



**GRUPPO
ISTITUTO ITALIANO DELLA SALDATURA**

REGOLAMENTO PER LA CERTIFICAZIONE DI SISTEMA

Documento n° CER_QAS 019 R

INDICE

1	SCOPO E CAMPO DI APPLICAZIONE
2	RIFERIMENTI
3	DEFINIZIONI
4	REQUISITI PER LA CERTIFICAZIONE
5	CERTIFICAZIONE INIZIALE
6	MANTENIMENTO DELLA CERTIFICAZIONE
7	RINNOVO
8	GESTIONE DEI CERTIFICATI DI CONFORMITÀ
9	MODIFICA DELLA CERTIFICAZIONE E COMUNICAZIONE DEI CAMBIAMENTI
10	ORGANIZZAZIONI MULTISITO
11	SPECIFICITÀ PER I SETTORI IAF 28, IAF 34, IAF 35
12	TRASFERIMENTO DI CERTIFICATI ACCREDITATI
13	SOSPENSIONE, RIPRISTINO E REVOCA DELLA CERTIFICAZIONE
14	RINUNCIA ALLA CERTIFICAZIONE
15	UNIFICAZIONE DELLE DATE DI VISITA PER DIVERSE CERTIFICAZIONI
16	DOCUMENTI DI REGISTRAZIONE
17	CONDIZIONI CONTRATTUALI
ALLEGATI	
A	Particolarità per la certificazione di sistemi di gestione per la qualità
B	Particolarità per la certificazione di sistemi di gestione ambientale
C	Particolarità per la certificazione di sistemi di gestione per la salute e la sicurezza sul lavoro

1 REGOLAMENTO PER LA CERTIFICAZIONE DI SISTEMA SCOPO E CAMPO DI APPLICAZIONE

- 1.1** Il presente Regolamento definisce i criteri che IIS CERT applica nelle attività di certificazione di sistemi di gestione (qualità, ambiente, salute e sicurezza).
Esso tratta le modalità di richiesta, ottenimento, mantenimento ed utilizzazione, nonché l'eventuale sospensione e revoca di tale certificazione.
- Il Regolamento è suddiviso in:
- una Parte generale, comune ai tre schemi suddetti;
 - tre Allegati, cioè un Allegato specifico per ciascuno schema (qualità, ambiente, salute e sicurezza).
- Gli Allegati richiamano nella numerazione dei paragrafi i corrispondenti paragrafi del Regolamento per i quali sono introdotti requisiti aggiuntivi.
- 1.2** Per quanto non previsto dal presente documento, si richiamano le condizioni generali di contratto stabilite nel regolamento CER_QAS 017 R (vedere § 2) reperibile sul sito web di IIS CERT.
- 1.3** IIS CERT rilascia la certificazione in accordo ai requisiti della norma UNI CEI EN ISO/IEC 17021-1 ad Organizzazioni il cui sistema di gestione sia stato riconosciuto conforme a tutti i requisiti previsti dalla norma o documento normativo di riferimento.
- 1.4** L'accesso alla certificazione è aperto a tutte le Organizzazioni e non è condizionato dalla loro appartenenza o meno a qualsiasi Associazione o Gruppo.
Per l'attività certificativa, IIS CERT applica le proprie tariffe vigenti, garantendone l'equità e l'uniformità di applicazione.
IIS CERT può legittimamente non accettare richieste di certificazione che riguardino Organizzazioni sottoposte, o la cui produzione o attività sia sottoposta, a misure restrittive, sospensive o interdittive da parte di una pubblica Autorità.
- 1.5** La certificazione rilasciata da IIS CERT è riferita esclusivamente alla singola Organizzazione, dove per Organizzazione si intende un gruppo, società, azienda, impresa, ente o istituzione, ovvero loro parti o combinazioni, in forma associata o meno, pubblica o privata, che abbia una propria struttura funzionale ed amministrativa.
Per Organizzazioni con più unità operative, ogni singola unità operativa può essere definita come Organizzazione.
- 1.6** ACCREDIA, quale Organismo garante delle certificazioni emesse da IIS CERT, può richiedere la partecipazione di suoi osservatori agli audit effettuati da IIS CERT stesso, allo scopo di accertare che le modalità di valutazione adottate da IIS CERT siano conformi alle norme per esso applicabili; la partecipazione di tali osservatori è previamente concordata tra IIS CERT e l'Organizzazione.
- Inoltre, ACCREDIA può richiedere di effettuare direttamente proprie verifiche presso le Organizzazioni certificate, nella modalità definita *Market Surveillance*, che consiste in una visita breve di un giorno per verificare il grado di fiducia nella conformità del sistema di gestione a requisiti specifici nonché l'efficacia del processo di certificazione accreditata.
- Il diniego da parte dell'Organizzazione a concedere il proprio benessere per le suddette verifiche può comportare la sospensione e successivamente la revoca della certificazione.

2 RIFERIMENTI

CER_QAS 002 R	Regolamento per l'uso del marchio IIS CERT
CER_QAS 017 R	Regolamento per le valutazioni di sistema, personale, prodotto – Condizioni generali di contratto
CER_QAS 024 R	Regolamento per la certificazione dei costruttori secondo:

	- Schemi EWF/IIW (ISO 3834, EMS, SMS)
	- EN 15085
UNI EN ISO 9000	Sistemi di gestione per la qualità – Fondamenti e vocabolario
UNI EN ISO 9001	Sistemi di gestione per la qualità – Requisiti
UNI EN ISO 14001	Sistemi di gestione ambientale – Requisiti e guida per l'uso
BS OHSAS 18001	Occupational health and safety management systems – Requirements
UNI EN ISO 3834-2	Requisiti di qualità per la saldatura per fusione dei materiali metallici – Parte 2: Requisiti di qualità estesi
UNI EN ISO 3834-3	Requisiti di qualità per la saldatura per fusione dei materiali metallici – Parte 3: Requisiti di qualità normali
UNI EN ISO 3834-4	Requisiti di qualità per la saldatura per fusione dei materiali metallici – Parte 4: Requisiti di qualità elementari
UNI EN ISO 19011	Linee guida per audit di sistemi di gestione
UNI CEI EN ISO/IEC 17000	Valutazione della conformità – Vocabolario e principi generali
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
IAF MD 1	Certification of Multiple Sites Based on Sampling
IAF MD 2	Transfer of Accredited Certification of Management Systems
IAF MD 5	Duration of QMS and EMS Audits
IAF MD 11	Application of ISO/IEC 17021 for Audits of Integrated Management Systems
IAF ID 4	Market Surveillance Visits to Certified Organizations
EA-6/02	Guidelines on the use of EN 45011 and ISO/IEC 17021 for certification to EN ISO 3834
EA-7/04	Legal Compliance as a part of Accredited ISO 14001:2004 certification
RG-01 (doc. ACCREDIA)	Regolamento per l'accreditamento degli Organismi di Certificazione e Ispezione – Parte generale
RG-01-01 (doc. ACCREDIA)	Regolamento per l'accreditamento degli Organismi di Certificazione del sistema di gestione
RG-09 (doc. ACCREDIA)	Regolamento per l'utilizzo del marchio ACCREDIA
RT-05 (doc. ACCREDIA)	Prescrizioni per l'accreditamento degli Organismi operanti la valutazione e certificazione dei sistemi di gestione per la qualità delle imprese di costruzione ed installazione di impianti e servizi (sett. EA 28)
RT-09 (doc. ACCREDIA)	Prescrizioni per l'accreditamento degli organismi operanti la certificazione dei sistemi di gestione ambientale (SGA)
RT-12 (doc. ACCREDIA)	Prescrizioni per l'accreditamento degli Organismi di Certificazione operanti la certificazione dei sistemi di gestione per la salute e la sicurezza dei lavoratori
Disposizione ACCREDIA	Disposizione in materia di Accredimento nello schema SCR [del 2012-02-23]

I documenti di riferimento citati sono applicati nell'ultima edizione e/o revisione valida (vedere anche Nota successiva).

Nota *Relativamente alla ISO 9001 ed alla ISO 14001, si intendono applicabili come riferimenti sia rispettivamente le edizioni 2008 e 2004, che la edizione 2015, fino al termine del relativo periodo di transizione.*

3 DEFINIZIONI

Si applicano in generale le definizioni delle norme della serie ISO/IEC 17000 (vedere § 2). Inoltre, per quanto riguarda i termini generali relativi alla qualità e all'accreditamento, si usano le definizioni delle norme UNI EN ISO 9000 ed UNI CEI EN ISO/IEC 17000 (con preferenza per la seconda nel caso di differenze), integrate dalle seguenti.

Rilievo:	Riscontro ottenuto da IIS CERT nel corso degli audit condotti sulle Organizzazioni e formalizzato nei relativi rapporti di audit. Ai fini del presente Regolamento, i rilievi sono suddivisi in:
-----------------	---

	<ul style="list-style-type: none"> - non conformità; - osservazioni; - commenti.
Non conformità:	<p>Mancato soddisfacimento, da parte di un'Organizzazione, di un requisito stabilito dai riferimenti normativi applicabili (documento di riferimento ⁽¹⁾, regolamento presente, regolamenti CER_QAS 002 R e CER_QAS 017 R).</p> <p>La condizione di non soddisfacimento di un requisito può essere dovuta ad una o ad ambedue le cause seguenti:</p> <ul style="list-style-type: none"> a) mancata o insufficiente presa in considerazione del requisito medesimo e/o mancata o insufficiente definizione dei criteri e modalità adottati per il soddisfacimento del requisito stesso; b) mancata o insufficiente attuazione pratica di suddetti criteri e modalità attuative. <p>Ai fini delle prescrizioni contenute nel presente Regolamento, un rilievo viene classificato come non conformità quando il mancato soddisfacimento del corrispondente requisito nelle forme sopra specificate è tale da compromettere il valore delle certificazioni rilasciate da IIS CERT in termini di efficace e credibile assicurazione della conformità dell'oggetto delle certificazioni medesime.</p> <p><i>Nota: Il rilievo definito da IIS CERT come "Non conformità" è indicato nella ISO/IEC 17021-1 (vedere § 2) come "Non conformità maggiore".</i></p>
Osservazione:	<p>Il rilievo formalizzato da IIS CERT nei confronti dell'Organizzazione è classificato come osservazione quando il mancato soddisfacimento del requisito, pur essendo indicativo di un comportamento inadeguato da parte dell'Organizzazione e, come tale, necessitante di correzione, non è tale da compromettere immediatamente il valore delle certificazioni rilasciate nei termini sopra evidenziati.</p> <p><i>Nota: Il rilievo definito da IIS CERT come "Osservazione" è indicato nella ISO/IEC 17021-1 (vedere § 2) come "Non conformità minore".</i></p>
Commento:	<p>Il rilievo sollevato da IIS CERT nei confronti dell'Organizzazione è classificato come commento quando non è conseguente al riscontro di una situazione oggettiva di mancato soddisfacimento di un requisito, ma è finalizzato a prevenire che tale situazione si verifichi (in quanto potenzialmente realizzabile) e/o a fornire indicazioni per il miglioramento delle prestazioni dell'Organizzazione.</p>
Risultanza:	<p>Riscontro ottenuto da IIS CERT esclusivamente nel corso degli audit preliminari e di stage 1.</p> <p>Nel primo caso, si tratta di indicazioni sullo stato di applicazione della norma; nel secondo caso, si tratta di indicazioni che potranno, se non opportunamente gestite da parte dell'Organizzazione, trasformarsi in "rilievi".</p>
<p>Note:</p> <p>(1) come documento di riferimento si intende ISO 9001, oppure ISO 14001, oppure OHSAS 18001, oppure ISO 3834 (Parte 2, 3 o 4).</p>	

4 REQUISITI PER LA CERTIFICAZIONE

4.1 Per ottenere la certificazione da parte di IIS CERT, un sistema di gestione deve soddisfare inizialmente e nel tempo i requisiti della norma o documento normativo di riferimento e quelli indicati ai punti seguenti, oltre ad eventuali elementi aggiuntivi previsti dagli Organismi di accreditamento (es. documenti "RT" emessi da ACCREDIA).

Nell'ambito dell'accREDITamento, infatti, IIS CERT si attiene a determinati documenti di riferimento emessi dagli Organismi di accREDITamento stessi.

Tali documenti sono reperibili contattando IIS CERT o direttamente gli Organismi di accREDITamento (ad esempio consultando i relativi siti web).

4.2 In particolare, per ottenere la certificazione del sistema di gestione, l'Organizzazione deve:

a) aver istituito e mantenuto attivo e completamente operativo un sistema di gestione in totale ottemperanza ai requisiti della norma o documento normativo di riferimento.

Il sistema di gestione si intende completamente operativo quando:

- il sistema di audit interni è completamente attuato ed è possibile dimostrarne l'efficacia;
- è stato svolto e documentato almeno un riesame del sistema da parte della direzione;
- sono stati determinati gli obiettivi ed i processi necessari ad ottenere risultati in accordo con i requisiti del cliente e con le politiche aziendali;
- sono stati sviluppati tali processi;
- sono stati effettuati e registrati monitoraggi e misure dei processi e dei prodotti rispetto alle politiche, agli

- obiettivi ed ai requisiti per il prodotto;
- sono state messe in atto azioni per il miglioramento continuo dei processi.
- b) disporre di un Manuale (vedere Nota 1) che:
- definisca lo scopo/campo di applicazione del sistema di gestione, descriva i principali processi ed elementi del sistema e le loro interazioni e contenga o richiami le relative procedure documentate; la descrizione dei processi e delle loro interazioni deve essere estesa a tutti quelli sviluppati dall'Organizzazione (anche a processi affidati all'esterno) necessari alla realizzazione di un determinato prodotto/servizio, determinanti ai fini della capacità del prodotto/servizio stesso di soddisfare i requisiti applicabili (tale descrizione può avvenire in vario modo come descrizioni, schemi di flusso o logogrammi, tabelle o matrici, etc.);
 - evidenzi le eventuali esclusioni (vedere Nota 2) di requisiti della norma e/o di linee di produzione, nei limiti consentiti, illustrandone in modo adeguato le motivazioni;
 - prenda in considerazione i requisiti della norma e fornisca una descrizione, anche breve, delle risorse e dei procedimenti posti in atto per assicurare la conformità a tali requisiti;
 - contenga una adeguata descrizione dell'Organizzazione aziendale.

Nota 1 *Il Manuale non è richiesto nel caso di certificazione di conformità alle ISO 9001:2015 ed ISO 14001:2015.*

Nota 2 *Le esclusioni non sono applicabili per le ISO 9001:2015 ed ISO 14001:2015.*

- 4.3** I requisiti di cui al § 4.2 sono verificati da IIS CERT attraverso un processo di audit iniziale composto da due stage:
- a) audit di stage 1, che può essere effettuato:
- in parte in ufficio (per un massimo del 10% del totale del tempo previsto) ed in parte presso il sito dell'Organizzazione, oppure
 - completamente presso il/i sito/i dell'Organizzazione;
- b) audit di stage 2, presso il/i sito/i dell'Organizzazione.
- Le peculiarità dell'audit iniziale sono dettagliate nel capitolo successivo.

5 CERTIFICAZIONE INIZIALE

5.1 Condizioni generali

Le Organizzazioni che intendono ottenere la certificazione del proprio sistema di gestione devono fornire ad IIS CERT i dati essenziali della loro Organizzazione e relative attività svolte e la localizzazione del sito/i, inviando l'apposita domanda compilata in tutte le sue parti (disponibile sul sito www.iiscert.it), sulla base dei quali viene formulata da IIS CERT un'offerta economica (sotto forma di contratto da controfirmare).

Tali informazioni sono richieste allo scopo di verificare preventivamente l'applicazione di alcuni requisiti della norma e di predisporre un'offerta economica adeguata.

Le Organizzazioni, in caso di accettazione dell'offerta economica, formalizzano la richiesta di certificazione inviando ad IIS CERT la domanda di certificazione, contenente informazioni relative a:

- scopo di certificazione richiesto;
- siti interessati alla certificazione, con relativi processi ed attività operative, risorse umane e tecniche (ove applicabile), obblighi legali;
- processi affidati all'esterno utilizzati dall'Organizzazione che influenzano la conformità ai requisiti;
- norma a fronte della quale è richiesta la certificazione;
- presenza eventuale di consulenza esterna, con relativi estremi;
- presenza eventuale di turni.

Al ricevimento della domanda di certificazione, IIS CERT effettua un riesame della documentazione ricevuta allo scopo di accertarsi che:

- le informazioni ricevute siano sufficienti a sviluppare un programma di audit;
- siano chiarite eventuali divergenze di comprensione;
- abbia le competenze per realizzare le attività di certificazione richieste;
- siano presi in considerazione lo scopo di certificazione, i siti del richiedente, i tempi richiesti per l'audit

ed altri elementi che possano influenzare la specifica attività di certificazione richiesta.

Effettuato il riesame, IIS CERT invia all'Organizzazione per iscritto la conferma di accettazione della domanda.

La domanda dell'Organizzazione, nella quale è espressamente richiamato il presente Regolamento, e la relativa accettazione da parte di IIS CERT formalizzano contrattualmente il rapporto tra IIS CERT e l'Organizzazione e l'applicabilità del presente Regolamento.

Il contratto stipulato tra IIS CERT e l'Organizzazione comprende:

- l'audit iniziale composto da due stage e, in caso di esito positivo, il rilascio del certificato;
- i successivi audit di sorveglianza e di ricertificazione;
- eventuali servizi aggiuntivi specificati nell'offerta (es. un audit preliminare, se richiesto).

5.2 Audit preliminare

Dietro formale richiesta dell'Organizzazione, può essere effettuato, prima dell'audit di valutazione, un audit preliminare del sistema, per verificarne lo stato generale di applicazione.

Tale audit preliminare è condotto in modo da esaminare i requisiti della norma, senza seguire le prassi formali previste per l'attività di valutazione (es. non sono utilizzate liste di riscontro).

L'Organizzazione è informata del risultato con un rapporto di audit.

I risultati sono registrati come "risultanze" (vedere § 3).

5.3 Documentazione richiesta

Unitamente alla richiesta di certificazione, o successivamente alla stessa, l'Organizzazione dovrà rendere disponibile a IIS CERT la seguente documentazione:

- manuale del sistema di gestione (non richiesto nel caso di richiesta di certificazione di conformità alla ISO 9001:2015 o alla ISO 14001:2015), che descriva la politica, gli obiettivi ed i programmi per il sistema di gestione;
- copia della visura camerale, quale evidenza dell'esistenza dell'Organizzazione e dell'attività effettuata;
- pianta del sito o dei siti (non per la ISO 9001);
- elenco delle principali leggi e/o regolamenti applicabili (al prodotto/servizio fornito o necessarie per la corretta applicazione del sistema di gestione);
- elenco dei cantieri in corso, con descrizione delle attività ivi espletate, ove applicabile.

IIS CERT può richiedere a sua discrezione, per esame, anche altri documenti oltre quelli indicati in precedenza, giudicati importanti ai fini della valutazione del sistema di gestione (vedere anche Nota successiva).

La documentazione di cui sopra è valutata da IIS CERT per conformità alla norma di riferimento ed ai requisiti del presente Regolamento.

Nota Qualora IIS CERT prendesse in considerazione una eventuale certificazione già rilasciata da altri, l'Organizzazione dovrà anche rendere disponibile le relative evidenze (come rapporti, azioni correttive, etc.); il trasferimento di una certificazione emessa sotto accreditamento è trattato in dettaglio al § 12 del presente regolamento.

5.4 Audit di stage 1

IIS CERT comunica all'Organizzazione i nomi degli Auditor incaricati dell'effettuazione dell'audit di stage 1 e dell'audit di stage 2 (vedere anche Nota 1 successiva); l'Organizzazione può fare obiezione sulla nomina di tali Auditor, entro 5 giorni dalla nomina stessa, giustificandone i motivi.

Durante l'audit iniziale, l'Organizzazione deve dimostrare che il sistema di gestione è pienamente operante e di applicare effettivamente il sistema stesso e le relative procedure documentate.

Le finalità dell'audit di stage 1 sono:

- sottoporre ad audit la documentazione del sistema di gestione del cliente;
- valutare la localizzazione e le condizioni particolari del sito del cliente e intraprendere uno scambio di informazioni con il personale del cliente al fine di stabilire il grado di preparazione per l'audit di stage 2;
- riesaminare lo stato e la comprensione del cliente riguardo i requisiti della norma, con particolare riferimento all'identificazione di prestazioni chiave o di aspetti, processi, obiettivi e funzionamento

significativi del sistema di gestione;

- raccogliere le informazioni necessarie riguardanti il campo di applicazione del sistema di gestione, i processi e le localizzazioni del cliente, compresi i relativi aspetti legali e regolamentari e la conformità ad essi;
- riesaminare l'assegnazione di risorse per l'audit di stage 2 e concordare con il cliente i dettagli di tale audit;
- mettere a fuoco la pianificazione dell'audit di stage 2, acquisendo una sufficiente conoscenza del sistema di gestione e delle attività del sito del cliente, con riferimento ai possibili aspetti significativi;
- valutare se gli audit interni e il riesame da parte della direzione siano stati pianificati ed eseguiti e che il livello di attuazione del sistema di gestione fornisca l'evidenza che il cliente è pronto per l'audit di stage 2.

L'esito dell'audit di stage 1 è comunicato all'Organizzazione con un apposito rapporto di audit di stage 1 (vedere anche Nota 2 successiva), sul quale sono tra l'altro riportate tutte le risultanze, incluse quelle che potrebbero essere classificate come non conformità durante l'audit di stage 2: queste ultime dovranno essere risolte prima di procedere con l'audit di stage 2; la presenza di risultanze particolarmente critiche potrebbe portare al rinvio o alla cancellazione delle stage 2, così come la necessità di cambiamenti significativi con impatto sul sistema di gestione potrebbero comportare la ripetizione (totale o parziale) dello stage 1 (entrambe le circostanze sarebbero indicate nel rapporto di stage 1).

Le azioni intraprese dall'Organizzazione per il trattamento delle risultanze sono verificate durante l'audit di stage 2.

L'audit di stage 2 dovrà essere effettuato entro un termine massimo di 12 mesi dalla conclusione dell'audit di stage 1, oltre il quale dovrà essere ripetuto l'audit di stage 1.

Nota 1 *Nella assegnazione degli Auditor, IIS CERT tiene in considerazione i seguenti elementi:*

- obiettivi, scopo, criteri e tempi stimati dell'audit;
- eventualità di effettuare audit combinati, congiunti o integrati;
- competenza globale necessaria per raggiungere gli obiettivi dell'audit;
- requisiti di certificazione, compresi quelli di natura legislativa, regolamentare e/o contrattuale;
- lingua e cultura.

All'audit possono anche presenziare uno o più esperti tecnici, previo accordo con l'Organizzazione.

Nota 2 *In caso di stage 1 e stage 2 effettuati in modo consecutivo, potrà essere emesso un unico rapporto, comprensivo degli esiti di entrambe le fasi.*

5.5 Audit di stage 2

L'audit di stage 2 è effettuato presso l'Organizzazione al fine di verificare la corretta ed efficace attuazione del sistema di gestione; in particolare, l'attività di audit prevede la ricerca di evidenze relative a:

- conformità relativa a tutti i requisiti della norma del sistema di gestione interessato;
- monitoraggio, misurazione, reportazione e riesame sui principali obiettivi di prestazione;
- capacità del sistema di gestione analizzato di adempiere a tutti i requisiti legislativi, regolamentari e contrattuali applicabili;
- controllo operativo dei processi aziendali;
- audit interno e riesame della direzione;
- responsabilità della direzione a riguardo delle politiche dei clienti.

IIS CERT invia all'Organizzazione, prima dell'effettuazione dell'audit di stage 2 presso il/i sito/i, un piano di audit dove è riportata la descrizione delle attività e delle disposizioni per la conduzione dell'audit.

Qualora le attività da verificare siano svolte su più siti operativi, l'audit è svolto secondo criteri previamente stabiliti e comunicati da IIS CERT all'Organizzazione.

5.5.1 Dettagli operativi

5.5.1.1 Riunione di apertura

Prima di effettuare l'audit di valutazione, il gruppo di audit (GV) esegue la riunione di apertura, verbalizzando sul rapporto di audit l'incontro con la Direzione dell'Organizzazione o il suo Rappresentante ed i principali responsabili di funzione.

Nel corso dell'incontro, il Responsabile del GV (RGV):

- presenta i componenti del GV;

- illustra e fornisce eventuali chiarimenti sul piano di audit;
- fornisce un breve sommario sulle modalità di conduzione dell'audit;
- richiede la definizione dei canali ufficiali di comunicazione tra il GV e l'Organizzazione;
- richiede, ove applicabile, di impegnare più persone al fine di permettere agli Auditor di operare separatamente;
- ribadisce l'impegno alla riservatezza degli Auditor e di tutto il personale coinvolto nella pratica di certificazione;
- ribadisce che l'eventuale consulente, utilizzato per la predisposizione della documentazione, rispetti rigorosamente il ruolo di osservatore;
- ribadisce che l'audit è di natura campionatoria;
- precisa che l'audit riguarda il prodotto/servizio relativo alla certificazione, come definito nello Stage 1;
- definisce la data e l'ora della riunione di chiusura;
- presenta gli ispettori di ACCREDIA, quando presenti.

5.5.1.2 Conduzione dell'audit

Durante l'audit, l'Organizzazione è tenuta a mettere a disposizione il personale e a concedere libero accesso alle aree aziendali, alle informazioni e alla documentazione relativa alla norma per la quale è stata richiesta la certificazione, oltre a fornire assistenza agli Auditor di IIS CERT.

L'applicazione dei requisiti è verificata mediante:

- interviste al personale coinvolto nelle attività (a tutti i livelli);
- esame di documenti, procedure, rapporti, etc. per verificare la conformità ai documenti di riferimento;
- verifica delle eventuali esclusioni;
- corretta definizione dello scopo della certificazione.

La verifica viene effettuata con l'ausilio dei questionari applicabili su cui possono essere annotate le osservazioni e le carenze riscontrate.

Nota Qualora nel corso degli audit, tenuto conto della natura campionatoria delle medesime, venissero incidentalmente riscontrate da parte di IIS CERT inosservanze di requisiti di legge non riguardanti aspetti direttamente correlati al sistema valutato o al prodotto ispezionato, ma correlati ad altri aspetti delle attività svolte dall'Organizzazione, tali anomalie vengono debitamente registrate dagli Auditor in modo disgiunto dal rapporto di audit e tempestivamente portate a conoscenza della Direzione dell'Organizzazione valutata, affinché questa provveda ai trattamenti ed alle azioni correttive applicabili; la registrazione viene altresì trasmessa alla Direzione di IIS CERT per le valutazioni del caso.

5.5.1.3 Riunione del Gruppo di audit

Al termine della verifica e prima della riunione di chiusura, il GV si riunisce per:

- verificare di aver considerato tutti i requisiti applicabili della norma oggetto della certificazione;
- descrivere le eventuali non conformità nell'apposito rapporto (Mod. CSQ 020);
- elaborare il rapporto di audit in cui riportare le eventuali osservazioni e/o commenti.

5.5.1.4 Riunione di chiusura

L'audit di valutazione termina con la riunione di chiusura, in cui l'RGV illustra ai rappresentanti dell'Organizzazione:

- gli eventuali rapporti di non conformità;
- le eventuali osservazioni e/o commenti (descritti nel rapporto di audit);
- il rapporto di audit.

I documenti suddetti sono consegnati al rappresentante dell'Organizzazione, che se d'accordo li firma per accettazione e ne trattiene copia, se non è d'accordo esplicita le proprie riserve nello spazio apposito del rapporto di audit.

5.6 Conclusioni dell'audit

Al termine dell'audit di stage 2 è consegnato all'Organizzazione il rapporto di audit (vedere Nota successiva).

Nota *Il rapporto di audit include o fa riferimento ai seguenti elementi:*

- *identificazione di IIS CERT;*
- *riferimenti ed indirizzo dell'Organizzazione;*
- *tipo di audit;*
- *criteri, obiettivi e scopo dell'audit;*
- *eventuali deviazioni dal piano di audit, con relative giustificazioni;*
- *eventuali circostanze particolari che hanno avuto impatto sull'audit;*
- *identificazione dell'RGV e di tutti gli Auditor;*
- *date e siti dove sono state effettuate le attività di audit;*
- *eventuali rilievi riscontrati;*
- *eventuali cambiamenti significativi intercorsi dal precedente audit aventi impatto sul sistema di gestione;*
- *eventuale effettuazione di audit combinato, integrato o congiunto;*
- *eventuali questioni irrisolte;*
- *dichiarazione indicante che l'audit è stato basato sul campionamento delle informazioni disponibili;*
- *raccomandazione da parte del GV;*
- *evidenza del corretto uso del marchio di IIS CERT;*
- *verifica dell'efficacia delle azioni intraprese a seguito dei rilievi dell'audit precedente (ove applicabile);*
- *dichiarazione sulla conformità e sull'efficacia del sistema di gestione;*
- *sintesi sulla capacità del sistema di gestione di soddisfare i requisiti applicabili ed i risultati attesi;*
- *conclusioni sull'adeguatezza dello scopo di certificazione;*
- *conferma che gli obiettivi dell'audit sono stati realizzati.*

L'Organizzazione può annotare sue eventuali riserve, in merito ai rilievi espressi da IIS CERT, su un apposito spazio del rapporto di audit.

Il contenuto di tale rapporto è successivamente confermato da IIS CERT tramite una comunicazione scritta; in assenza di comunicazione scritta da parte di IIS CERT, il rapporto si ritiene confermato dopo 15 giorni dalla sua consegna all'Organizzazione.

Tutte le eventuali non conformità formalizzate da IIS CERT in base ai criteri sopra enunciati devono formare oggetto dei necessari trattamenti e azioni correttive da parte dell'Organizzazione, i quali devono essere inviati ad IIS CERT entro 30 giorni solari dalla loro emissione per la loro approvazione.

IIS CERT si riserva entro 15 giorni solari di richiedere variazioni relative al contenuto del rapporto di audit e alle eventuali non conformità formulate dagli Auditor; passato tale termine, sia il rapporto che i rilievi si ritengono approvati, con il silenzio-assenso.

In presenza di non conformità, la certificazione o l'estensione non vengono concessi fino alla conferma dell'avvenuta applicazione dei necessari trattamenti, chiusura delle corrispondenti azioni correttive e relativa verifica di efficacia da parte di IIS CERT (generalmente effettuata dall'RGV); l'accettazione di tali proposte e dei tempi previsti per l'attuazione è comunicata all'Organizzazione in forma scritta.

Qualora non sia possibile verificare l'attuazione dei trattamenti e delle azioni correttive entro 6 mesi dal termine dello stage 2, IIS CERT effettuerà un secondo stage 2 prima di prendere la decisione sulla certificazione.

Nel caso di eventuali osservazioni, la certificazione viene concessa previa approvazione, da parte di IIS CERT, di un apposito piano di trattamenti ed azioni correttive che l'Organizzazione deve fornire ad IIS CERT entro 30 giorni solari dalla emissione delle osservazioni relative.

5.7 Audit aggiuntivi

In presenza di non conformità, il processo di certificazione è sospeso; nel caso di osservazioni la cui numerosità e/o tipologia, a giudizio del gruppo di audit, sia tale da pregiudicare il corretto funzionamento del sistema di gestione, il processo di certificazione è ugualmente sospeso.

In tali casi, IIS CERT effettuerà, entro 6 mesi, un audit aggiuntivo, presso la sede dell'Organizzazione, finalizzato a verificare l'efficacia dei trattamenti e delle azioni correttive proposte; in caso di esito positivo di tale audit, il processo di certificazione è ripreso.

L'audit aggiuntivo può essere effettuato sul sito dell'Organizzazione oppure su base documentale presso la sede di IIS CERT, in base alla tipologia delle azioni correttive da verificare a giudizio del team di audit.

Tutte le spese relative ad eventuali audit aggiuntivi conseguenti a carenze del sistema di gestione sono da considerarsi a carico dell'Organizzazione.

In caso di esito negativo dell'audit aggiuntivo, IIS CERT applica la revoca della certificazione (vedere anche § 13).

5.8 Delibera della certificazione e rilascio del certificato

Le pratiche di certificazione che hanno avuto una conclusione favorevole (chiusura delle non conformità, accettazione del piano per la chiusura delle osservazioni) sono presentate entro 5 giorni lavorativi ad un apposito organo di delibera, che, sulla base di tutte le evidenze raccolte dal RGV e di eventuali notizie di pubblico dominio che abbiano rilevanza per la certificazione, esprime la decisione sul rilascio della certificazione medesima, entro 5 giorni lavorativi dalla presentazione.

In caso di esito favorevole di tale decisione, è rilasciato, per il sistema di gestione in esame, un certificato di conformità con validità di tre anni: il certificato è messo a disposizione dell'Organizzazione in formato elettronico nella sua area riservata del sito web di IIS CERT, entro 5 giorni lavorativi dalla data della decisione del suo rilascio.

La validità del certificato è subordinata al risultato dei successivi audit di sorveglianza annuali ed al rinnovo triennale.

La periodicità e l'estensione dei successivi audit per il mantenimento della certificazione sono stabiliti da IIS CERT caso per caso mediante l'elaborazione di un programma triennale di audit.

Per il dettaglio sulla gestione e la validità dei certificati di conformità rilasciati da IIS CERT, si rimanda al successivo § 8.

6 MANTENIMENTO DELLA CERTIFICAZIONE

6.1 L'Organizzazione deve mantenere la conformità del proprio sistema di gestione alla norma di riferimento.

6.2 L'Organizzazione deve tenere registrazioni degli eventuali reclami e delle relative azioni correttive intraprese e deve renderle disponibili a IIS CERT unitamente alle azioni correttive intraprese a fronte delle osservazioni scaturite durante gli audit periodici.

6.3 IIS CERT effettua audit periodici sul sistema di gestione al fine di valutare il mantenimento della conformità ai requisiti della norma di riferimento.

Gli audit per il mantenimento della certificazione si dividono in due tipologie:

- audit di sorveglianza, con periodicità di regola almeno annuale e comunque condotti almeno una volta all'anno (per i sistemi di gestione della salute e sicurezza sul lavoro, vedere in particolare il § C.6.3), effettuando una valutazione parziale a campione sul sistema in accordo al programma di cui al § 5.8;
- audit di rinnovo (vedere § 5), con rivalutazione del sistema di gestione.

6.4 Gli audit di sorveglianza sono condotti presso il sito/i dell'Organizzazione, secondo un programma triennale che consenta di verificare almeno una volta, nell'arco di validità della certificazione, almeno una volta, ogni punto relativo alle prescrizioni contenute nella norma di riferimento secondo cui il sistema di gestione è stato certificato, tenendo conto dei documenti di cui al § 3.4 e tutti i processi realizzativi compresi nello scopo di certificazione.

Durante gli audit di sorveglianza saranno comunque presi in considerazione i seguenti elementi:

- a) audit interni e riesami da parte della direzione;
- b) riesame delle azioni intraprese a seguito dei rilievi identificati durante il precedente audit;
- c) trattamento dei reclami;
- d) efficacia del sistema di gestione riguardo il conseguimento degli obiettivi;
- e) avanzamento delle attività pianificate mirate al miglioramento continuo;
- f) controllo operativo continuo;
- g) riesame di ogni cambiamento.

La descrizione delle attività e delle disposizioni per la conduzione dell'audit di sorveglianza presso il sito/i è riportato, in dettaglio, nel piano di audit di sorveglianza che IIS CERT invia all'Organizzazione prima dell'effettuazione dell'audit stesso.

6.5 Deve essere effettuato almeno un audit di sorveglianza con periodicità non superiore a 12 mesi (per i sistemi di gestione della salute e sicurezza sul lavoro, vedere in particolare il § C.6.3).

La data entro la quale devono essere effettuati gli audit è riportata sul programma di audit triennale; tale programma può essere modificato da IIS CERT sulla base degli audit di sorveglianza precedenti.

Eventuali scostamenti degli audit di sorveglianza oltre tali limiti (e comunque non superiori a 3 mesi), dovuti a giustificati motivi, devono essere concordati preventivamente con IIS CERT e devono comunque essere recuperati al primo audit successivo.

In ogni caso, il primo audit di sorveglianza, successivo alla certificazione iniziale, dovrà essere effettuato entro dodici mesi dalla chiusura dell'audit di stage 2 (per i sistemi di gestione della salute e sicurezza sul lavoro, vedere in particolare il § C.6.5).

6.6 IIS CERT si riserva inoltre di effettuare audit con breve preavviso o senza preavviso (e aggiuntivi) rispetto a quelli previsti dal programma triennale presso l'Organizzazione:

- nel caso gli pervengano reclami o segnalazioni, ritenute particolarmente significative, relative alla non rispondenza del sistema di gestione ai requisiti della norma di riferimento e al presente Regolamento;
- in relazione a cambiamenti intervenuti nell'Organizzazione;
- ad Organizzazioni cui è stata sospesa la certificazione.

In tali casi, IIS CERT rende noto in anticipo delle condizioni ridotte in base alle quali sono condotti tali audit, in deroga parziale rispetto a quanto indicato ai punti precedenti.

In caso di rifiuto, senza valide motivazioni, da parte dell'Organizzazione, IIS CERT può avviare l'iter di sospensione/revoca della certificazione.

Nel caso in cui i reclami e le segnalazioni siano ritenute giustificate da IIS CERT, il costo dell'effettuazione dell'audit senza preavviso è a carico dell'Organizzazione.

6.7 Le date di esecuzione degli audit di sorveglianza sono concordate con l'Organizzazione con adeguato anticipo e ad essa ufficialmente confermate tramite una comunicazione scritta.

I nominativi degli Auditor qualificati incaricati all'effettuazione all'audit sono preventivamente comunicati da IIS CERT all'Organizzazione, la quale può fare obiezione sulla loro nomina, entro 5 giorni dalla nomina stessa, giustificandone i motivi.

6.8 Per le modalità di comunicazione dell'esito dell'audit si rimanda al precedente § 5.5.

La validità del certificato è considerata confermata a seguito dell'esito positivo dell'audit di sorveglianza (vedere anche Nota successiva).

Nota Gli organi deliberanti di IIS CERT effettuano comunque un monitoraggio di tutte le pratiche di sorveglianza.

6.9 In presenza di non conformità o di osservazioni la cui numerosità o tipologia, a giudizio del gruppo di audit, sia tale da pregiudicare il corretto funzionamento del sistema, la pratica viene comunque presentata dall'RGV all'organo di delibera (vedere § 5.8), che può richiedere all'Organizzazione di essere sottoposta ad un audit aggiuntivo – entro i tempi stabiliti da IIS CERT in relazione all'importanza delle non conformità/osservazioni stesse e comunque non oltre 6 mesi dal termine dell'audit di sorveglianza – finalizzato a verificare l'efficacia dei trattamenti e delle azioni correttive proposte.

Nel caso le non conformità non siano risolte entro i tempi stabiliti o qualora le osservazioni rilevate siano tali da non assicurare la rispondenza dei prodotti/servizi forniti alle richieste dei Clienti e delle normative di legge applicabili, IIS CERT può sospendere la certificazione sino a che le non conformità/osservazioni stesse non siano state corrette e comunque in accordo con quanto previsto dal § 13.1.

Tutte le spese relative ad eventuali audit supplementari conseguenti a carenze del sistema di gestione sono da considerarsi a carico dell'Organizzazione.

7 RINNOVO

7.1 In occasione dell'audit di ricertificazione del sistema di gestione, previsto ogni tre anni, l'Organizzazione deve contattare IIS CERT con sufficiente anticipo rispetto alla data prevista sul programma di audit triennale, al fine di poter pianificare l'attività e concordare la data di esecuzione dell'audit di ricertificazione.

In particolare, è responsabilità dell'Organizzazione aggiornare preventivamente in modo scritto le informazioni necessarie per l'emissione delle offerte di rinnovo; in mancanza dell'aggiornamento di tali informazioni, IIS CERT può emettere l'offerta per il rinnovo sulla base delle ultime informazioni rese disponibili (vedere anche successivo § 7.2).

La data di esecuzione dell'audit di ricertificazione, concordata con l'Organizzazione con adeguato anticipo, è ad essa ufficialmente confermata tramite una comunicazione scritta.

I nominativi degli Auditor incaricati dell'effettuazione dell'audit sono preventivamente comunicati da IIS CERT all'Organizzazione, la quale può fare obiezione sulla loro nomina, entro 5 giorni dalla nomina stessa, giustificandone i motivi.

7.2 L'audit di ricertificazione ha come scopo quello di confermare il mantenimento della conformità e dell'efficacia del sistema di gestione nel suo complesso e si basa principalmente su un audit in sito da effettuarsi, di regola, con gli stessi criteri dell'audit di stage 2.

In particolare, l'audit di ricertificazione comprende un audit in sito che prende in considerazione, tra l'altro, i seguenti aspetti:

- a) l'efficacia del sistema di gestione nella sua globalità alla luce di cambiamenti interni ed esterni e la sua continua pertinenza ed applicabilità per il campo di applicazione della certificazione;
- b) l'impegno dimostrato a mantenere l'efficacia e il miglioramento del sistema di gestione al fine di migliorare le prestazioni complessive;
- c) se l'operatività del sistema di gestione contribuisce al conseguimento della politica e degli obiettivi dell'Organizzazione.

La descrizione delle attività e delle disposizioni per la conduzione dell'audit di ricertificazione presso il sito/i è riportato, in dettaglio, nel piano di audit di ricertificazione che IIS CERT invia all'Organizzazione prima dell'effettuazione dell'audit stesso.

Qualora in sede di audit è rilevata una modifica del numero di addetti che influisce significativamente sulla durata della verifica a fronte delle tabelle del documento IAF MD 5 (vedere § 2), IIS CERT emette uno specifico rilievo (Non conformità o Osservazione) che dovrà essere preso in carico dall'Organizzazione.

7.3 A seguito dell'esito positivo dell'audit di ricertificazione, il gruppo di audit presenta all'organo di delibera la proposta di ricertificazione dell'Organizzazione ai fini della riemissione del certificato di conformità. Il certificato di conformità è riemesso da IIS CERT a seguito dell'esito positivo dell'esame della suddetta proposta; il certificato è nuovamente messo a disposizione dell'Organizzazione in formato elettronico nella sua area riservata del sito web di IIS CERT.

La conferma dell'approvazione da parte IIS CERT della ricertificazione con conseguente rilascio del certificato è inviata per iscritto all'Organizzazione.

Per il dettaglio su gestione e validità dei certificati di conformità rilasciati da IIS CERT si veda il successivo § 8.

7.4 L'iter di ricertificazione deve necessariamente concludersi, con esito positivo, prima della data di scadenza della certificazione riportata sul certificato, che non può essere prorogata da parte IIS CERT.

Di conseguenza l'audit di ricertificazione si deve concludere positivamente in tempo utile per permettere l'approvazione da parte IIS CERT della proposta di ricertificazione e la conseguente riemissione del certificato entro la suddetta data (almeno un mese prima della data di scadenza riportata sul certificato).

Qualora un'Organizzazione non ottemperi alle tempistiche suddette e quindi non ottenga la riemissione del certificato entro i termini di scadenza dello stesso, la relativa certificazione deve ritenersi scaduta a partire dal giorno successivo alla data di scadenza riportata sul certificato; IIS CERT informa l'Organizzazione delle relative conseguenze.

Qualora l'audit di rinnovo sia effettuato, per diversi motivi, dopo la scadenza del certificato, possono verificarsi i casi seguenti:

- 1) se le pratiche per il rinnovo sono iniziate prima della scadenza del certificato, l'audit segue le procedure previste per il rinnovo;
- 2) se le pratiche di rinnovo iniziano dopo la scadenza del certificato, l'audit di rinnovo segue le procedure previste per l'audit di stage 2, previa la conclusione positiva dello stesso entro 6 mesi dalla scadenza suddetta;
- 3) se sono trascorsi 6 mesi dalla scadenza del certificato, occorre seguire le pratiche per una prima valutazione (stage 1 + stage 2).

In ognuno dei casi sopra elencati viene emesso, ad esito positivo degli audit, un nuovo certificato a partire dalla relativa data di delibera, con scadenza coerente con il ciclo di certificazione precedente.

- 7.5** In presenza di non conformità oppure di osservazioni la cui numerosità e/o tipologia, a giudizio del gruppo di audit, sia tale da pregiudicare il corretto funzionamento del sistema di gestione, l'Organizzazione deve necessariamente applicare, in modo efficace, i relativi trattamenti prima della data di scadenza del certificato di conformità.

IIS CERT effettua quindi un audit aggiuntivo per la verifica della chiusura di tali rilievi in tempo utile per la successiva emissione del certificato.

I tempi stabiliti entro i quali l'Organizzazione deve sottoporsi all'audit aggiuntivo sono indicati nel rapporto di audit di rinnovo.

L'audit aggiuntivo può essere effettuato sul sito o su base documentale in relazione alla tipologia delle azioni correttive da verificare a giudizio del team di audit.

Tutte le spese relative ad eventuali audit aggiuntivi conseguenti a carenze del sistema di gestione sono da considerarsi a carico dell'Organizzazione.

- 7.6** Nel caso in cui l'Organizzazione non intenda rinnovare la certificazione, questa è da ritenersi scaduta a partire dal giorno successivo alla data di scadenza riportata sul certificato.

8 GESTIONE DEI CERTIFICATI DI CONFORMITÀ

- 8.1** Il certificato di conformità rilasciato da IIS CERT riporta, come minimo, i seguenti dati:
- a) la personalità giuridica dell'organizzazione oggetto della certificazione (Ragione sociale);
 - b) la norma di riferimento;
 - c) le tipologie di processi realizzati nell'ambito del sistema di gestione aziendale oggetto di certificazione;
 - d) i risultati delle attività svolte in termini di prodotti forniti e servizi erogati;
 - e) le unità operative (siti) nelle quali vengono svolte le attività oggetto di certificazione);
 - f) eventuali specificazioni e precisazioni necessarie od utili;
 - g) i riferimenti alla validità della certificazione (date di emissione del certificato, emissione corrente, scadenza);
 - h) il riferimento al Regolamento Tecnico ACCREDIA di schema/settore applicabile, ove applicabile.

Le voci c) e d) costituiscono, nel loro complesso, lo "scopo di certificazione".

La scadenza è calcolata, per ogni triennio di validità, a partire dalla data di delibera di prima certificazione.

- 8.2** La validità del certificato, nell'arco del triennio di validità, è subordinata al risultato dei successivi audit di sorveglianza.

Ad esito positivo dell'audit di rinnovo, come riportato al precedente § 7, è riemesso il certificato di conformità.

La validità del certificato può essere sospesa, revocata o rinunciata in accordo a quanto previsto al § 13.

IIS CERT pubblica e mantiene aggiornati direttamente sul proprio sito web:

- a) l'elenco delle Organizzazioni certificate;
- b) lo stato di validità dei certificati emessi.

Su richiesta, IIS CERT fornisce informazioni sulle cause che hanno reso non valido il certificato.

9 MODIFICA DELLA CERTIFICAZIONE E COMUNICAZIONE DEI CAMBIAMENTI

9.1 L'Organizzazione in possesso della certificazione può richiedere una modifica o estensione della stessa presentando una nuova richiesta di certificazione, corredata dalla documentazione di cui al § 5.2 debitamente aggiornata.

IIS CERT si riserva di esaminare caso per caso le richieste e di decidere le modalità di valutazione ai fini del rilascio di una nuova certificazione, in conformità a quanto previsto dalle condizioni generali di contratto stabilite nel "Regolamento generale per le valutazioni di sistema, personale, prodotto – Condizioni generali di contratto" (vedere § 2) ed alla norma di riferimento per il sistema di gestione.

9.2 Durante il periodo di validità della certificazione, l'Organizzazione deve tempestivamente comunicare ad IIS CERT ogni cambiamento significativo concernente:

- l'organizzazione aziendale;
- il cambio di ragione sociale e/o il cambio di indirizzo della sede e/o delle unità produttive;
- i siti produttivi;
- i processi;
- i prodotti;
- l'organico aziendale.

In relazione al tipo di modifiche introdotte, IIS CERT si riserva di:

- a) effettuare un audit di sorveglianza non programmata per valutare l'influenza delle variazioni sul sistema di gestione;
- b) rivedere le condizioni contrattuali per le successive visite.

Di seguito sono riportati alcuni casi.

9.3 Nei casi in cui cambia il soggetto giuridico titolare del certificato o all'interno del quale si colloca l'Organizzazione certificata, IIS CERT assume tutte le informazioni necessarie per capire l'entità e la natura dei cambiamenti nelle politiche, nelle attività e nell'organizzazione dell'Organizzazione; nei casi in cui vi è o vi possa essere un cambiamento di politiche e/o attività e/o organizzazione, IIS CERT valuta l'ipotesi di attivare un nuovo iter di certificazione con visita iniziale adeguatamente dimensionata e pianificata per assicurare l'esecuzione di tutte le necessarie verifiche: lo scopo e tutte le altre informazioni contenute nel certificato saranno adeguate alla nuova situazione.

Il certificato viene riemesso cambiando:

- il numero del certificato;
- l'intestazione dell'Organizzazione;
- la data di prima emissione;
- la data di emissione corrente.

9.4 Nei casi in cui le modifiche del soggetto giuridico non abbiano rilevanza significativa nell'organizzazione (es. non cambia l'oggetto dello statuto, non cambia l'assetto della proprietà e/o il Consiglio di Amministrazione o l'Amministratore Delegato, etc.), IIS CERT verifica le condizioni e può prendere in esame l'ipotesi di mantenere il numero, la data di emissione ed eventualmente lo scopo del certificato.

9.5 Nei casi in cui l'Organizzazione richieda modifiche o estensioni della certificazione (es.: aggiunta di prodotti, processi, materiali, siti diversi da quelli certificati), le modifiche sono da considerarsi come una estensione del campo di applicazione della certificazione (per i sistemi di gestione della salute e sicurezza sul lavoro, vedere in particolare il § C.9.6), con avviamento del relativo iter di delibera.

9.6 IIS CERT si riserva di esaminare caso per caso le richieste e di decidere le modalità di valutazione, incluso variazioni contrattuali, esecuzione di audit non programmati (aggiuntivi), ai fini del rilascio di una nuova certificazione o dell'estensione della certificazione in corso di validità.

Le decisioni prese in tal proposito sono registrate.

Il rifiuto da parte dell'Organizzazione equivale alla rescissione dal contratto.

10 ORGANIZZAZIONI MULTISITO

10.1 Qualora un'Organizzazione operi su più siti permanenti e sia richiesta un'unica certificazione, le attività di audit possono essere espletate per campionamento dei siti sottoposti ad audit, purché:

- i processi di tutti i siti siano sostanzialmente dello stesso genere e siano svolti con metodi e procedure simili; in presenza di processi differenti in luoghi differenti questi devono essere collegati (es. fabbricazione di componenti elettronici in un luogo, assemblaggio degli stessi componenti svolto dalla stessa Organizzazione in diversi altri luoghi);
- il sistema di gestione sia gestito e amministrato a livello centrale e sia sottoposto al riesame da parte della direzione centrale.

L'Organizzazione deve inoltre dimostrare che l'ufficio centrale ha istituito un sistema di gestione conforme alla norma di riferimento e che l'intera Organizzazione ne soddisfa i requisiti.

In particolare, almeno le seguenti attività devono essere gestite dalla funzione centrale dell'Organizzazione:

- valutazione delle necessità di addestramento;
- controllo della documentazione e delle sue modifiche;
- riesame del sistema di gestione da parte della direzione;
- gestione dei reclami;
- valutazione dell'efficacia delle azioni correttive e preventive;
- pianificazione ed esecuzione degli audit interni e valutazione dei loro risultati;
- presenza di differenti requisiti di legge.

Prima dell'audit iniziale da parte IIS CERT, l'Organizzazione deve aver effettuato un audit interno ad ogni sito e verificato la conformità del suo sistema di gestione alla norma di riferimento.

10.2 Qualora l'Organizzazione rispetti i requisiti precedenti, IIS CERT verifica comunque la fattibilità di un campionamento su tutti i siti ed eventualmente valuta se limitare tale campionamento in presenza di:

- requisiti connessi a fattori variabili locali;
- settori o attività che rientrano nello scopo;
- dimensioni dei siti idonei ad un audit multi-sito (per i sistemi di gestione della salute e sicurezza sul lavoro, vedere in particolare i §§ C.9.6 e C.10.1);
- variazioni nell'attuazione locale del sistema di gestione, come la necessità di ricorrere frequentemente all'utilizzo, nell'ambito del sistema di gestione, di piani aventi per oggetto attività differenti oppure sistemi contrattuali o normativi differenti;
- utilizzo di siti temporanei (cantieri operativi).

In caso di Organizzazioni che erogano servizi, se i siti in cui si svolgono le attività sottoposte a certificazione non sono tutti pronti contemporaneamente per essere presentati per la certificazione, l'Organizzazione deve comunicare preventivamente a IIS CERT i siti che essa desidera siano inclusi nella certificazione e quelli che ne devono essere esclusi.

10.3 Sulla base delle informazioni fornite dall'Organizzazione, IIS CERT stabilisce il piano di campionamento applicabile, sulla base delle regole del documento IAF MD 1 (vedere § 2).

Questa attività, in generale, è effettuata nel corso del processo di audit e può essere effettuata anche dopo aver ultimato l'audit presso la sede centrale, che deve sempre essere sottoposta ad audit; in ogni caso, IIS CERT informa l'ufficio centrale sui siti che dovranno far parte del campione.

10.4 IIS CERT rilascia un singolo certificato con il nome e l'indirizzo della sede centrale dell'Organizzazione.

Su un allegato, o sul certificato stesso, è riportato l'elenco di tutti i siti a cui si riferisce il certificato.

All'Organizzazione può essere rilasciato uno stralcio del certificato per ciascun sito coperto dalla certificazione, a condizione che esso contenga lo stesso scopo o un suo sotto-elemento ed includa un riferimento chiaro al certificato principale.

10.5 Per eventuali non conformità e/o osservazioni rilevate in un singolo sito durante gli audit, l'Organizzazione deve valutare se le stesse sono relative a carenze imputabili a più siti e se del caso, deve adottare azioni correttive sia presso la sede centrale che presso gli altri siti.

Se, invece, le non conformità e/o osservazioni non risultano essere del suddetto tipo, l'Organizzazione deve fornire adeguate evidenze e motivazioni per limitare la sua azione correttiva di follow-up.

Se sono rilevate non conformità anche su un solo sito, l'iter di certificazione è sospeso all'intera rete di siti elencati, sino a che le non conformità stesse non siano state corrette e comunque in accordo con quanto previsto dal § 10.1.

Non è ammissibile che, per aggirare l'ostacolo creato dall'esistenza di una non conformità in un singolo sito, l'Organizzazione escluda dallo scopo tale/i sito/i durante il corso del processo di certificazione.

10.6 L'Organizzazione deve tenere informato IIS CERT sulla chiusura di qualsiasi sito coperto dalla certificazione; se tali informazioni non verranno comunicate, IIS CERT potrà valutare se procedere in accordo con quanto previsto dal § 10.1.

In una certificazione già esistente possono essere inseriti siti aggiuntivi a seguito di audit di sorveglianza o di ricertificazione o a seguito di specifici audit di estensione.

11 SPECIFICITÀ PER I SETTORI IAF 28, IAF 34, IAF 35

11.1 Nel caso di Organizzazioni operanti nei Settori IAF 28, IAF 34 o IAF 35, vale quanto segue:

- a) in sede di certificazione iniziale, tutte le tipologie di attività devono essere sottoposte ad audit in cantiere/ sito esterno, con le seguenti precisazioni:
 - se in uno stesso cantiere/sito esterno sono effettuate lavorazioni/attività riconducibili a più processi realizzativi, l'audit presso tale cantiere/sito può essere ritenuto valido per coprire l'insieme degli stessi;
 - almeno un cantiere/sito esterno deve trovarsi in stadi di avanzamento dei lavori/attività significativo;
- b) la sorveglianza annuale prevede almeno un audit in cantiere/sito esterno, in modo tale che, nell'arco di validità della certificazione, tutti i processi realizzativi e rientranti nello scopo di certificazione siano sottoposti a verifica (vedere anche Note 1 e 2 successive).

Nota 1 *Nello scopo di certificazione saranno comunque riportati solo i processi realizzativi che siano stati oggetto di verifica per almeno due volte nel passato triennio di certificazione, fatte salve eventuali estensioni intervenute nel triennio e/o nella stessa verifica di rinnovo.*

Nota 2 *Eventuali variazioni rispetto a quanto programmato o definito dovranno essere registrate e, nei casi più critici (per esempio, la mancanza di cantieri/siti esterni aperti), sottoposte all'Organo Deliberante.*

12 TRASFERIMENTO DI CERTIFICATI ACCREDITATI

12.1 Qualora un'Organizzazione con certificazione in corso di validità rilasciata da un altro Organismo di Certificazione di sistemi di gestione (nel seguito "OdC cedente"), accreditato da un Organismo di Accreditamento (OdA) che aderisce all'accordo di mutuo riconoscimento IAF MLA, voglia trasferire la propria certificazione ad IIS CERT, deve inviare ad IIS CERT medesima la domanda di certificazione di cui al § 5.1, precisando le motivazioni della richiesta di trasferimento.

L'Organizzazione, in caso di accettazione dell'offerta economica, deve inviare ad IIS CERT la domanda di certificazione allegando i seguenti documenti:

- a) copia del certificato emesso dall'OdC cedente, in corso di validità;
- b) copia del rapporto di audit di certificazione, oppure dell'ultimo rapporto di audit di rinnovo, e dei rapporti degli audit di sorveglianza seguenti;
- c) copia dell'ultimo riesame della direzione.

L'Organizzazione deve inoltre comunicare ad IIS CERT:

- eventuali osservazioni o segnalazioni pervenute dalle autorità nazionali o locali preposte;
- eventuali reclami ricevuti e relative azioni intraprese.

La documentazione suddetta è esaminata per verificare se lo scopo della certificazione è compreso tra gli scopi per i quali IIS CERT è accreditato, la validità della certificazione rilasciata dall'*OdC cedente* e lo stato di chiusura di eventuali rilievi.

Nel caso in cui la certificazione rilasciata dall'*OdC cedente* sia sospesa oppure non sia possibile verificare lo stato di validità del certificato, questa certificazione non potrà essere ammessa alla procedura di trasferimento.

Le verifiche di cui sopra possono includere un audit in campo all'Organizzazione che ha richiesto il trasferimento della certificazione, della durata di un giorno.

In particolare, l'audit in campo è necessario qualora non sia stato possibile:

- stabilire un qualsiasi contatto con l'*OdC cedente*;
- ricevere una conferma della validità del certificato da parte dell'*OdC cedente*;
- entrare in possesso di tutta la documentazione di audit sopra descritta (comprese le check list compilate) relativa al ciclo di certificazione in corso.

In ogni caso, IIS CERT emette un rapporto su tutte le verifiche condotte prima dell'audit in campo, anche tenendo conto di quanto previsto dal documento di *pre-transfer review* indicato nella guida IAF MD 2 (vedere § 2).

A completamento con esito favorevole dell'attività sopra riportata, è prevista una apposita delibera di *pre-transfer*, seguita o meno dalla stampa e messa a disposizione del cliente del certificato (comunque valido a tutti gli effetti), a seconda delle tempistiche previste per l'audit in campo; tale certificato mantiene, di regola, la scadenza già stabilita dall'*OdC* che ha emesso la precedente certificazione.

In generale, anche per l'effettuazione degli audit di sorveglianza e di rinnovo del sistema è mantenuta la programmazione già stabilita dall'*OdC* che ha emesso la precedente certificazione.

13 **SOSPENSIONE, RIPRISTINO E REVOCA DELLA CERTIFICAZIONE**

13.1 La validità del certificato di conformità può essere sospesa in accordo a quanto previsto dalle condizioni generali di stabilite nel "Regolamento generale per le valutazioni di sistema, personale, prodotto – Condizioni generale di contratto" (vedere § 2) e nei seguenti casi specifici:

- se l'Organizzazione non consente che siano condotti gli audit programmati alle frequenze richieste;
- se sono riscontrate non conformità non risolte entro i tempi stabiliti da IIS CERT;
- se l'Organizzazione non ha rispettato i termini fissati per la comunicazione delle azioni correttive, a seguito di non conformità/osservazioni segnalate sul rapporto di audit;
- se l'Organizzazione ha effettuato importanti ristrutturazioni interne al/i sito/i, ovvero si trasferisce in altro/i sito/i senza segnalare tali varianti ad IIS CERT;
- se l'Organizzazione ha apportato al suo sistema di gestione modifiche rilevanti che non siano state accettate da IIS CERT;
- in presenza di importanti ristrutturazioni dell'Organizzazione non comunicate ad IIS CERT;
- per rifiuto od ostacolo alla partecipazione agli audit di osservatori di un Ente di Accreditamento;
- per l'evidenza che il sistema di gestione non assicura il rispetto delle leggi e regolamenti cogenti applicabili ai prodotti/servizi forniti, alle attività e/o al/i sito/i;
- in presenza di riscontri di eventuali giustificati e gravi reclami pervenuti ad IIS CERT.

L'Organizzazione può inoltre richiedere ad IIS CERT, giustificandone i motivi, la sospensione della certificazione per un periodo in generale non superiore a 6 mesi e comunque non oltre la data di scadenza del certificato.

La sospensione è notificata per iscritto, precisando le condizioni per il ripristino della certificazione ed il termine entro il quale devono essere attuate; nel periodo di sospensione, la certificazione del sistema di gestione dell'Organizzazione è temporaneamente non valida.

La sospensione della validità del certificato è resa pubblica da IIS CERT direttamente sul proprio sito web come previsto al § 8.2.

13.2 Il ripristino della certificazione è subordinato all'accertamento della eliminazione delle carenze che avevano causato la sospensione stessa mediante un audit approfondito che verifichi la rispondenza del sistema di gestione a tutti i requisiti della norma di riferimento.

Esso è notificato per iscritto all'Organizzazione e reso pubblicamente noto da IIS CERT attraverso il proprio sito web come previsto dal § 8.2.

13.3 Il mancato soddisfacimento entro il termine prescritto delle condizioni di cui al § 13.2 causa la revoca del certificato di conformità.

La revoca del certificato di conformità può essere decisa in accordo a quanto previsto dalle condizioni generali di contratto stabilite nel "Regolamento generale per le valutazioni di sistema, personale, prodotto – Condizioni generali di contratto" (vedere § 2) e nei seguenti casi specifici:

- quando si verifichino circostanze, quali quelle citate al § 10.1 per la sospensione, che siano giudicate particolarmente gravi;
- se l'Organizzazione sospende le sue attività o servizi oggetto del sistema di gestione certificato per un periodo in generale superiore a 6 mesi;
- qualora l'Organizzazione non accetti le nuove condizioni economiche stabilite da IIS CERT per l'eventuale modifica del contratto;
- nel caso di Organizzazione multi-sito, qualora la sede centrale o uno dei siti non rispetti i criteri necessari per il mantenimento del certificato;
- per ogni altro serio motivo, a giudizio di IIS CERT, come ad esempio, a titolo non esaustivo, la provata incapacità del sistema di perseguire i propri obiettivi di rispetto dei vincoli legislativi o contrattuali o di sicurezza di prodotto.

L'avvenuta revoca del certificato di conformità è notificata per iscritto all'Organizzazione ed è resa pubblicamente nota da IIS CERT secondo quanto previsto dal § 6.3.

A seguito della revoca, l'Organizzazione non può più far uso in alcun modo del certificato di conformità.

Il certificato di conformità dell'Organizzazione è inoltre ritirato dalla sua area riservata del sito web di IIS CERT, dopo preventiva e formale informazione.

La revoca è inoltre comunicata da IIS CERT alla SOA, nei termini previsti da tale amministrazione.

L'Organizzazione che, dopo la revoca, intenda nuovamente accedere alla certificazione, deve presentare una nuova domanda seguendo l'intero iter.

14 RINUNCIA ALLA CERTIFICAZIONE

14.1 L'Organizzazione certificata può inviare una formale comunicazione di rinuncia alla certificazione ad IIS CERT, prima della scadenza del certificato, incluso il caso in cui l'Organizzazione stessa non voglia o non possa adeguarsi alle nuove istruzioni impartite da IIS CERT.

IIS CERT, al momento della ricezione di tale comunicazione, avvia l'iter per rendere lo stato del certificato non valido; in generale, entro un mese dalla data della avvenuta comunicazione, IIS CERT aggiorna lo stato di validità del certificato.

Alla scadenza, il certificato di conformità dell'Organizzazione sarà inoltre ritirato dalla sua area riservata del sito web di IIS CERT.

15 UNIFICAZIONE DELLE DATE DI VISITA PER DIVERSE CERTIFICAZIONI

15.1 Qualora un'Organizzazione certificata in tempi diversi, secondo norme differenti, avanzi una richiesta formale di unificare le date dei successivi audit, IIS CERT può acconsentire previo esame della richiesta e registrazione delle considerazioni/motivazioni che hanno portato alle decisioni, rimettendo i certificati, senza comunque eseguire audit con frequenza superiore ai 12 mesi.

Se gli audit di sorveglianza dovessero essere combinati con audit di altri schemi di sistemi di gestione, sia la pianificazione dell'audit che il rapporto indicheranno con chiarezza gli aspetti relativi ad ogni sistema (vedere anche Nota successiva).

Nota *Nel caso di audit combinati, IIS CERT nomina un RGV avente conoscenza approfondita di almeno una delle norme sui sistemi di gestione interessati e consapevolezza delle altre.*

16 DOCUMENTI DI REGISTRAZIONE

16.1 Le registrazioni delle attività svolte sono conservate in forma elettronica.

In generale sono conservati i seguenti documenti di registrazione (ciascuno ove applicabile):

- richiesta d'offerta,
- offerta/ordine,
- domanda di certificazione,
- accettazione della domanda,
- iscrizione alla CCIAA,
- procedure,
- nomina di RGV e/o Auditor (se previsti),
- giustificazione per la determinazione del tempo di audit;
- giustificazione della metodologia applicata per il campionamento;
- commenti al manuale della qualità e/o alle procedure,
- rapporto di audit preliminare (eventuale),
- chiusura dell'esame documentale,
- notifica degli audit,
- piano e programma di audit,
- questionari usati in audit,
- rapporti di non conformità e/o osservazioni (eventuali),
- rapporto di audit,
- evidenze di trattamenti ed azioni correttive (eventuali),
- decisioni relative alla delibera;
- copie dei certificati emessi da IIS CERT,
- reclami e ricorsi eventuali, con relative azioni a seguire;
- comunicazioni da e per l'Organizzazione.

Le registrazioni relative alle Organizzazioni con certificazione non più valida sono conservati per 6 anni dalla data dell'ultimo audit eseguito.

17 CONDIZIONI CONTRATTUALI

17.1 Per le condizioni contrattuali trovano applicazione le disposizioni contenute nel "Regolamento generale per le valutazioni di sistema, personale, prodotto – Condizioni generali di contratto" (vedere § 2), nella revisione in vigore.

ALL. A Particolarità per la certificazione di sistemi di gestione per la qualità

A.1 Scopo e campo di applicazione

A.1.1 Nel presente Allegato sono definite le regole supplementari, non sostitutive, applicate da IIS CERT per la certificazione di sistemi di gestione per la qualità rispetto a quanto già definito in precedenza nella Parte generale.

Sono sviluppati solo i punti della Parte generale per i quali sono applicabili regole supplementari e la relativa numerazione risulta corrispondente.

A.1.3 IIS CERT rilascia la certificazione in accordo ai requisiti della norma UNI CEI EN ISO/IEC 17021-1 (vedere § 2) ad Organizzazioni il cui sistema di gestione per la qualità sia stato riconosciuto conforme a tutti i requisiti previsti dalla norma ISO 9001.

Inoltre, su richiesta, IIS CERT può effettuare valutazioni di conformità di un sistema di gestione per la Qualità in accordo ad altri documenti normativi di riferimento e, se del caso, rilasciare la relativa certificazione.

In particolare, il presente Regolamento si applica anche per la certificazione di conformità alla serie di norme UNI EN ISO 3834, quando l'attività è gestita nell'ambito dell'accreditamento ISO/IEC 17021-1: per le particolarità di tale attività, si rimanda all'Allegato A del Regolamento CER_QAS 024 R (vedere § 2).

A.3 Definizioni

SGQ: sistema di gestione per la Qualità.

A.4 Requisiti

A.4.1 Per ottenere la certificazione da parte di IIS CERT, un SGQ deve soddisfare inizialmente e nel tempo i requisiti della norma ISO 9001 e quelli aggiuntivi previsti dagli Organismi di Accreditamento (esempio: Regolamento Tecnico ACCREDIA RT-05).

A.4.2 Il SGQ si intende completamente operativo quando, oltre a quanto stabilito nella Parte generale:

- sono state messe in atto azioni che diano garanzia di costanza nelle modalità di produzione e nella qualità dei prodotti/servizi forniti.

A.4.3 Oltre a quanto stabilito dal Regolamento, l'Organizzazione deve comunicare a IIS CERT:

- eventuali elementi della norma di riferimento che ritiene non siano applicabili alla sua Organizzazione o che necessitino di interpretazione o di adattamento, indicandone chiaramente i motivi.

A.4.4 Nel caso di richiesta di certificazione di conformità alla ISO 9001:2008, unitamente alla richiesta di certificazione, o successivamente alla stessa, l'Organizzazione, oltre a quanto stabilito dal Regolamento, dovrà rendere disponibile a IIS CERT anche un Manuale del SGQ che includa:

- la descrizione dei processi e delle loro interazioni;
- i motivi dell'esclusione di eventuali elementi della norma di riferimento che ritiene non applicabili ovvero che necessitino interpretazioni o adattamento;
- l'elenco delle principali leggi e/o regolamenti applicabili al prodotto/servizio fornito o necessarie per la corretta applicazione del sistema di gestione per la qualità.

A.9 Modifica della certificazione: transizione dalla ISO 9001:2008 alla ISO 9001:2015

L'Organizzazione in possesso della certificazione di conformità alla ISO 9001:2008 può chiedere la transizione alla ISO 9001:2015 in occasione di un audit di sorveglianza pianificato o di un audit di rinnovo o di un audit aggiuntivo (quindi con un singolo audit): nei primi due casi IIS CERT applica un tempo aggiuntivo rispetto al contratto in essere per avere certezza che tutte le attività siano coperte sia a fronte della norma esistente che della nuova.

ALL. B Particolarità per la certificazione di sistemi di gestione ambientale

B.1 Scopo e campo di applicazione

B.1.1 Nel presente Allegato sono definite le regole supplementari e/o sostitutive applicate da IIS CERT per la certificazione di sistemi di gestione ambientale rispetto a quanto già definito in precedenza nella Parte generale.

Sono sviluppati solo i punti della Parte generale per i quali sono applicabili regole supplementari e la relativa numerazione risulta corrispondente.

B.1.3 IIS CERT rilascia la certificazione in accordo ai requisiti della norma UNI CEI EN ISO/IEC 17021-1 (vedere § 2) ad Organizzazioni il cui sistema di gestione ambientale sia stato riconosciuto conforme a tutti i requisiti previsti dalla norma ISO 14001.

B.3 Definizioni

SGA: sistema di gestione Ambientale.

B.4 Requisiti

B.4.1 Per ottenere la certificazione da parte di IIS CERT, un SGA deve soddisfare inizialmente e nel tempo i requisiti della norma ISO 14001 e quelli aggiuntivi previsti dagli Organismi di Accreditamento (per esempio, dal Documento ACCREDIA RT-09).

B.4.2 In sostituzione a quanto stabilito dal corrispondente § 4.2 della Parte generale, per ottenere la certificazione del proprio SGA, l'Organizzazione deve:

- a) avere effettuato un'analisi ambientale preliminare del sito/i che comprenda:
 - una descrizione del tipo di attività svolte nel Sito/i per il quale viene richiesta la certificazione del SGA;
 - una identificazione degli aspetti ambientali associati alle proprie attività e relativi impatti;
- b) disporre di un Manuale che:
 - definisca campo di applicazione del SGA, descriva i principali elementi del sistema e le loro interazioni e contenga, o richiami, le relative procedure documentate;
 - prenda in considerazione i requisiti della Norma e fornisca una descrizione, anche breve, delle risorse e dei procedimenti posti in atto per assicurare la conformità a tali requisiti;
 - contenga una adeguata descrizione dell'Organizzazione aziendale.
- c) aver istituito, mantenuto attivo e completamente operativo un SGA in totale ottemperanza ai requisiti della Norma ISO 14001.

Il SGA si intende completamente operativo quando:

- è applicato da almeno tre mesi;
- il sistema di audit interno è completamente attuato ed è possibile dimostrarne l'efficacia;
- è stato svolto e documentato almeno un riesame del sistema da parte della Direzione;
- sono stati valutati e identificati gli aspetti ambientali significativi;
- sono stati stabiliti e documentati gli obiettivi ed i relativi programmi ambientali;
- sono stati effettuati e registrati monitoraggi degli impatti ambientali e controlli delle attività ad essi associate;
- sono state messe in atto azioni per il miglioramento continuo e prevenzione dell'inquinamento.

B.5 Certificazione iniziale

B.5.1 Oltre a quanto stabilito dal corrispondente § 5.1 della Parte generale, l'Organizzazione deve comunicare a IIS CERT eventuali attività/siti esclusi dal campo di applicazione del SGA ai fini della verifica dell'ammissibilità di tali esclusioni.

B.5.2 In sostituzione a quanto stabilito dal corrispondente § 5.2 della Parte generale, unitamente alla richiesta di certificazione, o successivamente alla stessa, l'Organizzazione dovrà rendere disponibile al IIS CERT la seguente documentazione:

- a) relazione conclusiva dell'analisi preliminare del sito/i comprensiva di:
 - lay-out del sito/i;
 - manuale del sistema di gestione ambientale che descriva Politica Ambientale, Obiettivi e Programma/i Ambientali ed SGA dell'Organizzazione (nell'ultima revisione valida);
 - organigramma dell'Organizzazione;
- b) elenco delle procedure interne rilevanti ai fini della gestione ambientale;
- c) elenco delle autorizzazioni di natura ambientale in possesso dell'Organizzazione ed elenco degli adempimenti ambientali applicabili all'Organizzazione compilando il modulo "Elenco autorizzazioni ed adempimenti ambientali" (allegato all'offerta) o fornendo documentazione equivalente;
- d) copia della visura camerale o documento equivalente, quale evidenza dell'esistenza dell'Organizzazione e dell'attività effettuata;
- e) elenco dei cantieri in corso, con descrizione delle attività ivi espletate, ove applicabile.

IIS CERT può richiedere a sua discrezione, per esame, anche altri documenti, oltre quelli indicati in precedenza, giudicati importanti ai fini della valutazione del SGA.

La documentazione di cui sopra è valutata dal IIS CERT per conformità alla norma di riferimento ed ai requisiti del presente Regolamento.

L'esito di questo esame è comunicato al richiedente con l'invio di una copia del rapporto di esame documentale (se questo è effettuato presso gli uffici del IIS CERT); eventuali rilievi riscontrati nella documentazione considerati critici devono essere risolti dall'Organizzazione, a soddisfazione di IIS CERT, prima del prosieguo dell'iter certificativo.

La documentazione di cui sopra è, in generale, trattenuta per uso di archivio da IIS CERT.

Se l'audit di stage 1 è effettuato completamente on-site, l'esito dell'esame della documentazione è comunque riportato sul rapporto di esame documentale e sarà consegnato all'Organizzazione unitamente al rapporto di stage1 di cui al § 5.3 della Parte generale.

B.5.3 Oltre a quanto stabilito dal corrispondente § 5.3 della Parte generale, durante l'audit Stage 1, sarà verificato quanto segue:

- a) che l'Organizzazione abbia documentato la valutazione degli aspetti ambientali significativi e l'affidabilità di tale valutazione in relazione alla tipologia dell'Organizzazione;
- b) che l'Organizzazione disponga di tutte le necessarie autorizzazioni di natura ambientale, relative alla sua attività, in corso di validità;
- c) che l'Organizzazione risulti conforme agli adempimenti contenuti nei documenti di cui alla lettera b) oltre che agli adempimenti richiesti dalla legislazione ambientale ad essa applicabile.

Nel caso in cui quanto specificato alle suddette lett. a) e b) non sia formalmente soddisfatto si rimanda a quanto esplicitato al § 5.6.

B.5.4 Oltre a quanto stabilito dal corrispondente § 5.4 della Parte generale,

- l'audit è effettuato anche sulla base del documento di Analisi Ambientale Preliminare nella revisione aggiornata;
- nel corso del sopralluogo presso il/i sito/i saranno, tra l'altro, effettuati accertamenti sugli impianti e colloqui con il personale dell'Organizzazione coinvolto nel SGA.

B.5.6 Oltre a quanto stabilito dal corrispondente § 5.6 della Parte generale, si intende non conformità anche una situazione tale da ridurre la capacità del SGA ad assicurare il controllo degli aspetti/impatti ambientali e/o il rispetto della legislazione.

Inoltre, in mancanza di autorizzazioni o documenti equivalenti in campo ambientale, richiesti dalla legislazione vigente, il processo di certificazione è sospeso a meno che l'Organizzazione non sia in grado di dimostrare quantomeno:

- a) di aver presentato la domanda di autorizzazione completa e corretta con un anticipo non inferiore al tempo che la legge concede all'Autorità Competente per rilasciare l'autorizzazione e di aver attuato correttamente tutti i passi previsti per l'iter autorizzativo;
- b) di riprodurre evidenze oggettive inerenti a formali solleciti inoltrati nei confronti delle autorità interlocutrici, successivamente alle scadenze di legge a cui tali autorità sarebbero state tenute a conformare;
- c) di rispettare comunque, se presenti, i limiti previsti dalla legge.

Il termine di cui al punto a) si può considerare interrotto fino alla trasmissione della risposta laddove l'Autorità richieda integrazioni alla documentazione trasmessa; qualora la legge non indichi un termine specifico questo dovrebbe essere reperito in regolamenti di carattere generale, sui procedimenti amministrativi o nei regolamenti interni di cui l'Autorità competente si è dotata per gestire gli specifici iter.

Se nessun termine può comunque essere reperito un termine di sei mesi può essere considerato ragionevole e prudentiale (a meno dei casi in cui la legislazione preveda il cosiddetto "silenzio-diniego").

In presenza di rilievi accertati nel corso dell'audit, legati al mancato rispetto di requisiti legislativi cogenti in campo ambientale (cioè limiti e/o disposizioni di legge e limiti e/o prescrizioni riportate su autorizzazioni o su altri documenti prescrittivi, etc.), il processo di certificazione è sospeso, salvo casi particolari, finì a quando l'Organizzazione non dimostri il rispetto di tali requisiti.

B.6 Mantenimento della certificazione

B.6.2 Oltre a quanto stabilito dal corrispondente § 6.2 della Parte generale, l'Organizzazione deve mantenere registrazioni relative a:

- aspetti/impatti ambientali;
- incidenti/emergenze ambientali occorsi nel sito/i e di altri eventi che potenzialmente avrebbero potuto avere effetti negativi sull'ambiente;
- eventuali reclami relativamente agli impatti ambientali da essa prodotti;
- eventuali osservazioni o segnalazioni pervenute dalle autorità nazionali o locali proposte al controllo ambientale

e deve renderle disponibile a IIS CERT unitamente alle relative azioni correttive intraprese durante gli audit periodici.

L'Organizzazione deve tenere prontamente informato IIS CERT circa la presenza di eventuali osservazioni/ segnalazioni pervenute dalle autorità nazionali o locali preposte al controllo ambientale o situazioni di non conformità legislativa per tutte le attività svolte dall'Organizzazione indipendentemente dal campo di applicazione del SGA.

B.9 Modifica della certificazione: transizione dalla ISO 14001:2004 alla ISO 14001:2015

L'Organizzazione in possesso della certificazione di conformità alla ISO 14001:2004 può chiedere la transizione alla ISO 14001:2015 in occasione di un audit di sorveglianza pianificato o di un audit di rinnovo o di un audit aggiuntivo (quindi con un singolo audit): nei primi due casi IIS CERT applica un tempo aggiuntivo rispetto al contratto in essere per avere certezza che tutte le attività siano coperte sia a fronte della norma esistente che della nuova.

B.10 Organizzazioni multisito

B.10.1 Oltre a quanto stabilito dal corrispondente § 10.1 della Parte generale, anche le seguenti attività devono essere gestite dalla funzione centrale dell'Organizzazione:

- analisi ambientale dei siti;
- modifiche degli aspetti e degli impatti associati per i sistemi di gestione ambientale.

ALL. C Particolarità per la certificazione di sistemi di gestione per la salute e la sicurezza sul lavoro

C.1 Scopo e campo di applicazione

C.1.1 Nel presente Allegato sono definite le regole supplementari e/o sostitutive applicate da IIS CERT per la certificazione di sistemi di gestione per la salute e la sicurezza sul lavoro rispetto a quanto già definito in precedenza nella Parte generale.

Sono sviluppati solo i punti della Parte generale per i quali sono applicabili regole supplementari e/o modifiche e la relativa numerazione risulta corrispondente.

C.1.3 IIS CERT rilascia la certificazione in accordo ai requisiti della norma UNI CEI EN ISO/IEC 17021-1 (vedere § 2 e Nota successiva) ad Organizzazioni il cui sistema di gestione per la salute e la sicurezza sul lavoro sia stato riconosciuto conforme a tutti i requisiti previsti dalla norma OHSAS 18001.

Nota Con riferimento ai requisiti aggiuntivi, ai fini dell'accreditamento, introdotti dal documento EA-3/13 (vedere § C.2), nel § C.19 sono elencati tutti gli elementi addizionali oppure rafforzativi/chiarificativi rispetto a quanto di seguito indicato; tali elementi saranno applicati da IIS CERT nei confronti delle Organizzazioni certificate/certificande dal momento della richiesta di transizione del proprio accreditamento, come da apposita comunicazione alle Organizzazioni stesse.

C.1.5 La certificazione rilasciata dal IIS CERT è riferita esclusivamente alla singola Organizzazione, dove per Organizzazione si intende un gruppo, società, azienda, impresa, ente o istituzione, ovvero loro parti o combinazioni, in forma associata o meno, pubblica o privata, che abbia una propria struttura funzionale ed amministrativa e che dipenda completamente da un Datore di Lavoro, avente la totale responsabilità del sistema di gestione per la salute e la sicurezza sul lavoro.

C.2 Riferimenti

EA-3/13 M:2016 EA Document on the Application of ISO/IEC 17021-1 for the Certification of Occupational Health and Safety Management Systems (OH&SMS)

C.3 Definizioni

Vale in generale la terminologia riportata nella Norma OHSAS 18001.

SGSSL: sistema di gestione per la Salute e la Sicurezza sul Lavoro (o sul Luogo di Lavoro).

C.4 Requisiti

C.4.1 Per ottenere la certificazione da parte di IIS CERT, un SGSSL deve soddisfare inizialmente e nel tempo i requisiti della norma OHSAS 18001 e quelli aggiuntivi previsti dagli Organismi di Accreditamento (es.: Regolamento Tecnico ACCREDIA RT-12, EA-3/13).

C.4.2 In particolare, per ottenere la certificazione del SGSSL, l'Organizzazione deve:

- a) rendere disponibile una dichiarazione formale di consapevolezza del fatto che il rispetto delle norme cogenti riguardanti salute e sicurezza sul lavoro sono un pre-requisito essenziale ed imprescindibile per l'attuazione di un SGSSL e che la propria Organizzazione ha già provveduto a verificarne l'esistenza;
- b) fornire le informazioni camerali (copia della visura camerale o documento equivalente), l'elenco delle risorse umane e delle risorse tecniche e logistiche e l'esistenza o meno di pregresse sanzioni e/o condanne relative ad aspetti di salute e sicurezza sul lavoro;
- c) avere effettuato un'analisi preliminare che comprenda:
 - una descrizione dettagliata del tipo di attività svolte nel sito/i per il quale è richiesta la certificazione del SGSSL e dei processi da sottoporre a valutazione, comprensiva di leggi e regolamenti che li disciplinano;
 - una identificazione dei pericoli sulla sicurezza e la salute sul lavoro associati alle proprie attività e relativi rischi e la procedura per l'identificazione puntuale dei pericoli, per la valutazione dei rischi e per l'attuazione delle necessarie misure di controllo;
- d) rendere disponibile:
 - una copia della documentazione che descrive il SGSSL incluso l'elenco degli estremi identificativi della normativa relativa a sicurezza e salute dei lavoratori cogente per il tipo di attività effettuata;
 - la procedura per l'identificazione puntuale dei pericoli, per la valutazione dei rischi e per l'attuazione delle necessarie misure di controllo;
 - la procedura per l'identificazione dei potenziali eventi accidentali e le potenziali situazioni di emergenza;
 - tutti i documenti inerenti la valutazione dei rischi, ove applicabili (DVR, DUVRI, POS, PSC, etc.).

C.5 Certificazione iniziale

C.5.1 Oltre a quanto stabilito nella Parte generale, l'Organizzazione deve comunicare a IIS CERT eventuali siti temporaneamente esclusi dal campo di applicazione del SGSSL ai fini della verifica dell'ammissibilità di tali esclusioni (vedere in proposito anche il § C.10.1).

C.5.2 Unitamente alla richiesta di certificazione, o successivamente alla stessa, l'Organizzazione, oltre a quanto stabilito nella Parte generale, dovrà rendere disponibile al IIS CERT anche una relazione conclusiva dell'analisi preliminare dell'Organizzazione.

La documentazione di cui sopra è valutata da IIS CERT per conformità alla Norma di riferimento ed ai requisiti del presente Regolamento.

L'esito di questo esame è comunicato al richiedente con l'invio di una copia del rapporto di esame documentale (se questo è effettuato presso gli uffici del IIS CERT); eventuali rilievi riscontrati nella documentazione considerati critici devono essere risolti dall'Organizzazione, a soddisfazione del IIS CERT, prima del prosieguo dell'iter certificativo.

La documentazione di cui sopra è, in generale, trattenuta per uso di archivio da IIS CERT.

Se l'audit di stage 1 è effettuato completamente on-site, l'esito dell'esame della documentazione è comunque riportato sul rapporto di esame documentale e sarà consegnato all'Organizzazione unitamente al rapporto di stage 1 "onsite" di cui al § 5.3.

C.5.3 Durante l'audit di stage 1 "on-site", gli Auditor qualificati di IIS CERT, effettuando anche sopralluoghi sul sito/i ed interviste con il personale dell'Organizzazione, verificano quantomeno:

- a) che la documentazione del sistema di gestione, incluse le procedure, copra tutti i requisiti della Norma di riferimento;
- b) che sia stato effettuato un ciclo di audit completo esteso a tutti i siti ed il relativo riesame della direzione;
- c) che il sistema di gestione comprenda un processo solido, dinamico e partecipato di identificazione dei pericoli e valutazione dei relativi rischi compresi anche quelli derivanti dai processi messi in essere da fornitori che operano, anche in modo sporadico, presso il/i sito/i certificando o quelli relativi alla presenza di visitatori;
- d) l'esistenza e l'efficacia di adeguati programmi e/o sistemi di manutenzione;
- e) che il processo di individuazione e di analisi dei pericoli e la valutazione dei rischi sia descritto in una specifica procedura, che specifichi nel tempo i criteri di monitoraggio di tali rischi e che coinvolga il personale addetto ai diversi processi;
- f) che l'individuazione e l'analisi dei pericoli e la valutazione dei relativi rischi siano, concretamente, l'input per il processo di miglioramento continuo;
- g) che siano stati redatti tutti i documenti applicabili inerenti la valutazione dei rischi (DVR, DUVRI, POS, etc.);
- h) che esistano adeguati obiettivi per la salute e la sicurezza sul lavoro e che tali obiettivi siano supportati da una pianificazione e programmazione tecnica e finanziaria; che gli obiettivi e gli indicatori siano coerenti con la valutazione dei rischi;
- i) che sia effettuato almeno il primo riesame da parte della direzione;
- j) che il piano di formazione e di informazione delle risorse umane sia definito in base alla relativa analisi delle esigenze ed attuato;
- k) che sia stata definita una procedura per l'analisi delle non conformità, degli incidenti, dei "quasi incidenti" e degli infortuni;
- l) che l'Organizzazione disponga delle necessarie autorizzazioni riguardanti la salute e la sicurezza, relative alle sue attività, in corso di validità;
- m) che l'Organizzazione risulti conforme agli adempimenti contenuti nei documenti di cui alla lettera k) oltre che agli adempimenti richiesti dalla alla legislazione sulla salute e sicurezza ad essa applicabile.

Nel caso in cui quanto specificato alle suddette lettere l) ed m) non sia formalmente soddisfatto si rimanda a quanto esplicitato al § 5.6.

C.5.4 L'audit è effettuato da Auditor qualificati di IIS CERT sulla base del rapporto di audit di stage 1 e dei seguenti documenti, oltre a quelli previsti dalla Parte generale, predisposti dall'Organizzazione nella revisione aggiornata:

- rapporto di audit di stage 1,
- documenti di valutazione dei rischi applicabili (DVR, DUVRI, POS, PSC, etc.).

C.5.5 L'audit di stage 2 prevede sempre:

- la verifica del turno di notte (ove applicabile);
- un'intervista riservata al Medico Competente (MC);
- un'intervista riservata al Rappresentante dei Lavoratori per la Sicurezza (RLS).

La valutazione di un sito o di un processo non può mai essere parziale.

C.5.6 In mancanza di autorizzazioni, o documenti equivalenti, in campo della salute e sicurezza sul luogo di lavoro, richiesti dalla legislazione vigente, il processo di certificazione è sospeso.

In presenza di rilievi, accertati nel corso degli audit, legati al mancato rispetto di requisiti legislativi cogenti in campo della salute e sicurezza sul luogo di lavoro (limiti e/o disposizioni di legge, limiti e/o prescrizioni riportate su autorizzazioni/Licenze o su altri documenti prescrittivi, etc.), il processo di certificazione, salvo casi particolari, è sospeso fino a quando l'Organizzazione non dimostri il rispetto di tali requisiti.

C.6 Mantenimento della certificazione

C.6.2 Oltre a quanto previsto dalla Parte generale, l'Organizzazione deve mantenere registrazioni relative a:

- a) incidenti/emergenze occorse nel sito/i e di altri eventi che potenzialmente avrebbero potuto avere effetti negativi sulla salute e sicurezza dei lavoratori;
- b) eventuali osservazioni o segnalazioni pervenute dalle autorità nazionali o locali preposte al controllo dei luoghi di lavoro

e deve renderle disponibile a IIS CERT unitamente alle relative azioni correttive intraprese durante gli audit periodici.

In particolare l'Organizzazione è tenuta a dare prontamente informazione ad IIS CERT, che valuterà le azioni da intraprendere, in merito ad eventuali osservazioni o segnalazioni pervenute dalle autorità nazionali o locali preposte al controllo dei luoghi di lavoro, riconducibili al § 5.6 per tutte le attività svolte dall'Organizzazione indipendentemente dal campo di applicazione del SGSSL.

Inoltre, nei casi in cui l'Organismo garante delle certificazioni emesse dal IIS CERT e/o le autorità competenti segnalano ad IIS CERT criticità legate alla gestione della salute e sicurezza nei luoghi di lavoro, si applica quanto indicato al § 6.5.

C.6.3 Per certificazioni rilasciate in Italia, devono essere effettuati 2 o 3 audit di sorveglianza presso il sito/i prima dell'inizio delle attività di ricertificazione con periodicità che varia a seconda dell'attività svolta dall'Organizzazione (in particolare dalla sua "complessità"), in base a quanto stabilito da ACCREDIA nel documento RT-12 (documento reperibile direttamente sul sito web di ACCREDIA o contattando IIS CERT).

C.6.4 Nel corso degli audit di sorveglianza è ripetuta almeno una volta l'intervista riservata al RLS.

C.6.5 Per le Organizzazioni definite ad alta complessità dal suddetto documento RT-12, l'audit di prima sorveglianza avviene entro 6 mesi dall'audit iniziale.

C.9 Modifica della certificazione e comunicazione dei cambiamenti

C.9.6 Le richieste di estensione della certificazione ad ogni nuovo sito o processo comportano sempre la pianificazione e l'esecuzione di audit aggiuntivi (di estensione), per i quali sarà avviato l'iter di delibera.

C.10 Organizzazioni multisito

C.10.1 Ove un'Organizzazione disponga di più siti, tutti gli stessi dovranno adottare e certificare il SGSSL, sulla scorta di un programma definito e delimitato in termini cronologici, che preveda la certificazione di tutti i siti entro 24 mesi dalla valutazione iniziale (salvo tempestiva e motivata comunicazione ad ACCREDIA di particolari esigenze di deroga a tale criterio).

Il campionamento dei siti seguirà anche le regole della disposizione ACCREDIA del 2010-02-23 (vedere § 2).

Oltre alle attività definite dalla Parte generale, anche l'analisi e la valutazione dei rischi nei siti devono essere gestite dalla funzione centrale dell'Organizzazione.

C.12 Trasferimento di certificati accreditati

C.12.1 Per il trasferimento di certificati accreditati si applicano anche le regole della disposizione ACCREDIA del 2010-02-23 (vedere § 2).

C.19 Elementi aggiuntivi previsti dal documento EA-3/13

Con riferimento ai requisiti aggiuntivi, ai fini dell'accreditamento, introdotti dal documento EA-3/13 (che elenca una serie di punti integrativi rispetto alla ISO/IEC 17021-1), nel presente paragrafo sono elencati tutti gli elementi aggiuntivi oppure rafforzativi/chiarificativi rispetto a quanto in precedenza indicato; tali elementi potranno essere applicati da IIS CERT nei confronti delle organizzazioni certificate/certificande dal momento della richiesta di transizione del proprio accreditamento, previa apposita comunicazione alle organizzazioni stesse.

Per comodità di confronto, i suddetti elementi riportano anche il riferimento ai pertinenti requisiti del documento EA-3/13 (i quali peraltro sono corrispondenti, a meno della lettera iniziale, ai punti della ISO/IEC 17021-1).

rif. EA-3/13	Requisiti aggiuntivi / integrativi												
C.19.1	<table border="1"> <tr> <td data-bbox="225 562 379 595">C.3</td> <td data-bbox="379 562 1482 595"><u>Introduzione</u></td> </tr> <tr> <td data-bbox="225 595 379 1458">C.3.1+C.3.8</td> <td data-bbox="379 595 1482 1458"> <p>La certificazione del SGSSL di un'organizzazione, rilasciata da IIS CERT sotto accreditamento, indica la conformità (<i>conformity</i>) ai requisiti della norma di certificazione ed include un impegno dimostrato ed effettivo alla conformità (<i>compliance</i>) ai requisiti legali applicabili; ciò comporta quanto segue:</p> <ul style="list-style-type: none"> - la tenuta sotto controllo della conformità legale da parte dell'organizzazione costituisce una componente importante della valutazione del SGSSL e rimane di responsabilità dell'organizzazione stessa; - gli Auditor di IIS CERT non sono ispettori delle autorità di controllo e pertanto non rilasciano dichiarazioni di conformità legale, potendo tuttavia verificare la conformità legale allo scopo di valutare la conformità alla norma di certificazione; - una certificazione accreditata di un SGSSL soddisfacente i requisiti della norma di certificazione non costituisce una garanzia assoluta e continua di conformità legale (come del resto nessuna certificazione o schema legale può garantire una conformità legale continua), pur tuttavia un SGSSL costituisce uno strumento collaudato ed efficace per raggiungere ed ottenere la conformità legale e fornisce all'alta direzione informazioni pertinenti e tempestive sullo stato di conformità dell'organizzazione; - le norme di certificazione richiedono un impegno al rispetto dei requisiti legali e l'organizzazione deve essere in grado di dimostrare di aver raggiunto la conformità ai requisiti legali applicabili anche attraverso una propria valutazione di conformità prima dell'intervento di IIS CERT; - la certificazione di un SGSSL come soddisfacente i requisiti della norma di certificazione conferma che lo stesso SGSSL ha dimostrato di essere efficace nel raggiungimento dei suoi impegni di politica aziendale, compresa la conformità legale, e fornisce la base ed il supporto per una continua conformità legale; - allo scopo di mantenere la fiducia delle parti interessate nei suddetti attributi di una certificazione emessa sotto accreditamento, IIS CERT opera in modo tale da assicurare che il sistema dimostri efficacia prima di emettere o confermare la certificazione; - un SGSSL può costituire uno strumento di dialogo tra l'organizzazione e le pertinenti autorità di controllo e rappresentare la base per una collaborazione fiduciosa, ribaltando eventuali diversi contraddittori ed inoltre le autorità di controllo ed il pubblico dovrebbero riporre fiducia nei confronti di organizzazioni certificate e percepirle come in grado di gestire in modo costante ed efficace la propria conformità legale. </td> </tr> </table>	C.3	<u>Introduzione</u>	C.3.1+C.3.8	<p>La certificazione del SGSSL di un'organizzazione, rilasciata da IIS CERT sotto accreditamento, indica la conformità (<i>conformity</i>) ai requisiti della norma di certificazione ed include un impegno dimostrato ed effettivo alla conformità (<i>compliance</i>) ai requisiti legali applicabili; ciò comporta quanto segue:</p> <ul style="list-style-type: none"> - la tenuta sotto controllo della conformità legale da parte dell'organizzazione costituisce una componente importante della valutazione del SGSSL e rimane di responsabilità dell'organizzazione stessa; - gli Auditor di IIS CERT non sono ispettori delle autorità di controllo e pertanto non rilasciano dichiarazioni di conformità legale, potendo tuttavia verificare la conformità legale allo scopo di valutare la conformità alla norma di certificazione; - una certificazione accreditata di un SGSSL soddisfacente i requisiti della norma di certificazione non costituisce una garanzia assoluta e continua di conformità legale (come del resto nessuna certificazione o schema legale può garantire una conformità legale continua), pur tuttavia un SGSSL costituisce uno strumento collaudato ed efficace per raggiungere ed ottenere la conformità legale e fornisce all'alta direzione informazioni pertinenti e tempestive sullo stato di conformità dell'organizzazione; - le norme di certificazione richiedono un impegno al rispetto dei requisiti legali e l'organizzazione deve essere in grado di dimostrare di aver raggiunto la conformità ai requisiti legali applicabili anche attraverso una propria valutazione di conformità prima dell'intervento di IIS CERT; - la certificazione di un SGSSL come soddisfacente i requisiti della norma di certificazione conferma che lo stesso SGSSL ha dimostrato di essere efficace nel raggiungimento dei suoi impegni di politica aziendale, compresa la conformità legale, e fornisce la base ed il supporto per una continua conformità legale; - allo scopo di mantenere la fiducia delle parti interessate nei suddetti attributi di una certificazione emessa sotto accreditamento, IIS CERT opera in modo tale da assicurare che il sistema dimostri efficacia prima di emettere o confermare la certificazione; - un SGSSL può costituire uno strumento di dialogo tra l'organizzazione e le pertinenti autorità di controllo e rappresentare la base per una collaborazione fiduciosa, ribaltando eventuali diversi contraddittori ed inoltre le autorità di controllo ed il pubblico dovrebbero riporre fiducia nei confronti di organizzazioni certificate e percepirle come in grado di gestire in modo costante ed efficace la propria conformità legale. 								
C.3	<u>Introduzione</u>												
C.3.1+C.3.8	<p>La certificazione del SGSSL di un'organizzazione, rilasciata da IIS CERT sotto accreditamento, indica la conformità (<i>conformity</i>) ai requisiti della norma di certificazione ed include un impegno dimostrato ed effettivo alla conformità (<i>compliance</i>) ai requisiti legali applicabili; ciò comporta quanto segue:</p> <ul style="list-style-type: none"> - la tenuta sotto controllo della conformità legale da parte dell'organizzazione costituisce una componente importante della valutazione del SGSSL e rimane di responsabilità dell'organizzazione stessa; - gli Auditor di IIS CERT non sono ispettori delle autorità di controllo e pertanto non rilasciano dichiarazioni di conformità legale, potendo tuttavia verificare la conformità legale allo scopo di valutare la conformità alla norma di certificazione; - una certificazione accreditata di un SGSSL soddisfacente i requisiti della norma di certificazione non costituisce una garanzia assoluta e continua di conformità legale (come del resto nessuna certificazione o schema legale può garantire una conformità legale continua), pur tuttavia un SGSSL costituisce uno strumento collaudato ed efficace per raggiungere ed ottenere la conformità legale e fornisce all'alta direzione informazioni pertinenti e tempestive sullo stato di conformità dell'organizzazione; - le norme di certificazione richiedono un impegno al rispetto dei requisiti legali e l'organizzazione deve essere in grado di dimostrare di aver raggiunto la conformità ai requisiti legali applicabili anche attraverso una propria valutazione di conformità prima dell'intervento di IIS CERT; - la certificazione di un SGSSL come soddisfacente i requisiti della norma di certificazione conferma che lo stesso SGSSL ha dimostrato di essere efficace nel raggiungimento dei suoi impegni di politica aziendale, compresa la conformità legale, e fornisce la base ed il supporto per una continua conformità legale; - allo scopo di mantenere la fiducia delle parti interessate nei suddetti attributi di una certificazione emessa sotto accreditamento, IIS CERT opera in modo tale da assicurare che il sistema dimostri efficacia prima di emettere o confermare la certificazione; - un SGSSL può costituire uno strumento di dialogo tra l'organizzazione e le pertinenti autorità di controllo e rappresentare la base per una collaborazione fiduciosa, ribaltando eventuali diversi contraddittori ed inoltre le autorità di controllo ed il pubblico dovrebbero riporre fiducia nei confronti di organizzazioni certificate e percepirle come in grado di gestire in modo costante ed efficace la propria conformità legale. 												
C.19.2	<table border="1"> <tr> <td data-bbox="225 1464 379 1498">C.1</td> <td data-bbox="379 1464 1482 1498"><u>Metodologia seguita da IIS CERT nella valutazione della conformità legale</u></td> </tr> <tr> <td data-bbox="225 1498 379 1621">C.1.1</td> <td data-bbox="379 1498 1482 1621">Attraverso il processo di valutazione, IIS CERT valuta la conformità dell'organizzazione ai requisiti della norma di certificazione per quanto questi si riferiscono alla conformità legale e non rilascia la certificazione finché la conformità non sia raggiunta; dopo l'emissione della certificazione, le sorveglianze ed il rinnovo successivi effettuati da IIS CERT si basano sulla medesima metodologia.</td> </tr> <tr> <td data-bbox="225 1621 379 1711">C.1.2</td> <td data-bbox="379 1621 1482 1711">Relativamente al bilanciamento tra il riesame di documenti e registrazioni presso i propri uffici e la valutazione della implementazione del SGSSL nel corso delle attività operative, IIS CERT assicura un audit adeguato della efficacia del SGSSL.</td> </tr> <tr> <td data-bbox="225 1711 379 1834">C.1.3</td> <td data-bbox="379 1711 1482 1834">IIS CERT assicura, attraverso un appropriato programma di sorveglianza, che la conformità è mantenuta durante il ciclo triennale di certificazione; gli Auditor di IIS CERT verificano la gestione della conformità legale basandosi sulla implementazione dimostrata del sistema e non solamente sui risultati pianificati o attesi.</td> </tr> <tr> <td data-bbox="225 1834 379 1924">C.1.4</td> <td data-bbox="379 1834 1482 1924">Una organizzazione che fallisca nel dimostrare il proprio impegno iniziale o continuo verso la conformità legale attraverso gli elementi chiave sotto descritti non sarà certificata da IIS CERT, o la certificazione già concessa non sarà mantenuta, come conforme ai requisiti della norma di certificazione.</td> </tr> <tr> <td data-bbox="225 1924 379 2009">C.1.5</td> <td data-bbox="379 1924 1482 2009">Una non conformità intenzionale o ripetuta è considerata da IIS CERT una grave mancanza nel sostenere l'impegno al raggiungimento della conformità legale e preclude il rilascio della certificazione o determina la sua sospensione o ritiro.</td> </tr> </table>	C.1	<u>Metodologia seguita da IIS CERT nella valutazione della conformità legale</u>	C.1.1	Attraverso il processo di valutazione, IIS CERT valuta la conformità dell'organizzazione ai requisiti della norma di certificazione per quanto questi si riferiscono alla conformità legale e non rilascia la certificazione finché la conformità non sia raggiunta; dopo l'emissione della certificazione, le sorveglianze ed il rinnovo successivi effettuati da IIS CERT si basano sulla medesima metodologia.	C.1.2	Relativamente al bilanciamento tra il riesame di documenti e registrazioni presso i propri uffici e la valutazione della implementazione del SGSSL nel corso delle attività operative, IIS CERT assicura un audit adeguato della efficacia del SGSSL.	C.1.3	IIS CERT assicura, attraverso un appropriato programma di sorveglianza, che la conformità è mantenuta durante il ciclo triennale di certificazione; gli Auditor di IIS CERT verificano la gestione della conformità legale basandosi sulla implementazione dimostrata del sistema e non solamente sui risultati pianificati o attesi.	C.1.4	Una organizzazione che fallisca nel dimostrare il proprio impegno iniziale o continuo verso la conformità legale attraverso gli elementi chiave sotto descritti non sarà certificata da IIS CERT, o la certificazione già concessa non sarà mantenuta, come conforme ai requisiti della norma di certificazione.	C.1.5	Una non conformità intenzionale o ripetuta è considerata da IIS CERT una grave mancanza nel sostenere l'impegno al raggiungimento della conformità legale e preclude il rilascio della certificazione o determina la sua sospensione o ritiro.
C.1	<u>Metodologia seguita da IIS CERT nella valutazione della conformità legale</u>												
C.1.1	Attraverso il processo di valutazione, IIS CERT valuta la conformità dell'organizzazione ai requisiti della norma di certificazione per quanto questi si riferiscono alla conformità legale e non rilascia la certificazione finché la conformità non sia raggiunta; dopo l'emissione della certificazione, le sorveglianze ed il rinnovo successivi effettuati da IIS CERT si basano sulla medesima metodologia.												
C.1.2	Relativamente al bilanciamento tra il riesame di documenti e registrazioni presso i propri uffici e la valutazione della implementazione del SGSSL nel corso delle attività operative, IIS CERT assicura un audit adeguato della efficacia del SGSSL.												
C.1.3	IIS CERT assicura, attraverso un appropriato programma di sorveglianza, che la conformità è mantenuta durante il ciclo triennale di certificazione; gli Auditor di IIS CERT verificano la gestione della conformità legale basandosi sulla implementazione dimostrata del sistema e non solamente sui risultati pianificati o attesi.												
C.1.4	Una organizzazione che fallisca nel dimostrare il proprio impegno iniziale o continuo verso la conformità legale attraverso gli elementi chiave sotto descritti non sarà certificata da IIS CERT, o la certificazione già concessa non sarà mantenuta, come conforme ai requisiti della norma di certificazione.												
C.1.5	Una non conformità intenzionale o ripetuta è considerata da IIS CERT una grave mancanza nel sostenere l'impegno al raggiungimento della conformità legale e preclude il rilascio della certificazione o determina la sua sospensione o ritiro.												

	C.1.6	Nel caso le strutture e le aree di lavoro siano soggette a chiusura, i rischi si modificano, in quanto potrebbero non esistere più i medesimi rischi per i lavoratori, ma potrebbero insorgere nuovi rischi nei confronti della comunità (es. in caso di mancanza di adeguate attività di manutenzione e sorveglianza): IIS CERT verifica che il sistema di gestione continui a soddisfare la norma di certificazione e sia efficacemente implementato a riguardo delle strutture e aree di lavoro chiuse e, in caso contrario, sospende la certificazione.
C.19.3	C.2	<u>Criteria di conformità da soddisfare ai fini della delibera della certificazione</u>
	C.2.1	Le parti interessate di un'organizzazione che sostiene la conformità ad una norma di certificazione si attendono una piena conformità legale: il valore percepito di una certificazione accreditata in questo campo è strettamente legato alla soddisfazione raggiunta dalle parti interessate nei confronti della conformità legale.
	C.2.2	L'organizzazione deve essere in grado di dimostrare di aver raggiunto la conformità ai requisiti legali ad essa applicabili attraverso una propria valutazione di conformità prima che IIS CERT rilasci la certificazione.
	C.2.3	Qualora l'organizzazione non abbia raggiunto la conformità legale, essa deve essere in grado di dimostrare un accordo documentato con l'autorità competente oppure un piano di implementazione per raggiungere la piena conformità; la riuscita implementazione di tale piano deve essere considerata prioritaria nell'ambito del sistema di gestione.
	C.2.4	IIS CERT può ancora concedere la certificazione in casi eccezionali, ma ricercherà evidenze oggettive che possano confermare che il SGSSL è in grado di raggiungere la conformità richiesta attraverso l'implementazione completa del piano suddetto.
C.19.4	App. B	<u>Determinazione dei tempi di audit</u> IIS CERT determina i tempi di audit sulla base della propria procedura CER_QAS 096 I, nella quale sono recepiti gli elementi addizionali della EA-3/13. <i>Di seguito sono riportati soltanto gli elementi della appendice B del documento EA-3/13 pertinenti ai fini del presente regolamento.</i>
	B.9.2	La necessità di visitare siti temporanei (dai più estesi siti di gestione dei progetti fino ai siti di installazione/servizio) e l'estensione del campionamento sono basate da IIS CERT sui rischi di fallimento del SGSSL nel controllo dei rischi associati con le operazioni del cliente; nel campionamento dei siti, IIS CERT tiene conto anche delle necessità di competenza e delle variazioni di servizio in considerazione delle dimensioni e dei tipi di attività, così come dello stato di avanzamento dei progetti e dei relativi rischi.
	B.9.3	Normalmente, IIS CERT prevede una visita ai siti temporanei; tuttavia, IIS CERT tiene in considerazione i seguenti metodi come alternative per sostituire quelle parti di un audit <i>on-site</i> ad un sito temporaneo non determinanti ai fini della verifica diretta del controllo operativo e di altre attività del SGSSL: <ul style="list-style-type: none"> - interviste o riunioni con il cliente e/o i suoi committenti, in persona o in teleconferenza; - riesame documentale delle attività del sito temporaneo; - accesso remoto a reti internet o intranet contenenti registrazioni o altre informazioni rilevanti ai fini della valutazione del SGSSL e del sito temporaneo; - utilizzo di video o teleconferenza ed altre tecnologie che consentano un audit remoto efficace.
	B.11.1	Qualora una organizzazione subappalti una parte delle proprie funzioni o dei propri processi, IIS CERT ricerca evidenze che l'organizzazione abbia effettivamente determinato il tipo e l'estensione dei controlli da applicare allo scopo di garantire che le funzioni o i processi esterni non influenzino negativamente l'efficacia del SGSSL, inclusa la capacità dell'organizzazione di tenere sotto controllo i propri rischi e l'impegno a rispettare la conformità di requisiti di legge.
	B.11.2	IIS CERT sottopone ad audit e valuta l'efficacia del SGSSL dell'organizzazione nel gestire le attività subappaltate ed il rischio che questo pone alle prestazioni, in tema di salute e sicurezza sul lavoro, delle proprie attività e dei propri processi ed ai requisiti di conformità. Quanto sopra include una raccolta di informazioni di ritorno sul livello di efficacia da parte dei fornitori, sulla base di quanto segue: <ul style="list-style-type: none"> - criteri applicati dall'organizzazione per valutare, selezionare, monitorare le prestazioni e rivalutare tali fornitori esterni, basati sulla capacità di questi di fornire funzioni o processi in accordo a requisiti specifici, in conformità ai requisiti di legge, e - rischio che i fornitori esterni possano influenzare negativamente la capacità dell'organizzazione di tenere sotto controllo i propri rischi.
	B.11.3	Nella pianificazione e nella realizzazione di un audit efficace, IIS CERT tiene in conto quei processi o quelle funzioni inclusi nello scopo del SGSSL di un'organizzazione che siano stati esternalizzati, pur considerando che non è richiesto un audit completo al sistema di gestione del fornitore.
	B.11.4	IIS CERT stabilisce quanto al punto precedente sia durante la preparazione del programma di certificazione, verificandolo successivamente durante l'audit iniziale, sia prima di ogni audit di sorveglianza e di rinnovo.

C.19.5	4	<u>Principi generali</u>
	G 4.1.2	Oltre ai lavoratori permanenti e temporanei ed ai loro rappresentanti, le parti che hanno un interesse in una certificazione del SGSSL includono (non esaustivamente): -) autorità giuridiche e regolamentari (locali, regionali, nazionali o internazionali); -) società madri; -) fornitori, appaltatori e subappaltatori; -) sindacati dei lavoratori e organizzazioni datoriali; -) proprietà, azionisti, clienti, visitatori, comunità locali e vicinato dell'organizzazione e il pubblico in generale; -) clienti, servizi medici ed altri servizi sociali, media, mondo accademico, associazioni imprenditoriali e organizzazioni non governative; -) organizzazioni e professionisti (es. dottori ed infermieri) di salute e sicurezza sul lavoro.
C.19.6	8	<u>Requisiti relativi alle informazioni</u>
	G 8.5.3	IIS CERT richiede di essere tempestivamente informato dal cliente certificato in caso di un incidente grave o di una violazione di legge che richieda l'intervento dell'autorità preposta.
C.19.7	9	<u>Requisiti di processo</u>
	G 9.1.1	Le informazioni fornite a IIS CERT da parte del rappresentante autorizzato dell'organizzazione richiedente su aspetti significativi dei suoi processi ed operazioni comprende anche l'identificazione dei rischi significativi per la salute e sicurezza sul lavoro, i materiali pericolosi utilizzati nei processi e gli eventuali obblighi di legge relativi alla legislazione applicabile; la richiesta deve contenere dettagli dei dipendenti che lavorano presso le sedi dell'organizzazione e di quelli che lavorano al di fuori di esse.
	G 9.1.4	IIS CERT determina i tempi di audit sulla base della propria procedura CER_QAS 096 I, che tiene conto dei requisiti fissati nei documenti IAF MD 5 ed EA-3/13. Se il richiedente fornisce personale ad altre organizzazioni, IIS CERT verifica che il suo SGSSL tenga conto di tale situazione; nella determinazione del tempo di audit, IIS CERT può considerare necessario, registrando la decisione, sottoporre ad audit il sito dell'organizzazione dove tale personale opera, in considerazione dei rischi associati alle attività ivi realizzate, degli accordi contrattuali tra le diverse organizzazioni, della presenza di certificazioni aziendali pertinenti, del sistema di audit interno e delle statistiche su incidenti e quasi-incidenti.
	G 9.1.5	Nel caso di un SGSSL operato su più siti, IIS CERT stabilisce se il campionamento è applicabile oppure no, sulla base del livello dei rischi associati alla natura delle attività e dei processi realizzati in ciascun sito incluso nello scopo della certificazione, e determina la decisione sulla base dell'Appendice B del documento EA-3/13; IIS CERT può altresì applicare riduzioni quando certi processi del sistema di gestione non sono importanti per un determinato sito e ricadono sotto la responsabilità primaria del sito principale, documentando le decisioni relative al piano di campionamento per ciascun cliente. In caso di siti multipli che non ricoprono le medesime attività ed i medesimi processi ed organizzazioni ad alta complessità di rischio, IIS CERT non applica il campionamento. Anche se un sito realizza processi simili o fabbrica prodotti simili rispetto ad altri siti, IIS CERT tiene in considerazione le differenze tra le operazioni di ciascun sito (tecnologia, attrezzature, quantità di materiali pericolosi utilizzati ed immagazzinati, ambiente di lavoro, locali, etc.). Quando il campionamento è ritenuto applicabile, IIS CERT assicura che il campionamento dei siti da visitare è rappresentativo di tutti i livelli e tipi di processi, attività e rischi esistenti nell'organizzazione da certificare. IIS CERT considera altresì che i siti temporanei coperti dal SGSSL sono soggetti ad audit sulla base del campionamento, allo scopo di fornire evidenza del funzionamento e dell'efficacia del sistema di gestione.
	G 9.2.1.2 b)	Ai fini della determinazione della capacità del sistema di gestione di assicurare che il cliente soddisfa i requisiti di legge, normativi e contrattuali applicabili, IIS CERT applica l'approccio descritto nell'Appendice A del documento EA-3/13, come indicato ai punti da C.19.1 a C.19.3.
	G 9.2.1.3	Definito lo scopo, il SGSSL deve includere le attività, i prodotti ed i servizi sotto il controllo o l'influenza dell'organizzazione che possono impattare sulle prestazioni del sistema stesso. I siti temporanei (per esempio i cantieri di costruzione) devono essere compresi nel SGSSL dell'organizzazione che ha il controllo degli stessi, indipendentemente da dove sono localizzati; IIS CERT determina la necessità di visitare tali siti e l'estensione del campionamento sulla base di una valutazione del rischio di fallimento del sistema di gestione nel controllo dei rischi associati con le operazioni del cliente.
	G 9.4.4.2	In sede di valutazione, gli Auditor di IIS CERT effettuano sempre interviste al seguente personale: -) personale dirigente con responsabilità legale per gli aspetti di salute e sicurezza; -) rappresentante dei lavoratori per la sicurezza (RLS); -) personale responsabile per il monitoraggio della salute degli impiegati (es. medici); -) impiegati permanenti e temporanei.

	<p>Gli Auditor di IIS CERT possono anche effettuare interviste al seguente personale:</p> <ul style="list-style-type: none"> -) dirigenti per la sicurezza e preposti; -) dirigenti ed impiegati degli appaltatori.
G 9.4.5.3	In caso rilevi una non conformità rispetto ai requisiti di legge, IIS CERT la comunica immediatamente alla organizzazione sottoposta ad audit (la gestione di tale non conformità è la medesima descritta ai §§ 3 e 5.6 della parte generale del presente regolamento).
G 9.4.7.1	Il personale invitato da IIS CERT a presenziare alla riunione di chiusura dell'audit comprende il responsabile del SGSSL, il personale responsabile del monitoraggio della salute dei lavoratori ed il RLS.
G 9.6.4.2	Indipendentemente dal coinvolgimento dell'autorità competente, IIS CERT può ritenere necessario un audit aggiuntivo qualora venga a conoscenza di un incidente rilevante inerente la salute e sicurezza dei lavoratori (es. un infortunio grave oppure una violazione di legge), allo scopo di indagare se il sistema di gestione risulti compromesso o funzioni efficacemente, documentando l'esito di tale attività.
G 9.6.5.2	Le informazioni relative ad incidenti, quali un infortunio grave oppure una violazione di legge che comportino l'interessamento dell'autorità preposta, comunicato dal cliente (vedere § C.19.4) o direttamente registrato dagli Auditor durante l'audit aggiuntivo (vedere § C.19.13), devono fornire elementi sufficienti ad IIS CERT per decidere le azioni da intraprendere, compresa la sospensione o il ritiro della certificazione, qualora si evidenzi che il sistema ha fallito nel soddisfare i requisiti della certificazione.
C.19.8	<p>App. A</p> <p><u>Qualifica degli auditor</u> <i>Per qualificare i propri auditor, IIS CERT applica quanto contenuto nella procedura CER_QAS 006 P.</i></p>