Icmq S.p.A. (A Socio Unico)
Società Benefit
Via G. De Castillia, 10 – 20124 Milano
Tel. 02 7015081 – Fax 02 70150854
icmq@icmq.org – www.icmq.it
P.I. 13218350158

Condizioni Generali di Contratto

PER LA CERTIFICAZIONE ED IL MANTENIMENTO DEI SISTEMI DI GESTIONE

ALLEGATO
Sistemi di Gestione
per la
Sicurezza delle Informazioni

PREMESSA

Il presente documento costituisce parte integrante delle Condizioni Generali 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 delle informazioni (SGSI) e dei servizi in cloud, che elaborano dati personali soggetti alle normative privacy e che agiscano in qualità di Data Processor, in riferimento:

- alle norme ISO/IEC 27001 e ISO/IEC 27006;
- alle linee guida ISO/IEC 27017 e ISO/IEC 27018.

Tutte le sopra citate norme si intendono in versione corrente.

1. Istruzione della Richiesta di Certificazione

Prima dell'avvio delle attività di certificazione, ICMQ emette un preventivo basato sulle informazioni fornite dal Cliente.

Al momento della richiesta di offerta l'Organizzazione compila un apposito allegato con il quale fornisce a ICMQ tutte le informazioni necessarie per l'effettuazione del calcolo dei tempi di audit che si determinano sulla base delle Appendici C e D della ISO/IEC 27006 tenendo conto di:

fattori connessi all'Organizzazione e al suo ramo di business,

- tipologia di attività;
- processi e procedure;
- livello di attuazione del Sistema di Gestione;

fattori connessi con l'ambiente IT,

- complessità della struttura informatica,
- dipendenza da outsourcing
- sviluppo del sistema informativo.

Nel caso di organizzazioni con più siti, l'Organizzazione compila il sopra citato allegato alla richiesta di offerta per ogni singolo sito da certificare.

Prima dell'avvio delle attività di certificazione, l'Organizzazione deve segnalare a ICMQ se alcune informazioni relative al suo SGSI (ad esempio, registrazioni del SGSI o informazioni sulla progettazione e l'efficacia dei controlli) non possono essere rese disponibili per la verifica iniziale (cfr. Art. 4) perché contengono informazioni riservate o sensibili. Nel caso, ICMQ valuta se il SGSI può essere comunque sottoposto adeguatamente ad audit in assenza di tali informazioni. Se tale valutazione ha esito negativo, ICMQ informa il cliente che la verifica iniziale non può aver luogo finché non vengono concesse adeguate modalità di accesso.

2. Dichiarazione di Applicabilità

L'Organizzazione deve rendere disponibile a ICMQ la Dichiarazione di Applicabilità (Statement of Applicability) richiesta dalla ISO/IEC 27001; la versione/revisione di tale documento viene riportata nel certificato. In caso di modifica alla Dichiarazione di Applicabilità, l'Organizzazione deve darne comunicazione a ICMQ indicando altresì se vi sono modifiche ai controlli attuati. Sulla base delle informazioni fornite, ICMQ aggiorna direttamente il certificato dell'Organizzazione oppure valuta la necessità di un'attività supplementare.

Una modifica alla Dichiarazione di Applicabilità che non modifichi la copertura dei controlli nell'ambito della certificazione non richiede un aggiornamento del certificato dell'Organizzazione, né la necessità di un'attività supplementare.

3. 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 può proseguire fino a quando si sono concordate adeguate modalità di consultazione.

4. 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 deve rendere accessibili i report degli audit interni e del Riesame Indipendente della Sicurezza delle Informazioni.

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

- informazioni generali sul Sistema di Gestione per la Sicurezza delle Informazioni e sulle attività da esso coperte;
- documentazione specifica richiesta dalla 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.

5. Confini del Sistema di Gestione

Le interfacce con servizi o attività non completamente rientranti nell'ambito del Sistema di Gestione per la Sicurezza delle Informazioni (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.

6. Organizzazioni multisito

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

- tutti i siti operano nell'ambito dello stesso Sistema di Gestione per la Sicurezza delle Informazioni 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 può valutare l'applicazione di un piano di campionamento sviluppato in coerenza ai Regolamenti applicabili a livello nazionale (Accredia) e internazionale (EA, IAF).

7. 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 è formulato indicando le attività che sono state oggetto di verifica.

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

L'identificazione dei siti dell'Organizzazione da inserire nel campo di applicazione del certificato è stabilita sulla base delle informazioni gestite dal singolo sito, tenendo presente che l'obiettivo del sistema di gestione è quello della protezione dei dati relativi alle attività rientranti nel medesimo campo di applicazione del certificato (ad esempio, potrebbe essere necessario includere un data center non presidiato mentre a sua volta potrebbe essere escluso un punto di appoggio logistico nel quale non sono archiviate o gestite informazioni significative).

Qualora nessuna delle attività rientranti nel campo di applicazione del certificato viene svolta dall'Organizzazione in una sede fisica definita, il certificato viene rilasciato con l'indicazione esplicita che in quella sede le attività dell'Organizzazione vengono svolte da remoto.

8. Certificazione ISO/IEC 27001 con integrazione delle linee guida ISO/IEC 27017 e ISO/IEC 27018

La linea guida ISO/IEC 27017 sui controlli per la sicurezza delle informazioni per i servizi in cloud può essere oggetto di estensione della certificazione ISO/IEC 27001 anche da sola. Ove si intenda considerare tale estensione anche in ottica di Protezione Dati Personali, l'estensione alla ISO/IEC 27017 deve essere integrata con la ISO/IEC 27018. Non è ammessa l'estensione alla sola ISO/IEC 27018.

Pertanto, qualora l'Organizzazione richiedesse l'integrazione di un certificato ISO/IEC 27001 esistente alle Linee Guida ISO/IEC 27017 e ISO/IEC 27018, ICMQ deve applicare un tempo aggiuntivo, per ogni verifica ed in qualsiasi fase, di almeno 1 g/u

per Linea Guida ulteriore integrata.

Salvo il buon esito della verifica di estensione, il certificato dell'Organizzazione, che in ogni caso rimane conforme unicamente alla ISO/IEC 27001, deve riportare, in aggiunta al proprio scopo secondo la Dichiarazione di Applicabilità (cfr. § 2), anche la successiva dicitura "…*integrata dai controlli previsti dalle linee guida ISO/IEC 27017 e ISO/IEC 27018*".

9. Data Center in Outsourcing

Se i Data Center utilizzati per le attività "cloud" sono in outsourcing presso fornitori in possesso di certificazioni ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018 accreditate e riconosciute a livello MLA, non è necessario tempo aggiuntivo di audit presso tali siti. In tutti gli altri casi, devono essere aggiunte tante mezze giornate quanti sono i siti in outsourcing da verificare con osservazione diretta. Nel caso di siti ove non fosse possibile svolgere un audit diretto (es. fornitori come AWS, AZURE), deve essere utilizzata presso il sito centrale una mezza giornata aggiuntiva per la valutazione degli aspetti contrattuali e di controllo operativo con tali fornitori. Questo ultimo requisito è applicabile solamente nel caso di Data Center in possesso di certificazioni TIER III o TIER IV.

10. Audit di sorveglianza e rinnovo

Le verifiche mantenimento e rinnovo sono previste come indicato nel paragrafo 10.5 delle Condizioni Generali di Contratto. In aggiunta a quanto già indicato dal documento sopra citato si specifica che tali audit saranno condotti sempre su tutte le linee guida applicabili assieme alla ISO/IEC 27001, prevedendo, per ogni linea guida, almeno 1 g/u aggiuntivo di verifica (cfr. § 8).

11. 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.