

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



1	OGGETTO E CAMPO DI APPLICAZIONE	1
2	TERMINI E DEFINIZIONI.....	1
3	DOCUMENTI DI RIFERIMENTO.....	1
4	REGOLE PARTICOLARI – CERTIFICAZIONE IN ACCORDO ALLE NORME DI RIFERIMENTO.....	1

1 OGGETTO E CAMPO DI APPLICAZIONE

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 Italia per la certificazione di ISMS in accordo alle norme UNI EN ISO serie 27000, 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 per la Certificazione di Sistemi di Gestione Aziendale".

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 27001:2005 (UNI EN ISO/IEC 27001:2006)	"Information technology - Security techniques - Information security management systems - Requirements"
ISO/IEC 27002:2005	"Information technology - Security techniques - Code of practice for information security management systems"
ISO/IEC 27005:2005	"Information technology - Security techniques - Information security management risk management"
UNI EN ISO 19011:2003	"Linee guida per gli audit dei sistemi di gestione per la qualità e/o di gestione ambientale"
UNI EN ISO 9000:2005	"Sistemi di gestione per la qualità - Fondamenti e Vocabolario"
ISO/IEC 27006:2005	"Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems"

4 REGOLE PARTICOLARI – CERTIFICAZIONE IN ACCORDO ALLE NORME DI RIFERIMENTO

Reviewed by: SIC	Valid for: All in DNV Italy	Revision: 1	No.: Std-ce-aqsc-ISO_IEC27001.doc
Approved by: PRIV	Author: FVF	Date: 2009-05-29	Page: 1 of 6

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



L'Organizzazione deve avere un Sistema di Gestione in accordo ai requisiti della normativa di riferimento per la certificazione ISO/IEC 27001:2005.

4.1 Referente per DNV Italia

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 che ricopre il ruolo di referente per DNV Italia e che abbia 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.

4.2 Verifiche

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

4.2.1 Verifica 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 per la Certificazione di Sistemi di Gestione Aziendale", si segnala che lo standard di riferimento non indica, tra la documentazione obbligatoria, un "Manuale". Al suo posto, si fa riferimento ad un insieme di documenti:

- Scopo dell'ISMS
- Politica dell'ISMS
- Procedura di descrizione della metodologia di Risk Assessment
- Statement of Applicability

Nel corso della valutazione della documentazione verrà definito lo "Scopo di certificazione" (paragrafo 4.4), che potrà essere modificato e revisionato anche nelle successive verifiche.

Altre considerazioni in merito alla documentazione sono riportate nel paragrafo 4.3.

Al termine della valutazione della documentazione che DNV svolge presso l'Organizzazione, il Lead Auditor illustra le eventuali Non Conformità riscontrate alle specifiche richieste dello standard.

4.2.2 Visita 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 della Verifica Ispettiva Iniziale".

Viene valutata la capacità del Sistema di Gestione di fornire una giustificata confidenza a mantenersi conforme ai requisiti legislativi ed a prescrizioni eventualmente sottoscritte dall'Organizzazione relative alla sicurezza delle informazioni (regolamenti, contratti, ...) e coerenti con il campo di applicazione della certificazione.

A tal scopo, nel corso della visita 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 della metodologia e dei report di analisi e valutazione del rischio, nonché della coerenza del Piano di Trattamento del Rischio e dello Statement of Applicability con le politiche e gli obiettivi dell'Organizzazione.

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

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

Reviewed by: SIC	Valid for: All in DNV Italy	Revision: 1	No.: Std-ce-aqsc-ISO_IEC27001.doc
Approved by: PRIV	Author: FVF	Date: 2009-05-29	Page: 2 of 6

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



Al termine della valutazione preliminare, che DNV 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 la Verifica Ispettiva Iniziale e, in tal caso, prepara un piano per tale verifica.

Nota: E' possibile condurre congiuntamente la Verifica della documentazione e la Verifica Preliminare (dipende dal grado di maturità del sistema, dichiarato dal cliente).

4.2.3 Verifica Ispettiva Iniziale (Stage 2)

Oltre a quanto già indicato dal "Regolamento per la Certificazione di Sistemi di Gestione Aziendale", nel corso di questa fase 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 indirizzate e incluse nell'Analisi dei Rischi.

Viene anche indicata come "Stage 2".

4.2.4 Verifiche periodiche

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

4.3 Documentazione

Tra la documentazione dell'ISMS, l'Organizzazione deve garantire che lo scopo dell'ISMS, il Piano di trattamento del rischio 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. Non si esclude che il contenuto di tali documenti possa essere incluso in altri (come, per esempio, il "Manuale" dell'ISMS, il Riesame della Direzione, eccetera) e in tal caso saranno riportati sul rapporto di verifica gli opportuni riferimenti.

4.3.1 Scopo dell'ISMS

Lo Scopo dell'ISMS (distinto dallo "Scopo di certificazione" trattato nel successivo 4.4) 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 quali siano gli asset coinvolti dall'ISMS, tra cui:

- personale e struttura organizzativa,
- dati e informazioni
- infrastrutture
- siti
- sistemi informatici
- reti informatiche

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

Tali interrelazioni e interfacce devono essere considerate dal processo di analisi e valutazione del rischio.

L'Organizzazione non può escludere dallo scopo dell'ISMS processi che trattano informazioni o dati per i quali il certificato rilasciato da DNV Italia 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 Italia.

Lo "Scopo dell'ISMS" può essere riportato su un documento specifico, o essere parte di un altro documento (es. "Manuale dell'ISMS", Statement of Applicability, eccetera) o composto da più documenti (per esempio: grafici, ordini di servizio,

Reviewed by: SIC	Valid for: All in DNV Italy	Revision: 1	No.: Std-ce-aqsc-ISO_IEC27001.doc
Approved by: PRIV	Author: FVF	Date: 2009-05-29	Page: 3 of 6

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



mappe di processo, eccetera) che devono essere in forma controllata ed essere riferiti dal sistema documentale come elementi dello "Scopo dell'ISMS".

4.3.2 Metodologia per l'analisi e valutazione del rischio

L'Organizzazione deve aver sviluppato una metodologia per l'analisi e valutazione del rischio che

- sia sistematica,
- consideri tutte le minacce e vulnerabilità relative agli asset inclusi nello scopo dell'ISMS,
- consenta di analizzare le correlazioni tra i controlli applicati e le minacce e vulnerabilità per il cui trattamento sono stati scelti,
- garantisca risultati comparabili e riproducibili,
- sia mantenuta nel tempo.

4.3.3 Conformità legislativa

DNV Italia verifica che l'Organizzazione abbia stabilito e mantenga un'efficace procedura per identificare ed avere accesso ai requisiti di legge relativi alla sicurezza delle informazioni 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)

4.4 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) ed 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 il CNIPA (già AIPA) in documenti quali il numero **Error! Reference source not found.** riportato al paragrafo 3).

4.5 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.

Le verifiche ispettive presso fornitori dell'Organizzazione possono avvenire nell'ambito della Verifica Ispettiva Iniziale e/o delle Verifiche periodiche di mantenimento.

La scelta di condurre tali verifiche dipenderà dall'influenza dell'outsoucer 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 ad essere sottoposti ad Audit, farà decadere la possibilità di certificare la medesima Organizzazione.

4.6 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).

Reviewed by: SIC	Valid for: All in DNV Italy	Revision: 1	No.: Std-ce-aqsc-ISO_IEC27001.doc
Approved by: PRIV	Author: FVF	Date: 2009-05-29	Page: 4 of 6

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



4.7 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 il monitoraggio 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 4.8), 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.

4.7.1 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 Analisi e Valutazione 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.

4.7.2 Siti condivisi

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

- deve avere identificato nel documento di Scopo dell'ISMS tale situazione e considerarla nell'ambito dell'Analisi e Valutazione 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.

4.8 Classificazione delle non-conformità

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

4.8.1 NC di categoria 1 (Maggiore)

- Il mancato rispetto degli obblighi di legge (es. normativa Privacy, 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 un Business Continuity Plan.
- La non esecuzione di Riesami della Direzione dell'ISMS nei 12-15 mesi precedenti alla verifica.
- La non esecuzione di un ciclo completo di audit interni precedenti la verifica ispettiva iniziale e di rinnovo del certificato svolti nel triennio precedente secondo un programma di audit coerente con i requisiti della norma di riferimento.

Reviewed by: SIC	Valid for: All in DNV Italy	Revision: 1	No.: Std-ce-aqsc-ISO_IEC27001.doc
Approved by: PRIV	Author: FVF	Date: 2009-05-29	Page: 5 of 6

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



4.8.2 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) od operativa (applicativa).

4.8.3 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.

4.9 Registri delle organizzazioni certificate

Al termine di ogni verifica, il rapporto rilasciato dal Lead Auditor riporta anche le scelte dell'Organizzazione in merito alla pubblicazione dei dati del certificato (ragione sociale, siti certificati e scopo di certificazione) sui registri delle organizzazioni certificate (consultabili anche via web).

I registri a cui il DNV Italia 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:

- Det Norske Veritas Italia (<http://www.dnv.it>)
- Sincert (<http://www.sincert.it>)
- Xisec (<http://www.xisec.com>)

4.10 Uso del marchio

L'Organizzazione, una volta certificata, ha il diritto di utilizzare il marchio e il certificato in accordo ai requisiti definiti nel "Regolamento e manuale d'uso del marchio di certificazione di sistema del DNV Italia"

Reviewed by: SIC	Valid for: All in DNV Italy	Revision: 1	No.: Std-ce-aqsc-ISO_IEC27001.doc
Approved by: PRIV	Author: FVF	Date: 2009-05-29	Page: 6 of 6