VERIFICA: GIOVANNI ZANVETTOR **APPROVA**: CRISTIANO PUCCI

REV	NOTE DI MODIFICA	DATA
0	Prima emissione	28.11.2022
1	Eliminata la data di scadenza di validità annuale	11.03.2024

QUESTO DOCUMENTO È DISTRIBUITO			
	COPIA CONTROLLATA		COPIA NON CONTROLLATA

INDICE

1. SCOPO E VALIDITÀ

Scopo del presente documento è definire e stabilire i requisiti tecnici per l'iter e le regole per la gestione, il rilascio, la sorveglianza della Certificazione dei Sistemi di Gestione per la Sicurezza Informatica.

Il presente documento è da considerarsi supplementare, e quindi non sostitutivo, a quanto definito nel "Regolamento Certificazione - Requisiti Generali".

Pertanto, ai fini della completa regolarizzazione del rapporto contrattuale, è richiesto all'Organizzazione richiedente i servizi di certificazione di procedere all'accettazione di entrambi i succitati Regolamenti secondo le modalità allo scopo stabilite nel "Regolamento Certificazione - Requisiti Generali".

2. DEFINIZIONI, ACRONIMI E SINONIMI

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

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

- SGSI (ISMS): acronimo di Sistema di Gestione per la Sicurezza Informatica (Information Security Management System);
- SI Cert: sinonimo di SI CERT SAGL;
- 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 ed 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 Regolamento Certificazione, talune definizioni o significati di alcuni termini e/o locuzione sono riportate contestualmente all'utilizzo del termine o della locuzione stessa.

3. RIFERIMENTI

I riferimenti normativi per la certificazione dei Sistemi di Gestione della Continuità Operativa ed i servizi ad essa collegati, sono di seguito riportati, anche se non a titolo esaustivo:

- ISO/IEC 17021-1 "Valutazione della conformità – Requisiti per gli organismi che forniscono Audit e certificazione di sistemi di gestione – Parte 1: Requisiti"
- ISO/IEC 17000 "Valutazione delle conformità – vocabolario e principi generali"
- Regolamenti e prescrizioni degli Organismi di Accreditamento
- Linee Guide IAF, EA o Regolamenti ISO per gli organismi di certificazione (ad esempio IAF MD1, IAF MD2, IAF MD4, IAF MD5, IAF MD11, IAF MD13, IAF MD15, IAF MD23, IAF ID3, IAF ID4, IAF ID12).
- ISO Guide 73, Risk management - Vocabulary
- EN ISO 9000, Sistemi di Gestione per la Qualità – Fondamenti e vocabolario
- CEI ISO/IEC 27001, Sistema di Gestione per la Sicurezza Informatica
- ISO/IEC 27000 "Tecnologie informatiche - Tecniche di sicurezza - Sistemi di gestione della sicurezza dell'informazione - Descrizione e vocabolario"
- ISO/IEC 27006:2015/AMD 1:2020 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems
- CEI ISO/IEC 27002 "Tecnologie Informatiche - Tecniche di sicurezza - Codice di pratica per la gestione della sicurezza delle informazioni"
- ISO/IEC 27013, Information technology - Security techniques - Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
- ISO / IEC 27701, Sistema di Gestione per la Sicurezza delle Informazioni sulla Privacy
- ISO/IEC 27018, Sistema di Gestione per la Sicurezza Informatica Privacy nel Cloud
- ISO/IEC 27017, Sistema di Gestione per la Sicurezza Informatica per i Servizi Cloud

I riferimenti sopra riportati sono quelli aggiornati ed in ultima edizione al momento del loro utilizzo.
Altri riferimenti sono presi in considerazione da parte di SI CERT SAGL e sono esplicitati all'interno delle pertinenti Procedure Operative interne, che all'occorrenza sono rese disponibili a chi ne facesse esplicita richiesta.

4. CAMPO DI APPLICAZIONE

Il campo di applicazione del Regolamento Certificazione si riferisce alla certificazione dei Sistemi di Gestione per la Sicurezza Informatica secondo la norma:

ISO/IEC 27001 Sistema di Gestione Sicurezza Informatica

e le relative line guida

ISO/IEC 27701 Sistema di Gestione Sicurezza delle informazioni sulla privacy

ISO/IEC 27017 Sistema di Gestione Sicurezza Informatica per i servizi cloud

ISO/IEC 27018 Sistema di Gestione Sicurezza Informatica PRIVACY nel cloud

nelle edizioni correnti e descrive le modalità operative applicate da parte di SI CERT SAGL.

5. ITER DI CERTIFICAZIONE

L'Organizzazione richiedente la Certificazione deve:

a) avere un Sistema di Gestione per la Sicurezza delle Informazioni 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) avere effettuato un ciclo completo di Verifiche Ispettive Interne ed un Riesame della Direzione;
c) mantenere a disposizione di SI CERT SAGL le registrazioni di tutti i reclami ricevuti e delle relative azioni conseguenti;
d) mantenere aggiornata la raccolta delle norme, leggi e regolamenti cogenti applicabili all'attività, processo, servizio, prodotto incluso nel campo di applicazione della Certificazione.

6. ATTIVITÀ DI 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 (vedi paragrafo 6.9 "Audit da remoto").
Nel caso di Organizzazioni multi-sito, le attività di Audit, siano queste di certificazione, di sorveglianza e/o rinnovo sono pianificate in modo da rispettare le guide applicative della norma ISO/IEC 17021-1 (a titolo di esempio: IAF MD1, IAF MD2, IAF MD4, IAF MD5, IAF MD11, IAF MD13, IAF MD15, IAF MD21, IAF MD22, IAF MD23. IAF ID1, IAF ID3, IAF ID12) ed altri documenti allo scopo applicabili emessi da SAS.
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 e 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 di 5 giorni, come 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 indicata sul frontespizio della stessa.
Eventuali rilievi che dovessero emergere al termine dell'Audit devono essere presi in carico dall'Organizzazione e la loro gestione comunicata a SI CERT SAGL (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 SAGL.
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 di SI CERT SAGL e degli OdA qualora fossero già nelle disponibilità dell'Organizzazione in accordo a quanto previsto nel Regolamento dell'Uso del Marchio.
Oltre ai criteri generali di conduzione degli audit, la valutazione in campo è condotta con il supporto del modulo "Diario di Verifica ISO 22301"; in occasione di ogni audit (iniziale, sorveglianza e rinnovo) dovranno essere valutati i seguenti aspetti (fornendo adeguate informazioni nel rapporto di audit):

- la completezza e correttezza dei dati forniti dall'Organizzazione e dello scopo di certificazione;
- l'individuazione ed eventuale aggiornamento del contesto operativo, dei fattori interni ed esterni, delle Parti Interessate e relative aspettative,
- l'aggiornamento dell'analisi dei rischi e delle opportunità con le azioni a seguire decise/predisposte,
- che la valutazione dei rischi abbia un senso per le parti interessate, che le misure predisposte dall'organizzazione, per rispondere agli scenari di rischio, siano coerenti con tali valutazioni e che, in particolare, sia stata stabilita la tolleranza al rischio per i processi oggetto della gestione della continuità operativa (si sottolinea che a seconda delle parti interessate, la misura del rischio può essere basata su criteri diversi: per la proprietà potranno essere economici e reputazionali, per la collettività di tipo maggiormente operativo);
- che tali valutazioni tengano conto anche delle prestazioni, affidabilità ed esposizione a rischi specifici dei fornitori e che, laddove applicabile, sia stata effettuata una specifica valutazione per i servizi dati in "outsourcing";
- l'adeguatezza dell'addestramento delle risorse umane e delle relative esercitazioni, con riferimento alla copertura degli scenari interruttivi individuati dall'analisi di impatto sul business;
- che il sistema di gestione garantisca che l'organizzazione sia in grado di conoscere, gestire come documenti di origine esterna e rispettare le pertinenti disposizioni di legge, comprendendo quali siano gli obblighi e quali siano le opportunità disponibili (i requisiti legali attinenti la gestione della continuità operativa sono molti, e in alcuni settori sono legati ai concetti di "infrastruttura critica" ed ai principi della sicurezza nazionale e comunitaria);
- che le scelte dell'organizzazione sui comportamenti da adottare in relazione alla continuità operativa, siano congruenti, almeno, con le disposizioni di legge applicabili.

6.1. 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 in un'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.

6.2. 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 o cantieri (così come previsto dai requisiti degli OdA):

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

Lo Stage 2 può essere effettuato solo dopo il completamento dello Stage 1 e deve aver luogo entro e non oltre 6 mesi dalla prima verifica altrimenti questa deve essere ripetuta.

Nel caso di integrazione alla ISO/IEC 27017 ("servizi cloud") oppure alle ISO/IEC27017 e ISO/IEC 27018 ("Privacy nel cloud") prima del rilascio della certificazione, salvo diverse disposizioni degli OdA, devono essere verificati tutti i Data Center presso cui sono dislocati i server che gestiscono il cloud; qualora i Data Center utilizzati per le attività "cloud" siano in outsourcing presso fornitori in possesso di certificazioni ISO/IEC 27001, ISO/IEC 27017 (e ISO/IEC 27018) accreditate e riconosciute a livello MLA, o nel caso di Data Center in possesso di certificazioni TIER III o TIER IV, ove non fosse possibile svolgere un audit diretto, potrà essere utilizzata la sola valutazione documentale degli aspetti contrattuali e di controllo operativo verso tali fornitori.

Nel caso di integrazioni alla ISO/IEC 27701 ("Privacy Information Management System") prima del rilascio della certificazione, salvo diverse disposizioni degli OdA, si dovrà verificare se l'organizzazione si sottopone periodicamente a *vulnerability assesment* / *penetration test*, e con quali modalità (es. *vulnerability assesment* condotti da LAB accreditati, *penetration test* condotti da LAB che abbiano caratteristiche organizzative e gestionali equivalenti ai requisiti della Norma ISO/IEC 17025).

6.2.1. Audit di Primo Stage (S1)

Questo Audit è effettuato, generalmente presso la sede dell'Organizzazione, 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 che:

- La Politica e gli Obiettivi per la Sicurezza definiti siano appropriati all'organizzazione ed ai suoi traguardi di business, sia legali sia contrattuali; Politica ed Obiettivi siano approvati dalla Direzione ed inoltre siano attuati opportuni meccanismi per il loro riesame e aggiornamento;
- siano elencate e prese in carico dall'organizzazione le norme, e leggi e i regolamenti applicabili (comprese autorizzazioni, implicazioni normative o regolamenti aggiuntivi/inusuali per il settore siano essi volontari ovvero imposti dai propri clienti);
- la Dichiarazione relativa al "Campo di Applicazione" definisca in modo chiaro, completo e circoscritto l'ambiente fisico (uffici e/o edifici e/o siti etc), il dominio logico (lan, campus, wan e relative apparecchiature) e la struttura organizzativa (processi/attività interne e/o svolte dai fornitori) rispetto al quale si richieda la certificazione;
- esista e sia applicata la procedura di valutazione e gestione dei rischi che tenga conto di criteri di misurazione dei rischi, tali da avere senso per le parti interessate ed in particolare che sia stata stabilita la tolleranza al rischio per i processi;
- esistano eventuali processi o aree che necessitano di particolari attenzioni;
- gli Audit interni e il Riesame da parte della Direzione siano stati pianificati almeno con cadenza annuale, eseguiti e che il livello di attuazione del Sistema di Gestione fornisca l'evidenza che l'Organizzazione è pronta per lo Stage 2 Audit;
- il piano di formazione ed informazione delle risorse umane sia definito in base alla relativa analisi delle esigenze ed attuato (o ne sia stata prevista l'attuazione);
- sia stata definita una 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.
- la corretta stesura e applicazione del Sistema di Gestione per la Sicurezza delle Informazioni in conformità alla norma e alle eventuali relative linee guida che l'Organizzazione intende adottare (o alle norme prese a riferimento nel caso di Sistemi di Gestione Integrati);
- i dati forniti dall'Organizzazione in fase di richiesta di offerta economica, al fine di pianificare correttamente le successive attività di Secondo Stage (ad esempio: sedi dichiarate, dimensioni in termini di forza lavoro che ha incidenza sul Sistema o sul prodotto/servizio realizzato, incluse eventuali attività di outsourcing, numero siti produttivi e/o unità produttive o operative, e/o cantieri, orari e/o turni di lavoro);
- sia documentata la configurazione di rete;
- esista la planimetria del sito che identifichi le aree sicure e che sia, preferibilmente, comprensiva degli impianti elettrici e meccanici di supporto;

- esistano adeguati obiettivi per la Sicurezza e questi siano supportati da una programmazione e, ove possibile, da una pianificazione tecnica e finanziaria;
- gli obiettivi per la sicurezza e relativi indicatori siano coerenti con la valutazione dei rischi e con la politica per la sicurezza per l'esercizio dell'attività l'Organizzazione sia in possesso di tutte le necessarie licenze relative al software applicativo impiegato;
- il Sistema di Gestione tenga traccia e risponda alle principali istanze delle parti interessate riguardo la Sicurezza delle Informazioni;

Nel caso di estensione alla/e ISO/IEC 27017 ("servizi cloud") oppure alle ISO/IEC27017 e ISO/IEC 27018 ("Privacy nel cloud")

- la presenza di accordi contrattuali con gli eventuali outsorcers a cui sono appoggiati i servizi Cloud e le relative certificazioni possedute.

Nel caso di estensione alla ISO/IEC 27701 ("Privacy Information Management System"):

- la presenza di rapporti di Vulnerability Assessement e Penetretion Test e le qualifiche dei laboratori che li hanno condotti;
- la presenza di accordi contrattuali con gli eventuali outsorcers fornitori dei Data Center e le relative certificazioni possedute.

Di estrema importanza, in questa fase, verificare che non esistano eventuali registrazioni del SGSI o siti inclusi nello scopo che non possono essere rese/i disponibili per la verifica da parte del Gruppo di Verifica, perché contengono informazioni riservate o sensibili ovvero per motivi di sicurezza. In questo caso si dovrà stabilire se il sistema di gestione potrà essere adeguatamente verificato, anche non potendo avere accesso a questi record/siti. Qualora si concluda che non sia possibile verificare adeguatamente il SGSI, si informerà l'organizzazione che l'audit di certificazione non potrà aver luogo, se non saranno definite e concesse modalità di accesso adeguate, oppure apportando modifiche al campo di applicazione.

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 e gli eventuali siti operativi esterni (ad esempio: cantieri per settore IAF 28, centri di cottura o somministrazione pasti per settore IAF 30 o siti dove sono eseguite attività di pulizia per il settore IAF 35, ecc.) coinvolti dall'Audit S2, scelti tra quelli comunicati dall'Organizzazione in fase di richiesta/accettazione offerta economica.

La validità dei contenuti dell'Audit di S1 è pari a 6 mesi a partire dalla data di chiusura dello stesso. Nel caso in cui non sia possibile eseguire l'Audit S2 entro i 6 mesi, si deve ricominciare l'iter, ripartendo dall'Audit S1.

In ogni caso, prima di procedere con lo stage 2 il Responsabile del Gruppo di verifica deve confermare se il Gruppo di Verifica eventualmente precedentemente individuato per l'audit di stage 2 possiede, nel complesso, la competenza necessaria in relazione al tipo di Organizzazione ovvero è necessario apportarvi modifiche e/o integrazioni. Nel secondo caso concorda con la Pianificazione le modifiche/integrazioni necessarie/opportune le quali saranno comunicate all'Organizzazione.

6.2.2. 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 SGSI implementato dall'Organizzazione.

Oltre quanto già riportato al paragrafo 6. Attività di Audit, durante lo Stage 2 Audit è prevista la valutazione che:

- siano stati presi in carico e risolti i Rilievi emersi durante lo Stage 1 Audit
- 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;
- sia adeguato e proattivo il comportamento dell'Organizzazione, nell'ambito di eventuali iter autorizzativi o prescrizioni che non siano risultati completati al momento dello Stage 1 Audit;
- siano disponibili e sufficienti le informazioni che consentano di confermare il campo di applicazione;
- l'Organizzazione tenga sotto controllo i processi compresi nel campo di applicazione;
- gli Audit interni ed il Riesame di Direzione siano stati effettuati;

A conclusione dell'Audit, il GA predispone il Rapporto di Audit che consegna al Rappresentante dell'Organizzazione con indicazioni delle risultanze e delle eventuali azioni da attuare per il prosieguo dell'iter di certificazione.

Chiusa la documentazione di audit da parte del GA, la pratica è sottoposta all'analisi della Funzione Deliberante che, sotto l'esclusiva responsabilità di SI CERT SAGL, decide sulla possibilità di rilasciare o meno il certificato per il Sistema di Gestione dell'Organizzazione in accordo con quanto previsto nel "Regolamento Certificazione – Requisiti Generali", soltanto dopo che eventuali NC (maggiori o minori) siano

gestite correttamente (vedi § 7 “Classificazione e gestione dei rilievi”) 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.
Nel caso in cui non sia possibile verificare l'attuazione delle correzioni e delle azioni correttive relative ad ogni eventuale NC maggiore, entro 6 mesi dopo l'ultimo giorno della Audit S2, esso deve essere ripetuto.
La verifica tecnico-operativa delle attività di certificazione avviene mediante procedura informatica (tramite e-mail) con Personale che non abbia partecipato alle precedenti attività di Audit e con le stesse competenze del GA che ha eseguito l’Audit. Questa attività è eseguita entro una settimana dalla comunicazione/conferma all’Organizzazione dell’accettazione dei contenuti riportati sui documenti di Audit da parte della Direzione Tecnica o suo incaricato, salvo la richiesta di approfondimento che dovessero emergere per alcune di esse. Ad esito positivo della fase di riesame della documentazione di Audit e di decisione per la certificazione, è emesso il certificato.
Il certificato ha validità 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.
Apposito Programma delle Sorveglianze è riportato all’interno del Rapporti di Audit ed è tenuto aggiornato ad ogni Audit effettuato nel periodo di validità della certificazione.
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 SAGL la propria certificazione per un ulteriore triennio, fatto salvo previsto dal Regolamento Certificazione in materia di recesso contrattuale.

6.3. 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 SAGL come di seguito riportato.

Tali frequenze sono da considerarsi perentorie, in modo particolare per il 1° Audit di sorveglianza successivo alla certificazione iniziale.
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 casi particolari, quali ad esempio fermo delle attività operative, le frequenze in precedenza indicate possono essere modificate, se l’Organizzazione ne fa richiesta con giustificate valide motivazioni di volta in volta valutate. In tali casi si procede comunque all’esecuzione dell’Audit sui punti previsti nel programma riportato nella registrazione delle precedenti attività di Audit, eseguendo l’Audit su base documentale per le sole attività operative, prevedendo l’esecuzione di un Audit disgiunto, possibilmente a breve termine, al fine di verificare le attività operative durante la loro effettuazione. I costi aggiuntivi sostenuti per le attività di Audit eseguite in modo disgiunto sono addebitati all’Organizzazione. In ogni caso, qualsiasi richiesta di variazione delle date previste per l’effettuazione degli Audit di Sorveglianza è esaminata da SI CERT SAGL e le decisioni in merito tempestivamente comunicate all’Organizzazione per le azioni del caso nel rispetto del presente Regolamento e delle prescrizioni di SAS.
Analogamente SI CERT SAGL si riserva la possibilità, dandone formale comunicazione all’Organizzazione, di modificare le frequenze e l’estensione degli Audit di Sorveglianza in base ai rilievi emersi dalle precedenti attività di Audit.
Nel caso l’Organizzazione non sia concorde con la decisione presa e comunicata da parte di SI CERT SAGL, può fare ricorso, rinunciare alla certificazione o vedersi il certificato sospeso/revocato d’ufficio (si vedano paragrafi specifici nel “Regolamento Certificazione - Requisiti Generali”).
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.
Almeno 40 giorni prima dell’esecuzione dell’Audit di Sorveglianza, SI CERT SAGL invia all’Organizzazione specifica comunicazione in modo da indicare il GA incaricato e poter concordare la data precisa di esecuzione dell’audit, oltre a richiedere conferma o aggiornamento dati tramite la richiesta di compilazione del modulo di aggiornamento dati. Tra i dati richiesti vi sono almeno i seguenti:

- modifiche sostanziali al Sistema di Gestione aziendale e/o allo scopo di certificazione e/o all’organizzazione e/o sedi/siti;
- dimensioni in forza lavoro, turni di lavoro, fatturato;
- eventuale elenco siti operativi esterni ove l'Organizzazione eroga il proprio servizio (ad esempio: cantieri per settore IAF 28, centri di cottura o somministrazione pasti per settore IAF 30 o siti dove sono eseguite attività di pulizia per il settore IAF 35);

Nel caso non si dovessero riscontrare variazioni rispetto ai dati forniti dall'Organizzazione per poter definire le attività dell'Audit Iniziale, restano valide le condizioni economiche dell'offerta originaria.
Caso contrario, SI CERT SAGL o suo Business Partner emette nuova offerta economica (per i dettagli vedi "Regolamento Certificazione – Requisiti Generali").

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.

A conclusione dell'Audit, il GA predispone il Rapporto di Audit che consegna al Rappresentante dell'Organizzazione con indicazioni delle risultanze e delle eventuali azioni da attuare per il prosieguo dell'iter di certificazione.
Chiusa la documentazione di audit da parte del GA, e soltanto dopo che eventuali NC (maggiori o minori) siano gestite correttamente (vedi § 7 "Classificazione e gestione dei rilievi") 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, la pratica è archiviata.
Si precisa infine che in assenza di qualsiasi richiesta di rinvio della data dell'Audit di Sorveglianza con motivate valide giustificazioni ed in assenza di qualsiasi risposta alla pianificazione trasmessa, non potendo SI CERT SAGL effettuare l'attività di Audit, il certificato perde di validità; la validità del certificato potrà essere riattivata con un audit della durata pari all'Audit di Sorveglianza, se effettuato entro i 3 mesi dalla data prevista per la sorveglianza, con un audit della durata pari, invece, all'Audit di Rinnovo, se effettuato dopo 3 mesi, con conseguente aumento dei costi.
SI CERT SAGL non si ritiene responsabile di eventuali problemi che l'Organizzazione dovesse incontrare in seguito all'esecuzione degli Audit di Sorveglianza in disaccordo con le tempistiche allo scopo previste, in particolare in caso di slittamento degli stessi.

6.4. AUDIT DI RINNOVO

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, in caso di Non Conformità Maggiori, ci sia il tempo necessario per valutare l'efficacia del trattamento e deliberarne il rinnovo.
Almeno 40 giorni prima dell'esecuzione della Audit di Rinnovo della certificazione per un ulteriore triennio, SI CERT SAGL invia all'Organizzazione specifica comunicazione in modo da indicare il GA incaricato e poter concordare la data precisa di esecuzione dell'audit, oltre a richiedere conferma o aggiornamento dati tramite la richiesta di compilazione del modulo di aggiornamento dati. Tra i dati richiesti vi sono almeno i seguenti:

- modifiche sostanziali al Sistema di Gestione aziendale e/o allo scopo di certificazione e/o all'organizzazione e/o siti;
- dimensioni in forza lavoro, turni di lavoro, fatturato;
- eventuale elenco siti operativi esterni ove l'Organizzazione eroga il proprio servizio (ad esempio: cantieri per settore IAF 28, centri di cottura o somministrazione pasti per settore IAF 30 o siti dove sono eseguite attività di pulizia per il settore IAF 35);

Nel caso non si dovessero riscontrare variazioni rispetto ai dati forniti dall'Organizzazione per il precedente triennio di certificazione, restano valide le condizioni economiche dell'offerta originaria.
Caso contrario, SI CERT SAGL o suo Business Partner emette apposita offerta economica per il successivo ciclo di certificazione, che è calcolata con i dati in possesso a SI CERT SAGL al momento dell'emissione della stessa (per i dettagli vedi "Regolamento Certificazione – Requisiti Generali").
In quest'ultimo caso, per l'Audit di Rinnovo potrebbe essere necessario un Audit S1 aggiuntivo, nel caso si siano verificate modifiche significative al Sistema di Gestione dell'Organizzazione o di altro tipo (per esempio cambiamenti nella legislazione).
L'Audit di Rinnovo ha durata pari a quella comunicata in fase di offerta e/o nelle comunicazioni successive, salvo variazioni collegate alle dimensioni dell'Organizzazione, dal momento che le tempistiche sono calcolate sulle dimensioni effettive dell'Organizzazione al momento dell'Audit.
L'Audit di Rinnovo 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 rinnovo della certificazione secondo il piano già in possesso dell'Organizzazione.

A conclusione dell'Audit, il GA predispone il Rapporto di Audit che consegna al Rappresentante dell'Organizzazione con indicazioni delle risultanze e delle eventuali azioni da attuare per il prosieguo dell'iter di certificazione.
Chiusa la documentazione di audit da parte del GA, la pratica è sottoposta all'analisi della Funzione Deliberante che, sotto l'esclusiva responsabilità di SI CERT SAGL, decide sulla possibilità di rilasciare o meno il certificato in accordo con quanto previsto nel "Regolamento Certificazione – Requisiti Generali", soltanto dopo che eventuali NC (maggiori o minori) siano gestite correttamente (vedi § 7 "Classificazione e gestione dei rilievi") 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.

L'Audit di Rinnovo può essere eseguito anche oltre la data di scadenza della certificazione, entro 6 mesi massimo oltre tale data, anche se in tale intervallo temporale la validità del/i certificato/i risulta/no scaduta/e. In tal caso il certificato è riemesso con chiara indicazione del periodo in cui la certificazione è stato inattiva. Pertanto, il certificato riporta la data originaria di certificazione o data di prima emissione, la data originaria di scadenza ossia basata sul ciclo di certificazione precedente, la data della ricertificazione corrispondente o successiva alla data di decisione della ricertificazione, la data di emissione corrente del certificato e la data di scadenza del certificato basata sul ciclo di certificazione precedente.
Qualora non sia possibile eseguire l'Audit di Rinnovo o non sia possibile verificare l'attuazione delle correzioni e delle azioni correttive relative ad ogni eventuale NC maggiore entro i tempi previsti, allora non sarà possibile rinnovare la certificazione né sarà possibile prorogare la validità del certificato, e 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 e in conformità ai documenti EA/IAF applicabili al presente schema di certificazione.
Solo in casi particolari, quali ad esempio fermo delle attività operative, si procede ad un Audit Documentale sui requisiti della norma legati all'operatività, prevedendo l'esecuzione di un Audit Disgiunto, possibilmente a breve termine, al fine di verificare le attività operative durante la loro effettiva effettuazione. I costi aggiuntivi sostenuti per le attività di Audit eseguite in modo disgiunto sono addebitati all'Organizzazione.
Durante l'Audit di Rinnovo, si sottopongono a verifica tutti i requisiti della/e norma/e presa/e a riferimento per il Sistema di Gestione oggetto di Audit.
L'Audit di Rinnovo ha anche lo scopo di confermare la continua conformità ed efficacia del Sistema di Gestione dell'Organizzazione nel suo complesso, e la sua continua pertinenza e applicabilità al campo di applicazione della certificazione.
SI CERT SAGL non si ritiene responsabile di eventuali problemi che l'Organizzazione dovesse incontrare in seguito all'esecuzione degli Audit di Rinnovo in disaccordo con le tempistiche allo scopo previste, in particolare in caso di slittamento degli stessi.

6.5. AUDIT PER ESTENSIONE DEL CAMPO DI APPLICAZIONE DEL CERTIFICATO

In seguito di richiesta di estensione del campo di applicazione pervenuta da un'Organizzazione certificata, SI CERT SAGL provvede a riesaminare quanto inviato dalla stessa, e stabilire quindi le attività di Audit necessarie per stabilire se l'estensione possa essere o meno concessa.
In caso di esito positivo, SI CERT SAGL o un suo Business Partner emette una specifica offerta economica per l'effettuazione di tale Audit.
Questo tipo di Audit può essere eseguito anche contestualmente all'Audit di Sorveglianza o di Rinnovo. In tal caso, SI CERT SAGL o un suo Business Partner, se ritenuto necessario, riformula l'offerta economica in funzione delle eventuali attività/tempi aggiuntivi necessari per eseguire tale Audit.
Le modalità di gestione di tale Audit di Estensione sono le stesse delle altre tipologie di Audit, ai quali si rimanda per i relativi dettagli operativi.
Ad esito positivo della fase di riesame della documentazione di Audit e di decisione della estensione della certificazione a cura della Funzione Deliberante e secondo le medesime modalità dell'Audit di Certificazione o di Rinnovo, è emesso il nuovo Certificato con l'ampliamento delle scopo di certificazione per effetto dell'estensione del campo di applicazione.

6.6. AUDIT SUPPLEMENTARI

Gli Audit Supplementari (così come già definiti all'omonimo paragrafo del Regolamento Contrattuale) 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 Contrattuale paragrafi "Sospensione" e "Revoca").
Oltre a quanto sopra indicato sono previsti e, all'occorrenza, eseguiti anche gli Audit di seguito descritti.

In particolare, SI CERT SAGL si riserva di effettuare Audit Supplementari non previsti nel Programma delle Sorveglianze nei casi di:

- Non Conformità per le quali il GA ritenga necessaria la verifica della correzione sul campo;
- modifiche significative dell''Organizzazione stessa oppure al campo di applicazione del certificato;
- segnalazioni negative sulla stessa Organizzazione oppure su quanto oggetto del campo di applicazione;
- scadenza del periodo di sospensione;
- mancata delibera per il rilascio del certificato da parte della Funzione Deliberante;
- variazioni delle norme di riferimento, delle prescrizioni degli Organismi di Accreditamento, del presente Regolamento, qualora tali variazioni non possano essere verificate durante una attività di Audit già inserita nel piano Programma delle Sorveglianze (attività Audit di Sorveglianza e/o Rinnovo);
- altre circostanze ritenute abbiano influenza negativa sulla certificazione (incluse segnalazioni derivanti dal Mercato, Terze Parti e valutazione di informazioni di pubblico dominio); in questo caso, gli Audit Supplementari possono avvenire con breve preavviso o senza preavviso. (vedi paragrafo 6.7. “Audit con Breve Preavviso”).

Qualora l’Audit Supplementare sia effettuato per la verifica dell’efficacia del trattamento delle Non Conformità Maggiori ed 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 6 mesi, trascorsi i quali la Sospensione si trasformerà in Revoca.

Infine, possono essere effettuati Audit su richiesta di SAS allo scopo di accertare che le modalità di valutazione adottate da SI CERT SAGL siano conformi alle norme ed ai Regolamenti di riferimento. Tali Audit fanno parte della Attività di Market Surveillance esercitata da SAS e per i quali si rimanda al successivo paragrafo 6.8 “Audit di market surveillance”.

Tali tipologie di Audit sono condotte con gli stessi criteri delle altre attività di Audit e non sono sostitutive degli Audit di Sorveglianza o di Rinnovo. Infine, a seconda della tipologia di Audit, essi sono a carico di SI CERT SAGL oppure dell’Organizzazione certificata in accordo al Tariffario in vigore al momento dell’Audit.

6.7. AUDIT CON BREVE PREAVVISO

In caso di necessità, SI CERT SAGL può eseguire Audit con Breve Preavviso verso Organizzazioni già certificate, ad esempio per indagare su reclami ricevuti, in seguito a modifiche, o come azione conseguente ad eventuali sospensioni del certificato. Nel caso in cui siano decise attività di Audit con Breve Preavviso, **l’Organizzazione non può ricusare il GA** incaricato.

Pertanto, SI CERT SAGL si impegna a selezionare con particolare cura i componenti del GA. Quest’Audit è addebitato secondo quanto indicato in offerta per le attività supplementari.

La mancata accettazione da parte dell’Organizzazione certificata dell’esecuzione dell’Audit con Breve Preavviso comporta prima la sospensione e successivamente la revoca del certificato.

Inoltre, essendo SI CERT SAGL un Organismo accreditato, è sottoposto ad Audit da parte di SAS, che può espletarsi anche presso le sedi delle Organizzazioni certificate da SI CERT SAGL. In particolare, possono essere disposte da SAS, Audit Supplementari e/o Straordinari a seguito dell’identificazione di situazioni critiche, sia direttamente da parte di SAS, sia a fronte di segnalazioni e/o reclami scritti e oggettivamente motivati, pervenuti a SAS, o di situazioni inadeguate delle quali SAS viene a conoscenza. A tali Audit si applica un preavviso minimo di 7 (sette) giorni lavorativi. I costi degli Audit straordinari non sono a carico dell’Organizzazione, ma addebitati a SI CERT SAGL, oppure sono sostenuti direttamente da SAS.

Altri metodi di controllo sono adottati da SAS per verificare l’operatività di SI CERT SAGL (vedi paragrafo successivo).

6.8. AUDIT DI MARKET SURVEILLANCE

Essendo SI CERT SAGL un Organismo accreditato, è sottoposto ad Audit da parte di SAS, che può espletarsi anche presso le sedi delle Organizzazioni certificate da SI CERT SAGL. In particolare, possono essere disposti da SAS, Audit denominati di “Market Surveillance” presso l’Organizzazione certificata, condotte direttamente da Personale incaricato da SAS e non da SI CERT SAGL. L’Audit si svolge con l’aiuto di un questionario (riportato in allegato al documento IAF ID 04) e alla presenza del Personale dell’Organizzazione (usualmente il solo Responsabile del Sistema di Gestione) e di Personale di SI CERT SAGL (se possibile con la partecipazione di un componente del GA che ha condotto l’Audit più recente).

L’Organizzazione oggetto dell’attività di Audit di “Market Surveillance” è scelta direttamente da SAS, in base ad alcuni fattori di rischio (es: scopo del certificato, dimensioni dell’Organizzazione, GA).

I costi di tale Audit non sono carico dell’Organizzazione, ma addebitati a SI CERT SAGL. Nel caso in cui l’Organizzazione rifiuti di effettuare

tale l'Audit, SI CERT SAGL deve intraprendere l'iter di revoca del certificato.

6.9. AUDIT DA REMOTO

In caso di eventi eccezionali o casi particolari al di fuori del controllo dell'Organizzazione e di SI CERT SAGL, quali ad esempio: calamità naturali, pandemie, sommosse, terrorismo, ecc., SI CERT SAGL può decidere di eseguire Audit parziali o totali da remoto. Per questi Audit, eseguiti in conformità ai pertinenti documenti IAF ed alle direttive di SAS, le modalità sono di volta in volta concordate e gestite in collaborazione con le Organizzazioni che siano in grado di sostenere l'Audit da Remoto.

In via del tutto eccezionale, possono essere eseguiti Audit da Remoto anche per nuove certificazioni.

Infine, SI CERT SAGL si riserva la possibilità di effettuare parte dell'Audit da remoto in accordo ai documenti IAF e SAS, anche laddove non sussistano le succitate condizioni eccezionali o casi particolari. In tal caso Si Cert definisce le specifiche modalità da utilizzare in relazione a: schema di riferimento, settore IAF e tipologia di audit (vedi anche PG Gestione Attività di Valutazione da Remoto).

Ciò premesso, oltre a quanto sopra riportato, tuttavia affinché si possa effettuare un Audit da Remoto è necessario che siano soddisfatte almeno le seguenti condizioni:

- disponibilità dell'Organizzazione ad effettuare l'Audit da Remoto e dei Responsabili Interessati, con sottoscrizione di informativa al trattamento dei dati;
- disponibilità di adeguate dotazioni informatiche da parte dell'Organizzazione (PC con possibilità di connessione audio-visiva, buona connessione per la trasmissione dati sia in download, sia in upload) (…);
- condivisione della piattaforma informatica da utilizzare per il collegamento da remoto e possibilità di creare più riunioni virtuali e di condividere schemi e documenti.

6.10. SUBENTRO AD ALTRO ENTE

Qualora un'Organizzazione in possesso di certificazione emessa da altro Organismo di Certificazione accreditato da Ente che aderisce agli accordi di mutuo riconoscimento EA o IAF presenti una richiesta di subentro (transfert) a SI CERT SAGL, questi provvede ad applicare i criteri riportati nelle linee guida applicative EA/IAF. In pratica SI CERT SAGL provvede a:

- informarsi delle motivazioni che hanno portato alla richiesta da parte dell'Organizzazione già certificata;
- verificare l'accreditamento e lo stato di validità dell'accreditamento dell'Organismo di Certificazione che ha rilasciato il certificato;
- verificare la validità del certificato in base anche allo scopo, ai siti produttivi ed alle precedenti attività di Audit condotte dal precedente Organismo di Certificazione;
- verificare e riesaminare i documenti delle precedenti attività di Audit erogate dal precedente Organismo e sostenute dall'Organizzazione (registrazioni di tutti gli Audit dell'ultimo triennio e dell'eventuale analisi documentale eseguita); in caso di mancanza di tale documentazione, si deve prevedere iter per una nuova certificazione;
- verificare e riesaminare eventuali reclami ricevuti dall'Organizzazione e le relative azioni intraprese;
- verificare e riesaminare eventuali richieste da parte di Pubbliche Amministrazioni o verbali/sanzioni per sopralluoghi di Organi di Controllo;
- verificare l'assenza di pendenze e contenziosi legali.

In seguito alla verifica della completezza e adeguatezza della documentazione acquisita (pre-transfer review), SI CERT SAGL o suo Business Partner emette la propria proposta economica che invia all'Organizzazione unitamente al Regolamento Certificazione.

A seguito ricezione dell'avvenuta accettazione dell'offerta e delle condizioni contrattuali da parte dell'Organizzazione, SI CERT SAGL provvede a pianificare le attività di Audit da svolgere. Nello specifico si sottolinea che:

- l'Audit in campo in fase di trasferimento del certificato (pre-transfer visit) è obbligatorio se dall'esame documentale (pre-transfer review) emerge la necessità, ad esempio in caso di NC maggiori non chiuse (il pre-transfer visit non si configura come Audit);
- l'attività di trasferimento di un certificato non può coincidere con un Audit di Sorveglianza o Rinnovo, per cui è necessario prima completare l'attività di transfer (esame documentale + eventuale pre-transfer visit), e solo dopo può essere svolto l'Audit di Sorveglianza o Rinnovo;
- dopo l'attività di transfer (esame documentale + eventuale pre-transfer visit), segue una normale attività di decisione per il rilascio della certificazione, svolta da Personale indipendente da chi ha svolto l'esame documentale e l'eventuale pre-transfer visit.

Nel caso in cui la richiesta di subentro provenga da un'Organizzazione il cui certificato è stato rilasciato da un Organismo di Certificazione il cui accreditamento è sospeso o revocato, o che abbia comunque cessato di operare, il certificato può essere trasferito entro un periodo massimo di 6 mesi o entro la scadenza della certificazione se precedente, e comunque sempre con l'effettuazione di un Audit in campo. In questi casi deve essere sempre informato SAS prima del trasferimento. Oltre i 6 mesi, si deve gestire la pratica come nuova certificazione

(Audit S1 + Audit S2).

I rapporti contrattuali tra SI CERT SAGL e l'Organizzazione che ha richiesto il subentro della certificazione sono gestiti secondo quanto riportato nel Regolamento Certificazione.

7. CLASSIFICAZIONE E GESTIONE RILIEVI

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

7.1. 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 sono risolte, mentre, per quelle riscontrate in fase di Audit di Sorveglianza se, scaduto il termine di 3 mesi per la loro risoluzione, queste non sono 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'attività per la verifica 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'attività di verifica 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 e 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'attività di verifica 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.

7.2. 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 della 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 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 e 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.

Per l'attività di verifica della correzione delle NC minori 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 minori, il RGA provvede al completamento delle apposite sezioni dei documenti utilizzati per questa attività e 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.
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.

7.3. 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 e 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.

8. EMISSIONE E VALIDITÀ DEL CERTIFICATO

Il Certificato ha validità triennale a partire dalla data di emissione (data di certificazione e/o rinnovo) ed 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, che hanno cadenza annuale e comunque devono effettuarsi entro l'anno solare di competenza, oltre ad una completa rivalutazione (Audit di Rinnovo) ogni 3 anni, entro il termine della scadenza del certificato stesso, nel caso l'Organizzazione intenda rinnovare con SI CERT SAGL la propria certificazione per un ulteriore triennio, fatto salvo quanto previsto dal Regolamento Certificazione in materia di recesso contrattuale.
Al fine di dare evidenza dello stato di validità o meno di un certificato e del rispetto dei contenuti del Regolamento Certificazione, sul certificato sono indicate:

1) **La data di prima emissione del certificato:** questa data è relativa alla prima emissione del certificato corrispondente alla pertinente decisione di certificazione; in caso di subentro ad una certificazione in corso di validità per la quale è stato possibile effettuare tale subentro, corrisponde alla data del certificato emesso dal precedente Organismo di Certificazione.
2) **La data di emissione corrente:** questa data è relativa ad ogni variazione intervenuta rispetto alla certificazione inziale, per esempio per variazione delle sedi e/o degli indirizzi, per modiche allo scopo di certificazione per effetto di estensione o riduzione dello stesso, ecc..; tale data è anche aggiornata in occasione dell'aggiornamento dello stato di validità, come sotto riportato.

3) **La data di scadenza del certificato (ciclo):** questa data indica la scadenza del ciclo contrattuale del certificato che, secondo quando previsto dai requisiti a cui un Organismo di Certificazione deve rispondere, ha una durata di 3 anni meno un giorno dalla data di prima emissione o emissione per rinnovo del certificato.
4) **Periodo di non validità del certificato:** indica il periodo di non validità del certificato con le diciture: *Dal gg.mm.aaaa*, *Al gg.mm.aaaaa*; queste date sono indicate nel caso in cui l'Audit di Rinnovo sia eseguito oltre la data di scadenza del certificato (ciclo), comunque entro 6 mesi dalla data stessa, e stanno ad indicare la non continuità del certificato stesso per il periodo indicato (vedi § 6.4 "Audit di Rinnovo").

(…)

Si precisa che la non effettuazione dell'Audit di Sorveglianza o Supplementari entro la data prevista, per contingenze dell'Organizzazione non comunicate a SI CERT SAGL al fine di concordare i successivi step da seguire, determina l'immediata sospensione della certificazione e l'attivazione della procedura legale per il recupero del credito vantato.

Allo stesso modo, si precisa che la non effettuazione dell'Audit di Rinnovo entro la data (…) di scadenza ciclo, come sopra riportato, per contingenze dell'Organizzazione non comunicate a SI CERT SAGL al fine di concordare i successivi step da seguire, determina l'immediata revoca della certificazione e l'attivazione della procedura legale per il recupero del credito vantato.

9. EVENTUALI REQUISITI AGGIUNTIVI

Nessuno

10. NOTE DI APPROVAZIONE DEL REGOLAMENTO

Ai fini dell'approvazione del Regolamento Certificazione ("Regolamento Certificazione - Requisiti Generali" e del presente "Regolamento Certificazione - Requisiti Tecnici") e dei capitoli e paragrafi in esso contenuti, il Legale Rappresentante dell'Organizzazione può procedere a firmare, anche mediante la propria firma elettronica, la specifica parte dell'offerta economica ricevuta e, nel caso di offerta emessa dal Business Partner, del contratto, con particolare riferimento ai capitoli e paragrafi del Regolamento Certificazione indicati.