REGOLAMENTO PARTICOLARE PER LA CERTIFICAZIONE DI SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Indice Revisioni

2	2015-02-09	• **Revisione generale.** • **Annulla e sostituisce il Regolamento "Std-ce-aqsc-ISO_IEC27001" Rev. 1.**
3	2017-01-10	• **Revisione Generale** • **Aggiornamenti relativi alla ISO/IEC 27006:2015.**
4	2017-09-04	• **Revisione Generale e inserimento riferimenti alla Circolare N° 13/2017 ACCREDIA**
5	2018-02-26	• **Aggiornamento §4 e §5.9, inserimento §5.10 riferimento alla UNI CEI EN ISO/IEC 27001:2017**
6	2018-03-12	• **Aggiornato §5.10**

1 OGGETTO E CAMPO DI APPLICAZIONE

REGOLAMENTO PARTICOLARE PER LA CERTIFICAZIONE DI SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Il presente documento costituisce il Regolamento relativo allo "Schema per la certificazione di sistemi di gestione per la sicurezza delle informazioni" (ISMS, Information Security Management System) e quindi descrive le condizioni e le procedure applicate da DNV GL Business Assurance Italia S.r.l. (in seguito DNV GL) per la certificazione di ISMS in accordo alla norma ISO/IEC 27001, operati da organizzazioni che realizzano prodotti e/o erogano servizi.

Il presente documento definisce condizioni e procedure supplementari (e non sostitutive) rispetto a quanto già definito nel:

- "**Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale (MSC)**".

2 TERMINI E DEFINIZIONI

Scopo dell'ISMS:
l'ambito di riferimento in cui opera l'ISMS, ossia le caratteristiche di business (servizi, attività), l'assetto organizzativo (ruoli, responsabilità) i siti coinvolti, le risorse (assets), le tecnologie e i confini e le relazioni con processi e sistemi informatici esterni all'ISMS.

Scopo di certificazione:
il paragrafo riportato sul certificato che descrive le attività sottoposte a certificazione. In generale si tratta di un breve periodo.

Organizzazione:
in questo documento, si intende con questo termine l'Organizzazione oggetto dell'audit o *auditee*.

3 DOCUMENTI DI RIFERIMENTO

Le norme e i documenti di riferimento per la certificazione e registrazione dei Sistemi di Gestione per la Sicurezza delle Informazioni sono i seguenti:

ISO/IEC 27001:2013 *(UNI CEI EN ISO/IEC 27001:2017)*	"Information technology - Security techniques - Information security management systems - Requirements"
ISO/IEC 27002:2013 *(UNI CEI EN ISO/IEC 27002:2017)*	"Information technology - Security techniques - Code of practice for information security management systems"
ISO 19011:2011 (UNI EN ISO 19011:2012)	"Guidelines for auditing management systems"
ISO 9000:2015	"Quality management systems -- Fundamentals and vocabulary"

REGOLAMENTO PARTICOLARE PER LA CERTIFICAZIONE DI SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

ISO/IEC 27006:2015	"Information technology - Security techniques – Requirements for bodies providing audit and certification of information security management systems"
Circolare informativa N° 27/2017 ACCREDIA	*Comunicazione in merito all'adeguamento delle certificazioni per lo schema SSI (UNI CEI EN ISO/IEC 27001:2017)*
Circolare N° 02/2018 ACCREDIA	*Informativa in merito all'accreditamento per lo schema di certificazione ISO/IEC 27001:2013 con integrazione delle linee guida ISO/IEC 270XX:20YY "Information Technology, Security techniques, Code of practice"*

REGOLAMENTO PARTICOLARE PER LA CERTIFICAZIONE DI SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

4 NUOVA EDIZIONE DELLO STANDARD DI ACCREDITAMENTO ISO/IEC 27006:2015

In relazione alla nuova edizione delle standard di accreditamento la ISO/IEC 27006:2015, ***tutte le offerte per nuove certificazioni (DI+IA) e i rinnovi (RC) devono fare riferimento alle nuove regole contenute nell'"ANNEX B (normative) AUDIT TIME" dello standard.***

5 REGOLE PARTICOLARI – CERTIFICAZIONE IN ACCORDO ALLE NORME DI RIFERIMENTO

L'Organizzazione deve avere un Sistema di Gestione in accordo ai requisiti della normativa di riferimento per la certificazione ISO/IEC 27001.

5.1 Referente per DNV GL

Lo standard di riferimento per la certificazione degli ISMS non richiede la nomina di un rappresentante della Direzione. Ciononostante, l'Organizzazione deve indicare la persona al suo interno come referente per DNV GL e con la necessaria autorità per garantire l'esecuzione dell'audit. In particolare, deve garantire l'accesso alla documentazione, a tutte le aree comprese nello scopo dell'ISMS, alle registrazioni che danno garanzia della corretta applicazione dell'ISMS, al personale compreso nello scopo dell'ISMS.

5.2 Audit

I paragrafi che seguono specificano i requisiti aggiuntivi rispetto a quanto già indicato dal "**Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale (MSC)**".

5.2.1 Audit della documentazione di sistema (**Stage 1**)

Viene verificato che l'Organizzazione abbia sviluppato una documentazione di sistema conforme ai requisiti della norma di riferimento.

Relativamente a quanto già indicato dal "Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale (MSC)", si segnala che lo standard di riferimento fa riferimento a una serie di informazioni documentate che devono essere rese disponibili, tra le quali segnaliamo:

- Scopo dell'ISMS;
- Politica dell'ISMS;
- Descrizione dei processi di valutazione e trattamento del rischio relativo alla sicurezza delle informazioni;
- Statement of Applicability (SOA);

REGOLAMENTO PARTICOLARE PER LA CERTIFICAZIONE DI SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Nel corso della valutazione della documentazione verrà definito lo "Scopo di certificazione" (paragrafo 5.4), che potrà essere modificato anche negli audit successivi.

Altre considerazioni in merito alla documentazione sono riportate nel paragrafo 5.3.

Al termine della valutazione della documentazione, che DNV GL svolge presso l'Organizzazione, il Lead Auditor illustra le eventuali anomalie riscontrate rispetto ai requisiti dello standard.

5.2.2 Audit preliminare (**Stage 1**)

Questa attività è svolta in accordo a quanto già indicato dal "Regolamento per la Certificazione di Sistemi di Gestione Aziendale". Viene anche indicata come "Stage 1".

Viene valutata la capacità del Sistema di Gestione di fornire una giustificata fiducia a mantenersi conforme ai requisiti relativi alla sicurezza delle informazioni e stabiliti dall'organizzazione. Tra questi requisiti devono essere inclusi quelli legislativi e normativi applicabili e gli accordi con i clienti eventualmente sottoscritti dall'Organizzazione.

A tal scopo, nel corso dell'audit preliminare sono analizzate le caratteristiche dei siti, dei processi, delle attività e dei servizi, dei sistemi e delle reti informatiche incluse nello scopo dell'ISMS al fine di valutare l'adeguatezza, la completezza e l'affidabilità del processo e dei report di valutazione e trattamento del rischio, incluso il piano di trattamento del rischio e la dichiarazione di applicabilità (SOA, Statement of Applicability) con le politiche e gli obiettivi dell'Organizzazione relativi alla sicurezza delle informazioni.

Ci si assicura inoltre che tutte le interfacce con i servizi o le attività che non sono incluse completamente all'interno dello scopo dell'ISMS siano correttamente affrontate dai processi di valutazione e trattamento del rischio.

L'Organizzazione deve altresì dimostrare di avere attivi i controlli di sicurezza richiesti a livello legislativo, regolamentare e contrattuale.

In questa fase, è esaminato il processo di gestione degli incidenti e il processo di gestione della continuità operativa per quanto pertinente lo scopo dell'ISMS.

Al termine della valutazione preliminare, che DNV GL svolge presso l'Organizzazione, il Lead Auditor illustra gli eventuali rilievi (Non Conformità, Osservazioni, Opportunità di Miglioramento) riscontrati, stabilisce se l'Organizzazione è pronta per l'Audit Iniziale e, in tal caso, prepara un piano per tale audit.

Nota: E' possibile condurre congiuntamente l'audit della documentazione e l'audit preliminare (dipende dal grado di maturità del sistema, dichiarato dal cliente).

5.2.3 Audit Iniziale (**Stage 2**)

REGOLAMENTO PARTICOLARE PER LA CERTIFICAZIONE DI SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Oltre a quanto già indicato dal "Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale (MSC)", nel corso di questa fase, anche indicata come "**Stage 2**", sarà verificata l'applicazione dei controlli di sicurezza presso i vari processi che fanno parte dello scopo dell'ISMS.

Inoltre, ci si assicura che tutte le interfacce con i servizi o le attività che non sono incluse completamente all'interno dello scopo dell'ISMS siano correttamente presidiate con opportuni controlli di sicurezza delle informazioni.

5.2.4 Audit periodici

Le regole che governano la frequenza delle verifiche periodiche sono le stesse specificate dal "Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale (MSC)".

5.3 Documentazione

Tra la documentazione dell'ISMS, l'Organizzazione deve garantire che la politica per la sicurezza delle informazioni, lo scopo dell'ISMS e lo Statement of Applicability siano gestiti in forma controllata e i riferimenti a titolo, numero di revisione e data saranno inclusi nel rapporto di verifica.

La versione dello Statement of Applicability sarà poi riportata sul certificato di conformità.

5.3.1 Scopo dell'ISMS

Lo Scopo dell'ISMS (distinto dallo "Scopo di certificazione" trattato nel successivo 5.4) deve essere descritto in modo da dare all'auditor tutti gli elementi per comprendere i processi e i controlli di sicurezza da valutare. In particolare, deve dare piena evidenza di cosa sia incluso ed escluso dall'ISMS relativamente a:

- personale e struttura organizzativa;
- attività;
- dati e informazioni;
- infrastrutture;
- siti;
- sistemi informatici;
- reti informatiche.

Vanno anche evidenziate le loro interrelazioni e interfacce con elementi non compresi nello scopo dell'ISMS. Tra questi, vanno anche segnalati elementi che utilizzano i medesimi siti e infrastruttura informatica.

REGOLAMENTO PARTICOLARE PER LA CERTIFICAZIONE DI SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

L'Organizzazione non può escludere dallo scopo dell'ISMS processi che trattano informazioni o dati per i quali il certificato rilasciato da DNV GL può essere interpretato come garanzia verso terze parti di una presa in carico della gestione della loro sicurezza (a titolo di esempio, non può essere escluso il processo di amministrazione contabile se questo ha accesso a dati dei clienti per i quali il certificato può essere interpretato come garanzia di una presa in carico della gestione della loro sicurezza).

Questo documento deve risultare sempre aggiornato alla situazione in essere al momento dell'audit. Modifiche significative allo scopo dell'ISMS devono essere riportate il più prontamente possibile in questo documento e comunicate a DNV GL.

5.3.2 Processo di valutazione del rischio

L'Organizzazione deve aver stabilito un processo di valutazione del rischio che:

- Sia sistematico;
- Consideri tutti i rischi, al corretto livello di dettaglio, relativi alla sicurezza delle informazioni incluse nello scopo dell'ISMS;
- Consenta di analizzare le correlazioni tra i controlli applicati e i rischi per il cui trattamento sono stati scelti;
- Garantisca risultati comparabili e riproducibili;
- Garantisca il mantenimento nel tempo dei suoi risultati.

5.3.3 Conformità legislativa

DNV GL verifica che l'Organizzazione abbia stabilito e mantenga un efficace processo per identificare ed avere accesso ai requisiti normativi relativi alla sicurezza delle informazioni e pertinenti allo scopo dell'ISMS, tra cui quelli legati al trattamento dei dati personali e a quelli specifici del settore in cui opera l'Organizzazione (a puro titolo di esempio: bancario, assicurativo, telecomunicazioni, eccetera).

Si rammenta che un audit di certificazione di sistema di gestione non è un audit di conformità legale.

5.4 Scopo di certificazione

In questo paragrafo, si intende con "scopo di certificazione" il paragrafo riportato sul certificato che descrive le attività sottoposte a certificazione.

Lo scopo di certificazione deve indicare le tipologie di processi (attività svolte) e i servizi offerti dall'Organizzazione a cui si riferiscono le informazioni oggetto dell'ISMS.

La descrizione dei servizi deve essere non ambigua e, nel caso si scelga di utilizzare dei termini specifici del settore informatico, questi devono essere riconosciuti al di là del segmento di mercato in cui opera l'Organizzazione (per esempio, tra i termini accettabili si segnalano: housing, hosting, facility

management). Si raccomanda, in alternativa, di utilizzare la terminologia proposta da organismi quali AgID (Agenzia per l'Italia Digitale).

5.5 Outsourcing

Ove l'Organizzazione abbia deciso di allocare dei processi che impattano sulla sicurezza delle informazioni all'esterno della stessa Organizzazione, le attività di Audit potranno essere estese presso tali outsoucer, al fine di verificare l'efficacia dell'ISMS anche presso tali Organizzazioni.

Gli audit presso fornitori dell'Organizzazione possono avvenire nell'ambito dell'Audit Iniziale e/o degli audit periodici di mantenimento.

La scelta di condurre tali audit dipenderanno dall'influenza dell'outsourcer sul Sistema Gestione per la Sicurezza delle Informazioni, la cui rilevanza sarà dettata dall'analisi e valutazione del rischio e dalle valutazioni del Lead Auditor.

La titolarità dell'efficacia del Sistema di Gestione delle Informazioni rimarrà dell'Organizzazione. La mancata disponibilità da parte di tali fornitori a essere sottoposti ad audit, farà decadere la possibilità di certificare la medesima Organizzazione.

5.6 Elenco dei reclami e incidenti

L'Organizzazione deve tenere aggiornato e rendere disponibile un elenco dei "reclami" e degli "incidenti" collegabili alla sicurezza delle informazioni incluse nello scopo dell'ISMS (tra i quali vanno anche considerate le comunicazioni tra l'Organizzazione e gli interessati del trattamento di eventuali dati personali inclusi nello scopo dell'ISMS).

5.7 Multisito

L'approccio multisito viene considerato possibile, ove le Organizzazioni che lo richiedono operino, nei diversi siti, con processi assimilabili (ad esempio gruppi di cliniche mediche o di laboratori di analisi, compagnie alberghiere o agenzie di viaggio o compagnie telefoniche o banche etc).

Il campionamento dovrà prevedere sempre la valutazione dell'efficacia dei controlli di sicurezza e delle responsabilità della Direzione, più un campione di siti, che consenta, in un periodo ragionevole e comunque prima del rinnovo della certificazione, la copertura di tutta la Organizzazione.

Le non-conformità (di cui al paragrafo 5.8), comunque classificate, rilevate nei vari siti, dovranno essere oggetto di un processo di miglioramento applicato a tutti i siti dell'Organizzazione.

L' eventuale persistenza di una Non Conformità maggiore, comporta il ritiro della certificazione a tutta l'Organizzazione e non solamente al singolo sito.

5.7.1 Organizzazioni di servizi (che erogano servizi)

Nei casi in cui l'Organizzazione dovesse erogare servizi che hanno impatti sull'ISMS anche in luoghi diversi dalle proprie sedi (per esempio, presso clienti), il documento di Scopo dell'ISMS deve indicare tale situazione, così come i report di valutazione e trattamento del rischio.

La scelta di condurre una verifica presso tali luoghi dipenderà dalla loro influenza sull'ISMS, la cui rilevanza sarà dettata dall'analisi e valutazione del rischio e dalle valutazioni del Lead Auditor.

5.7.2 Siti condivisi

Nel caso in cui l'Organizzazione condivida il proprio sito e la gestione delle infrastrutture con altre entità, essa:

- Deve avere identificato nel documento di Scopo dell'ISMS tale situazione e considerarla nell'ambito della valutazione e del trattamento del rischio;
- Deve aver identificato le proprie interfacce per la gestione del sito e delle infrastrutture con le altre identità;
- Deve dimostrare di esercitare un adeguato livello di controllo, sul sito e sulle infrastrutture, anche in ottica di miglioramento.

5.8 Classificazione delle non-conformità

In aggiunta a quanto già indicato dal "**Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale (MSC)**" valgono le seguenti definizioni.

5.8.1 NC di categoria 1 (**Maggiore**)

- Il mancato rispetto degli obblighi di legge (es. normativa Privacy, *Regolamento Europeo GDPR*, sul Diritto di autore o di settore);
- Il mancato rispetto di requisiti contrattuali eventualmente concordati con partner o clienti relativamente alla sicurezza delle informazioni e per i quali il certificato può essere interpretato come garanzia della loro presa in carico;
- La palese evidenza di un immediato rischio per le informazioni incluse nello scopo dell'ISMS o un'anomalia nei controlli o nelle procedure che possono causare un significativo rischio per la sicurezza delle informazioni;
- Nessuna evidenza oggettiva disponibile in relazione alla gestione degli incidenti o la mancanza di una pianificazione e attuazione di controlli di continuità operativa;
- La non esecuzione di riesami di Direzione dell'ISMS nei 12 mesi precedenti alla verifica;

- La non esecuzione di un ciclo completo di audit interni precedenti l'audit iniziale e di rinnovo del certificato svolti nel triennio precedente secondo un programma di audit coerente con i requisiti della norma di riferimento;
- *Il mancato svolgimento di attività di Vulnerability Assessment (VA) e Penetration Test (PT);*
- La mancata preventiva comunicazione delle modifiche "sostanziali", che impattano sulla sicurezza, al DNV GL per le necessarie valutazioni.

5.8.2 NC di categoria 2 (**Minore**)

- Un'anomalia isolata nei controlli o nelle procedure che non rappresenta un potenziale e significativo rischio per la sicurezza delle informazioni;
- Un'anomalia minore singola e isolata o l'insieme di alcune anomalie minori tale da non pregiudicare l'efficacia del sistema, di carattere formale (documentale) o operativa (applicativa).

5.8.3 Osservazioni

- Un'anomalia di una condizione esistente che, a giudizio del valutatore, richiede chiarimenti, indagini o migliore rispetto all'efficienza complessiva dell'ISMS;
- Un rilievo che non influenza significativamente la sicurezza delle informazioni comprese nello scopo dell'ISMS in questo momento ma che, a giudizio del valutatore, rappresenta una potenziale inadeguatezza del sistema.

5.9 Linee Guida ISO/IEC 270XX

*Premesso che le Linee Guida **NON** sono mai Certificabili, sono state sviluppate nel corso degli anni alcune linee guida che possono essere incluse come parte del campo applicativo della ISO/IEC 27001.*

- *ISO/IEC 27011 "Information Technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for telecommunication organizations"*
- *ISO/IEC 27017 "Information Technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services"*
- *ISO/IEC 27018 "Information Technology – Security techniques – Code of practice protection of personally identifiable information (PII) in public clouds acting as PII processors"*
- *ISO/IEC 27032 "Information Technology – Security techniques – Guidelines for cybersecurity"*

REGOLAMENTO PARTICOLARE PER LA CERTIFICAZIONE DI SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

- *ISO/IEC 27034 "Information Technology – Security techniques – Application security*
- *ISO 27799 "Information security management in health using ISO/IEC 27002"*

Come previsto dalla circolare ACCREDIA n. 02/2018 per le Linee Guida ISO/IEC 270XX:20YY.

E' quindi possibile "integrare" una certificazione ISO/IEC 27001:2013 esistente, andando ad aggiornare il campo applicativo con una frase, Esempio: "....mediante l'applicazione della Linea Guida ISO/IEC 270XX:20YY e in accordo con lo Statement of Applicability versione x.x", "…. using the guidance in ISO/IEC 270XX:20YY and in accordance with the Statement of Applicability version x.x".

Prima del rilascio della certificazione devono essere verificati tutti i datacenter presso cui sono dislocati i server che gestiscono il cloud.

Il certificato deve fare sempre riferimento alla Norma ISO/IEC 27001 citando l'utilizzo della linea guida ISO/IEC 270XX nella sua applicazione.

Devono essere indicati i prodotti / servizi / applicazioni / processi coperti dalla certificazione.

5.10 UNI CEI EN ISO/IEC 27001:2017

Come da Circolare informativa N° 27/2017 di ACCREDIA:

"Vi informiamo che a seguito dell'entrata in vigore della norma UNI CEI EN ISO/IEC 27001:2017, entro fine anno i vostri certificati di accreditamento saranno aggiornati con il riferimento a tale nuova edizione della norma nazionale, che sostituisce la UNI CEI ISO/IEC 27001:2014.

L'edizione 2017 è stata emessa in conseguenza della pubblicazione della norma europea EN ISO/IEC 27001:2017, che a sua volta recepisce la ISO/IEC 27001:2013 incorporando due Corrigendum (emessi dall'ISO nel 2014 e 2015).

Il primo corrigendum riguarda il requisito A.8.1.1: l'inventario, la classificazione e trattamento degli "asset" riguarda ora anche le "informazioni" cui gli asset sono associati.
Il secondo corrigendum riguarda il requisito 6.1.3: la Dichiarazione di Applicabilità deve specificare se sono implementati o meno i "controlli necessari", e non solo i controlli riferiti all'Annex A.

***Non essendo stati introdotti nuovi requisiti, la norma ISO/IEC resta in edizione 2013**, per cui l'unico impatto sui certificati emessi si potrà avere sul riferimento normativo nazionale in essi riportato."*

Nel nostro caso, tutti i certificati saranno emessi con il solo riferimento alla normativa internazionale **ISO/IEC 27001:2013** senza alcun riferimento alla norma locale UNI CEI EN ISO/IEC 27001:2017.

REGOLAMENTO PARTICOLARE PER LA CERTIFICAZIONE DI SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

5.11 Registri delle organizzazioni certificate

I registri cui il DNV GL comunica lo stato dei certificati relativi ai Sistemi di Gestione per la Sicurezza delle Informazioni e ai quali l'Organizzazione può autorizzare o non autorizzare la pubblicazione dei propri dati sono i seguenti:

- DNV GL (http://www.dnvgl.it)
- Accredia (http://www.accredia.it)

5.12 Uso del marchio

L'Organizzazione, una volta certificata, ha il diritto di utilizzare il marchio e il certificato in accordo ai requisiti definiti nei Manuali di utilizzo di DNV GL e dell'ente di accreditamento (Accredia, RVA, UKAS), scaricabili dal sito www.dnvgl.it.