Certiquality Srl
Via G. Giardino, 4
20123 Milano - IT
Ph. +39 02 8069171
certiquality.it

C.F. e P.I. 04591610961
R.I. MI 04591610961
R.E.A. MI 1759338
Cap. Soc. € 1.000.000 i.v.
info@certiquality.it

REGOLAMENTO PER LA CONCESSIONE E IL MANTENIMENTO DELLA CERTIFICAZIONE DEI SISTEMI DI GESTIONE (REG 01)

ALLEGATO 3 – PRESCRIZIONI INTEGRATIVE PER LA CONCESSIONE E IL MANTENIMENTO DELLA CERTIFICAZIONE DEL SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI (ISMS – INFORMATION SECURITY MANAGEMENT SYSTEMS) SECONDO LA NORMA UNI CEI EN ISO/IEC 27001:2017.

Il Marchio CQY-Certiquality è un marchio depositato in Italia ed Europa in conformità alla vigente legislazione in materia di marchi di certificazione.
Il presente documento integra per gli specifici punti indicati, il Regolamento per la concessione e il mantenimento della certificazione (REG 01).
In caso di disposizioni non omogenee prevale il presente regolamento e in caso di ulteriori dubbi si fa riferimento allo Standard di riferimento UNI CEI EN ISO/IEC 27001:2017.

2. SCOPO E CAMPO DI APPLICAZIONE

Nel presente Regolamento vengono definiti i rapporti tra CERTIQUALITY SRL - nel testo denominato Istituto - e le Organizzazioni che intendono ottenere e far registrare la Certificazione del proprio Sistema di Gestione della Sicurezza delle Informazioni in conformità allo Standard di riferimento ISO/IEC 27001.
Sull'applicazione del presente Regolamento sorveglia il Comitato per la Salvaguardia dell'Imparzialità, nominato dal Consiglio di Amministrazione dell'Istituto, nel quale sono rappresentate le parti interessate alla certificazione.

Il Certificato CERTIQUALITY è il documento con il quale l'Istituto attesta che l'Organizzazione richiedente opera con un Sistema di Gestione conforme alla norma di riferimento.

La certificazione può essere rilasciata sul sistema informativo aziendale nella sua interezza o in specifiche aree ed applicazioni di particolare criticità.
Il certificato riporta sempre la versione applicabile dello Statement of Applicability.

3. DEFINIZIONI

Per la terminologia specifica riguardante i sistemi di gestione della sicurezza delle informazioni valgono in generale le definizioni riportate nello Standard di riferimento UNI CEI EN ISO/IEC 27001:2017 e alla norma ISO/IEC 27006:2015.

4. CONDIZIONI GENERALI

4.2 Perché venga attivato l'iter certificativo da parte dell'Istituto, l'Organizzazione richiedente deve:

- documentare ed attuare un Sistema di Gestione in conformità allo Standard UNI CEI EN ISO/IEC 27001:2017 alle eventuali prescrizioni particolari stabilite per tipologie di processo/servizio;
- aver effettuato almeno un Riesame della Direzione e un audit interno sul ISMS che copra lo scopo di certificazione,
- accettare le regole fissate dal presente Regolamento e le condizioni comunicate dall'Istituto.

4.4 La Certificazione riguarda esclusivamente la conformità dei Sistemi di Gestione rispetto allo

Standard ISO/IEC 27001; il rispetto delle disposizioni di legge vigenti è di esclusiva responsabilità dell'Organizzazione certificata.

5. PROCEDURA PER LA CERTIFICAZIONE DEL SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

5.1 Richiesta di offerta/Domanda di Certificazione e accettazione dell'offerta

L'Organizzazione che intende essere certificata deve richiedere un'offerta all'Istituto compilando il modulo di domanda in ogni sua parte ed inviarlo unitamente alla documentazione richiesta.

L'offerta dell'Istituto comprende l'esame della documentazione presentata con verifica di completezza ed adeguatezza delle informazioni generali e le verifiche in campo ed è in funzione delle caratteristiche e complessità del sistema informativo oggetto dell'ISMS (Information Security Management System).
L'accettazione dell'offerta perfeziona il rapporto contrattuale fra le parti e comporta anche l'accettazione delle prescrizioni previste dalla norma di riferimento e nel presente Regolamento, e successive modifiche, che è disponibile sul sito Internet: www.certiquality.it

5.2 Rilascio della Certificazione

5.2.1 A seguito dell'accettazione dell'offerta l'Istituto concorda con l'Organizzazione il periodo di effettuazione dell'audit. L'accettazione del contratto non presuppone né indirettamente né direttamente l'obbligo di rilascio della certificazione da parte di Certiquality.
Prima dell'audit l'Organizzazione deve comunicare all'Istituto o al valutatore incaricato della verifica, se ritiene che uno o più documenti del ISMS non possano essere resi disponibili per la verifica. L'Istituto valuta se è possibile condurre una verifica completa a fronte della norma di riferimento anche in assenza di tali documenti.
In tali casi lo scopo di certificazione potrà comprendere solamente i processi che sono stati sottoposti ad audit.
L'audit iniziale di certificazione è condotto in due fasi:

- stage 1, presso l'Organizzazione, finalizzato a comprendere la struttura del sistema ISMS, la valutazione dei rischi e i trattamenti (inclusi i controlli determinati) e del grado di preparazione dell'Organizzazione per l'effettuazione dello stage 2.
- stage 2, presso l'Organizzazione, finalizzato alla valutazione dell'applicazione e dell'efficacia del ISMS.

5.2.2 Prima dell'audit di Stage 1 l'Organizzazione deve:

- mettere a disposizione del valutatore dell'Istituto le informazioni generali relative al ISMS e al campo di applicazione, e la documentazione richiesta dal ISMS,
- indicare al valutatore eventuali esigenze che richiedano che la valutazione documentale venga effettuata in un luogo diverso dalla sede oggetto della certificazione.

5.2.4 Al termine dello Stage 1 il GVI definisce i tempi per l'effettuazione dello stage 2.
Tra stage 1 e stage 2 non possono passare più di tre mesi. Trascorso tale termine l'audit di Stage 1 deve essere ripetuto.
Certiquality valuta i casi eccezionali in cui sussistono le condizioni per mantenere validi i risultati dello Stage 1.
Nello stage 1 il GVI procede all'esame della documentazione del ISMS dell'Organizzazione che deve essere costituito dai seguenti documenti:

a) dichiarazioni documentate della politica e degli obiettivi del ISMS;
b) campo di applicazione del ISMS;

c) procedure e controlli a supporto del ISMS;
d) descrizione della metodologia della valutazione del rischio;
e) rapporto della valutazione del rischio;
f) piano di trattamento del rischio;
g) procedure documentate necessarie all'Organizzazione per assicurare l'efficace pianificazione, operatività e controllo dei propri processi di sicurezza delle informazioni e per descrivere come misurare l'efficacia dei controlli;
h) le registrazioni richieste dalla ISO/IEC 27001;
i) Statement of Applicability.

La verifica di valutazione di stage 2 ha lo scopo di:

- confermare che l'organizzazione opera secondo quanto ha stabilito nelle proprie procedure e obiettivi.
- Confermare che il ISMS è conforme ai requisiti della norma UNI CEI EN ISO/IEC 27001:2017.

Nello stage 2 l'Organizzazione deve dimostrare che il ISMS impostato sia rilevante ed adeguato rispetto alle attività dell'Organizzazione stessa e alle minacce, alle vulnerabilità e agli impatti individuati.

Nel corso dell'audit l'Organizzazione deve inoltre dimostrare di avere un sistema di gestione in grado di assicurare la conformità alle leggi e regolamenti applicabili alla sicurezza delle informazioni.

In casi eccezionali possono essere effettuati Stage 1 e Stage 2 consecutivamente. Al termine della prima parte della verifica l'ispettore, in base alle evidenze raccolte, conferma o meno la possibilità di proseguire l'audit con la seconda fase.

5.2.8 Aziende Multisito

Certiquality può applicare il sistema di campionamento dei siti nel caso in cui l'azienda soddisfi i seguenti requisiti:

- tutti i siti operino nell'ambito dello stesso ISMS, amministrato e verificato centralmente e che è soggetto a revisione della Direzione centrale;
- tutti i siti sono inclusi nel programma di audit interni del ISMS interno;
- tutti i siti sono inclusi nel programma di Riesame della Direzione.

Siti esterni - Siti temporanei

In presenza di attività svolte in maniera continuativa e con personale specifico presso siti "esterni" all'Organizzazione è necessario prevedere il tempo per la verifica on site a campione di tali "cantieri".
L'azienda deve inoltre dichiarare l'eventuale presenza di siti temporanei, intesi come siti non elencati nel certificato in cui però vengono svolte, per un periodo di tempo stabilito, le attività comprese nell'oggetto del certificato stesso.
La necessità di verificare questi siti e quindi di estendere il campionamento deve essere valutata e le motivazioni registrate nell'ambito del calcolo della durata del audit.
La valutazione comprende il rischio che una non conformità originata in un sito temporaneo, possa causare una carenza nel ISMS dell'azienda.

5.2.9 Estensione alle Linee Guida ISO/IEC 27017 ed ISO/IEC 27018

L'azienda certificata a fronte della norma ISO/IEC 27001 può richiedere l'estensione ad una o entrambe le Linee Guida:

- ISO/IEC 27017:2015 (Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services)
- ISO/IEC 27018: 2019 (Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.

La Norma ISO 27017:2015 può essere oggetto di estensione della certificazione anche da sola. Ove si intenda considerare tale estensione anche in ottica di Protezione Dati Personali, l'estensione alla Norma ISO/IEC 27017:2015 dovrà essere integrata con la Norma ISO/IEC 27018:2019.
Non è ammessa l'estensione alla sola Norma ISO/IEC 27018:2019.
Prima del rilascio della certificazione devono essere verificati tutti i data center presso cui sono dislocati i server che gestiscono il cloud.
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 si potrà evitare di incrementare il tempo di audit presso tali siti. In tutti gli altri casi, dovrà essere aggiunto tempo specifico per ciascun sito in outsourcing da verificare "de visu". Nel caso di siti ove non fosse possibile svolgere un audit diretto (es. fornitori come AWS, AZURE), verrà incrementato il tempo di audit presso il sito centrale per la valutazione degli aspetti contrattuali e di controllo operativo con tali fornitori. Questo ultimo requisito è applicabile solo nel caso di Data Center in possesso di certificazioni TIER III o TIER IV.

6. VALIDITÀ DELLA CERTIFICAZIONE DEI SISTEMI DI GESTIONE

La Certificazione rilasciata da CERTIQUALITY è subordinata a sorveglianza periodica almeno annuale e al riesame completo del Sistema di Gestione con periodicità triennale. Il certificato rilasciato riporta la data di scadenza triennale.

7. DIRITTI E DOVERI DELL'ORGANIZZAZIONE IN POSSESSO DI CERTIFICAZIONE

7.3 L'Organizzazione certificata è tenuta a comunicare a Certiquality ogni modifica apportata al documento "Statement of Applicability".