ICMQ
Certificazioni e controlli
per le costruzioni

ICMQ S.p.A. (a socio unico)
via G. De Castillia, 10 - 20124 Milano
tel. 02.7015.081 - fax 02.7015.0854
icmq@icmq.org - www.icmq.org
Capitale sociale € 750.000 i.v.
REA: MI/1630715
Registro Imprese di Milano
Cod. Fisc. e Part. IVA 13218350158

Condizioni Generali di Contratto

PER LA CERTIFICAZIONE ED IL MANTENIMENTO DEI SISTEMI DI GESTIONE

ALLEGATO
Sistemi di Gestione per la Sicurezza dell'Informazione

Norma di riferimento: UNI CEI EN ISO/IEC 27001

PREMESSA

Il presente documento costituisce parte integrante delle Condizioni Generali di per la certificazione ed il mantenimento dei sistemi di gestione e specifica i requisiti aggiuntivi applicabili alla certificazione dei Sistemi di Gestione per la Sicurezza dell'informazione in riferimento alle norme UNI CEI EN ISO/IEC 27001 e UNI CEI EN ISO/IEC 27006.

1. Dichiarazione di Applicabilità

L'Organizzazione deve rendere disponibile la Dichiarazione di Applicabilità richiesta del paragrafo 6.1.3. della UNI CEI EN ISO/IEC 27001; la versione/revisione di tale documento sarà riportata nel certificato. In caso di modifica alla Dichiarazione di Applicabilità, l'Organizzazione dovrà darne comunicazione a ICMQ indicando se vi sono modifiche ai controlli attuati. Sulla base delle informazioni fornite ICMQ valuterà la necessità di un aggiornamento del certificato.

2. Accesso alle informazioni documentate

Prima dell'avvio dell'audit l'Organizzazione comunica ICMQ la presenza di informazioni documentate che non possono essere rese disponibili al team di audit perché contenenti dati sensibili e/o riservati Qualora ICMQ valutasse che la non disponibilità di tali informazioni documentate possa compromettere l'efficacia dell'audit, il processo di certificazione non potrà proseguire fino a quando si sanno concordate adeguate modalità di consultazione.

3. Preparazione della verifica iniziale

La verifica iniziale è suddivisa in Audit di Stage 1 e Audit di Stage 2 come indicato nel paragrafo 10.3 delle Condizioni Generali di Contratto per la certificazione ed il mantenimento dei sistemi di gestione.

In aggiunta a quanto già indicato dal documento sopra citato si specifica che l'Organizzazione dovrà rendere accessibili i report degli audit interni e del Riesame Indipendente della Sicurezza delle Informazioni.

Durante l'audit di Stage 1 dovranno essere disponibili almeno le seguenti informazioni:

- Informazioni generali sul Sistema di Gestione per la Sicurezza dell'informazione e sulle attività da esso coperte;
- Documentazione specifica richiesta sella UNI CEI EN ISO/IEC 27001.

La certificazione può essere rilasciata se l'organizzazione non ha eseguito almeno un ciclo completo di audit interni un Riesame della Direzione a coprire tutte le attività rientranti nel campo di applicazione del Sistema di Gestione per la Sicurezza dell'Informazione.

4. Confini del Sistema di Gestione

Le interfacce con servizi o attività non completamente rientranti nell'ambito del Sistema di Gestione per la Sicurezza dell'Informazione (es: sistemi, database, sistemi di telecomunicazione condivisi con altre organizzazioni) devono essere gestite nell'ambito del Sistema di Gestione e incluse nella valutazione del rischio relativo alla sicurezza delle informazioni.

5. Organizzazioni multisito

Nel caso di organizzazioni operanti su più siti, qualora si verifichino le seguenti condizioni:

- Tutti i siti operano nell'ambito dello stesso Sistema di Gestione per la Sicurezza dell'Informazione che è amministrato in maniera centralizzata e soggetto ad audit e a un Riesame della Direzione centralizzato;
- Tutti i siti sono compresi nel programma di audit interno dell'Organizzazione;
- Tutti i siti sono compresi nel programma di Riesame della Direzione dell'Organizzazione.

ICMQ potrà valutare l'applicazione di un piano di campionamento sviluppato in applicazione dei Regolamenti applicabili a livello nazionale (Accredia) e internazionale (EA, IAF).

6. Campo di applicazione della certificazione

La certificazione può essere rilasciata esclusivamente alle attività su cui l'Organizzazione ha dato evidenza di operare al momento della verifica ed i cui processi sono stati oggetto di specifica valutazione da parte di ICMQ.

Il campo di applicazione del certificato sarà formulato indicando le attività che sono state oggetto di verifica.

Ove presenti, la verifica delle attività rientranti nel campo di applicazione del certificato potrà avvenire presso i cantieri e/o siti temporanei attivi.

7. Audit straordinari

Qualora ICMQ venisse a conoscenza, direttamente (segnalazione del Cliente) o indirettamente (notizie di stampa o altre fonti), di incidenti significativi o infrazioni legislative che coinvolgono il Cliente, ICMQ potrà eseguire un audit straordinario allo scopo di verificare se il Sistema di Gestione è non ha funzionato o se ne è stato compromesso il funzionamento.

A seguito dell'audit, ICMQ valuterà le azioni da intraprendere. Qualora fosse dimostrato che il Sistema di Gestione non rispetta i requisiti della Norma, tali azioni possono includere la sospensione o la revoca della certificazione.

In deroga a quanto sopra, la certificazione potrebbe essere mantenuta a condizione che l'organizzazione rispetti i requisiti definiti agli ultimi due paragrafi dell'articolo 1.