Certificazione Sistemi di Gestione SGSI, SMS, SGPC e SGCO (ISO 27001, ISO 20000, ISO 37001 e ISO 22301) Parte 1 – Requisiti Generali paragrafi "Sospensione" e "Revoca").

12. Classificazione e Gestione Rilievi

Durante l'esecuzione degli Audit possono essere riscontrati i seguenti rilievi

12.1. Non Conformità Maggiori

Sono tutte quelle anomalie che scaturiscono da un mancato soddisfacimento, completo o parziale, di un requisito della norma di riferimento (assoluta mancanza della documentazione e/o non applicazione) oppure di un requisito legislativo o di un requisito contrattuale del Committente, riscontrate con evidenze oggettive, che influiscono in modo significativo sulla conformità del Sistema di Gestione, cioè che impediscono in modo costante e continuativo la sistematica e corretta applicazione della parte di Sistema risultata carente, ma soprattutto che non permettano il soddisfacimento dei requisiti relativi al prodotto/processo/servizio, siano tecnici sia legali.

L'Organizzazione deve provvedere quindi a definire le modalità di correzione di tali NC maggiori e le azioni intraprese come azioni correttive per eliminare le cause che le hanno determinato con le relative tempistiche, compilando la modulistica prevista. In particolare il termine entro cui presentare la proposta di risoluzione è al massimo di 10 giorni lavorativi. Infine, l'Organizzazione deve inoltrare secondo le modalità e tempistiche concordate con il RGA al termine dell'Audit, tutta la documentazione necessaria attestante l'avvenuto trattamento delle NC e l'efficacia delle azioni correttive attuate. Il termine entro cui chiudere le NC maggiori è al massimo di 3 mesi.

Le NC maggiori riscontrate durante l'Audit di Certificazione determinano la mancata presentazione del fascicolo dell'Organizzazione alla Funzione Deliberante fintanto che queste non siano risolte, mentre, per quelle riscontrate in fase di Audit di Sorveglianza se, scaduto il termine di 3 mesi per la loro risoluzione, queste non siano chiuse, scatta la sospensione del certificato per 6 mesi, oppure, nel caso le NC maggiori siano chiuse prima, fino al momento della loro effettiva chiusura. Trascorsi inutilmente i 6 mesi il certificato è revocato.

L'Audit della risoluzione (correzione) delle NC maggiori può avvenire:

- su base documentale,
- mediante apposito Audit Supplementare che è effettuato alle condizioni economiche riportate in Offerta.

Per l'Audit della correzione delle NC maggiori su base documentale, il RGA valuta la documentazione inviata dall'Organizzazione per dimostrare la completa correzione delle NC maggiori e, nel caso non fosse ritenuta soddisfacente, il RGA provvede alla richiesta di integrazioni all'Organizzazione. Solo alla ricezione di documentazione ritenuta soddisfacente che dia piena confidenza della correzione delle NC maggiori, il RGA provvede al completamento delle apposite sezioni dei documenti utilizzati per questa attività ed all'inoltro degli stessi alla Direzione Tecnica di SI Cert che, dopo averli verificati ed averne accettato i contenuti, provvede all'invio degli stessi all'Organizzazione.

Per l'Audit della correzione delle NC maggiori mediante Audit Supplementare, SI Cert provvede ad eseguire l'Audit secondo quanto indicato dal GA nei propri documenti e concordato con l'Organizzazione al termine dell'Audit (ad esempio: Audit limitato alle sole NC maggiori o Audit su tutti i requisiti del Sistema di Gestione) ed alle condizioni economiche riportate in Offerta.

12.2. Non Conformità Minori

Sono tutte quelle anomalie riscontrate con evidenze oggettive che influiscono in modo non significativo sulla conformità del Sistema di Gestione e che non inficiano il prosieguo dell'iter di certificazione e/o il mantenimento della stessa. Tali anomalie, che generalmente sono casuali, non ripetitive e non strutturali, non impediscono la sistematica e corretta applicazione della parte di sistema risultata carente.

Per le NC minori riscontrate durante le attività di Audit, il RGA al termine dell'Audit concorda con l'Organizzazione la tempistica e la modalità per la correzione delle stesse. L'Organizzazione deve provvedere quindi a definire le modalità di correzione di tali NC minori e le azioni intraprese come azioni correttive per eliminare le cause che le hanno determinato con le relative tempistiche, compilando la modulistica prevista. In particolare, il termine entro cui presentare la proposta di risoluzione delle stesse è al massimo di 30 giorni solari.

La verifica della correzione delle NC minori può avvenire:

- tramite accettazione della proposta di risoluzione da parte del RGA e quindi verifica dell'effettiva attuazione ed efficacia durante il successivo Audit di Sorveglianza,
- mediante apposito Audit Supplementare, nel caso durante gli Audit dovessero essere rilevate un numero elevato di NC minori.

Per la verifica della correzione delle NC minori tramite la sola proposta di risoluzione, il RGA valuta la/le proposta/e di correzione inviata/e dall'Organizzazione e, nel caso non fosse/fossero ritenuta/e soddisfacente/i, il RGA provvede alla richiesta di integrazioni all'Organizzazione. Solo alla ricezione di documentazione ritenuta soddisfacente, il RGA provvede al completamento delle apposite sezioni dei documenti utilizzati per questa attività ed all'inoltro degli stessi alla Direzione Tecnica di SI Cert che, dopo averli verificati ed averne accettato i contenuti, provvede all'invio degli stessi all'Organizzazione.

Durante il successivo Audit di Sorveglianza e/o Rinnovo, il GA provvede a verificare l'effettiva chiusura delle NC minori. Nel caso queste non siano state trattate o chiuse efficacemente, sono rilanciate aumentandole di peso (NC maggiore), mentre nel caso in cui siano parzialmente chiuse o non efficacemente chiuse, sono rilanciate con lo stesso peso.

Per la verifica della correzione delle NC minori mediante Audit supplementare, SI Cert provvede ad eseguire l'Audit secondo quanto indicato dal GA nei propri documenti e concordato con l'Organizzazione al termine dell'Audit (ad esempio Audit limitato alle sole NC minori o Audit su tutti i requisiti del Sistema di Gestione) ed alle condizioni economiche riportate in Offerta.

Nel caso queste non siano state trattate o chiuse efficacemente, sono rilanciate aumentandole di peso (NC maggiore), mentre nel caso in cui siano parzialmente chiuse o non efficacemente chiuse, sono rilanciate con lo stesso peso.

12.3. Raccomandazioni

Sono quei rilievi che non possono essere considerati NC minori, ma che possono dare un apporto migliorativo all'efficacia del Sistema di Gestione implementato dall'Organizzazione ed alla sua capacità di soddisfare in modo efficace ed efficiente i requisiti generali della norma di riferimento.

L'Organizzazione non ha l'obbligo di recepire le raccomandazioni formulate dal GA, ma deve dare evidenza, tramite un riesame delle stesse in forma documentata ed entro breve temine dalla fine dell'Audit (massimo 1 mese), di averle analizzate. Nel caso in cui non dovesse ritenere necessario recepire le raccomandazioni, l'Organizzazione, nella registrazione del riesame delle stesse, deve spiegare i motivi di tale decisione. Durante il successivo Audit di Sorveglianza e/o Rinnovo, il GA provvede a verificare l'effettiva analisi delle raccomandazioni. Per quelle raccomandazioni che l'Organizzazione ha recepito, il GA provvede a verificare l'effettiva applicazione della decisione intrapresa. Nel caso in cui questa non sia stata applicata o chiusa, la raccomandazione è rilanciata aumentandola di peso in NC minore. Nel caso in cui sia parzialmente applicata e/o chiusa la raccomandazione è rilanciata con lo stesso peso.