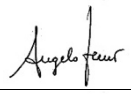
REGOLAMENTO DI CERTIFICAZIONE DEI SISTEMI DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

QM 86 03 00 Rev. 01,
Data 2022-05-31

CERTIFICATION
your sustainable revolution

CONTENUTI

Storia delle revisioni:				
N°	DATA	MOTIVI	EMESSO	APPROVATO
01	31.05.2022	Modifica immagine del logo		
00	30.07.2021	Prima emissione		

1. CAMPO DI APPLICAZIONE

Questo documento definisce le condizioni generali relativamente all'attività di certificazione di sistemi di gestione della Sicurezza delle Informazioni in conformità allo Standard di riferimento ISO/IEC 27001(ISMS).
Esso costituisce un'integrazione del Regolamento QI 86 01 00 "Regolamento di Certificazione dei Sistemi di Gestione" di **CERTIFICATION**, i cui requisiti continuano quindi ad essere totalmente applicabili per l'esecuzione dell'iter di certificazione ISMS.
Le disposizioni contenute all'interno del presente Regolamento, analogamente a quelle del QI 86 01 00, rivestono carattere contrattuale sia per **CERTIFICATION** che per l'Organizzazione richiedente la certificazione del proprio sistema di gestione per la prevenzione della corruzione (indicato anche come sistema di gestione anticorruzione, ISMS, implementato in conformità alla norma ISO/IEC 27001. Analogamente a quanto applicato a proposito dell'attività di certificazione degli altri sistemi di gestione, al fine di garantire la propria imparzialità e competenza **CERTIFICATION** sottopone il proprio operato ad un apposito Comitato, denominato Comitato per la Salvaguardia dell'Imparzialità, composto dai rappresentanti di tutte le parti interessate al processo di certificazione.
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.

2. 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, ISO/IEC 27006:2015, ISO/IEC 27006:2015 AMD 1:2020.

3. CERTIFICAZIONE INIZIALE

Le Organizzazioni che desiderino ottenere la certificazione del loro Sistema di Gestione della Sicurezza delle Informazione e/o l'estensione alle linee guida devono inviare a **CERTIFICATION** oltre al modulo Questionario Informativo, disponibile sul sito www.certificationsrl.it, compilato in tutte le sue parti.
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. Standard ISO/IEC 27001; il rispetto delle disposizioni di legge vigenti è di esclusiva responsabilità dell'Organizzazione certificata.
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.
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.
- Il Lead Auditor prima di decidere di procedere con lo stage 2, deve riesaminare il rapporto di audit dello stage 1 e confermare se i membri del gruppo di audit hanno la competenza necessaria per eseguire lo stage 2
- stage 2, presso l'Organizzazione, finalizzato alla valutazione dell'applicazione e dell'efficacia del ISMS.

Nello stage 1 si 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 il Lead Auditor, in base alle evidenze raccolte, conferma o meno la possibilità di proseguire l'audit con la seconda fase.

4. CERTIFICAZIONI MULTI-SITO

Si applica quanto già previsto nel Regolamento QI 86 01 00 di **CERTIFICATION**, con la precisazione che non possono essere esclusi dalla base del campionamento siti in base alla rilevanza del sito per il sistema di gestione e per i rischi individuati.

5. DURATA DEGLI AUDIT

Il calcolo della durata degli audit viene effettuata – come da disposizioni della norma ISO/IEC 17021-1, della norma ISO/IEC 27006:2015, ISO/IEC 27006:2015 AMD 1:2020.

6. 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.

7. VALIDITÀ DELLA CERTIFICAZIONE DEI SISTEMI DI GESTIONE

La Certificazione rilasciata da **CERTIFICATION** 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.

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

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