Regolamento per la certificazione di Sistemi di Gestione della Security

In vigore dal 1° luglio 2009

RINA Società per azioni
Via Corsica, 12 - 16128 Genova - Italia
Tel. +39 01053851 - Fax: +39 0105351000
www.rina.org

Regolamenti tecnici

INDICE

CAPITOLO 1
GENERALITÀ'

1.1

Nel presente Regolamento sono definite le procedure applicate dal RINA per la certificazione di Sistemi di Gestione Security (SMS) e le modalità di richiesta, ottenimento, mantenimento ed utilizzazione, nonché l'eventuale sospensione e revoca di tale certificazione.

Per quanto non previsto dal presente documento, si richiamano le "CONDIZIONI GENERALI DI CONTRATTO PER LA CERTIFICAZIONE DI SISTEMI, PRODOTTI E PERSONALE", reperibili sul sito web www.rina.org.

1.2

Il RINA rilascia la certificazione ad Organizzazioni il cui Sistema di Gestione Security sia stato riconosciuto conforme a tutti i requisiti previsti dalla norma

ISO 28000:2007

Inoltre, su richiesta, il RINA può effettuare valutazioni di conformità del Sistema di Gestione Security in accordo con altri documenti normativi di riferimento.

1.3

L'accesso alla certificazione è aperto a tutte le Organizzazioni e non è condizionato dalla loro appartenenza o meno a qualsiasi Associazione o Gruppo.

Per l'attività certificativa il RINA applica le proprie tariffe vigenti, garantendone l'equità e l'uniformità di applicazione. Il RINA può legittimamente non accettare richieste di certificazione che riguardino Organizzazioni sottoposte, o la cui produzione o attività sia sottoposta, a misure restrittive, sospensive o interdittive da parte di una pubblica Autorità.

1.4

La certificazione rilasciata dal RINA è riferita esclusivamente alla singola Organizzazione, dove per Organizzazione si intende un gruppo, società, azienda, impresa, ente o istituzione, ovvero loro parti o combinazioni, in forma associata o meno, pubblica o privata, che abbia una propria struttura funzionale ed amministrativa.

Per Organizzazioni con più unità operative, una singola unità operativa può essere definita come Organizzazione.

1.5

Le procedure contemplate nel presente Regolamento si applicano anche quando la certificazione del Sistema di Gestione Security sia richiesta in applicazione dei Regolamenti per la classificazione del RINA o di altra normativa applicabile all'Organizzazione; in tali casi devono essere ottemperati anche gli eventuali requisiti addizionali sul Sistema di Gestione Security in essi contemplati.

1.6

La terminologia usata nel presente Regolamento è quella riportata nelle norme ISO 28000:2007 ed UNI CEI EN ISO/IEC 17000:2005.

1.7

RINA assicura che tutti i membri degli Audit Team coinvolti, lavoreranno secondo le politiche RINA relative alla tutela della riservatezza delle informazioni emerse in sede di audit. Le informazioni relative al cliente non saranno divulgate a terze parti senza il consenso scritto del cliente/persona interessata.

RINA garantisce una gestione sicura delle informazioni riservate (es. Documenti, registrazioni) e di controllare in modo adeguato l'identificazione, l'archiviazione, la protezione, i tempi di conservazione e la disposizione dei documenti relativi agli adempimenti previsti dalla norma ISO 28000:2007.

Gli auditor impiegati da RINA, saranno sottoposti ad una "background investigation" e dovranno dimostrare la loro "security clearance".

CAPITOLO 2
NORMA DI RIFERIMENTO / REQUISITI PER LA CERTIFICAZIONE

2.1

Per ottenere la certificazione da parte del RINA, un Sistema di Gestione della Security deve soddisfare inizialmente e nel tempo i requisiti della norma ISO 28000:2007.

Le organizzazioni dovranno costituire, documentare, implementare, mantenere e migliorare continuamente un effettivo sistema di gestione della security idoneo ad individuare le minacce alla security, valutandone i rischi, controllando e mitigandone le loro conseguenze. L'effettiva implementazione del sistema dovrà essere attuata secondo i requisiti individuati al § 4 della norma ISO 28000:2007.

2.2

In particolare, per ottenere la certificazione del Sistema di Gestione Security, l'Organizzazione deve:

2.2.1 Aver istituito, mantenuto attivo e completamente operativo un Sistema di Gestione della Security in totale ottemperanza ai requisiti della norma ISO 28000:2007. Il Sistema di gestione della Security si intende completamente operativo quando:

- è applicato da almeno tre mesi,
- il sistema di audit interni è completamente attuato ed è possibile dimostrarne l'efficacia,
- è stato svolto e documentato almeno un riesame del sistema da parte della Direzione,
- sono stati definiti gli obiettivi ed i processi necessari ad ottenere risultati in accordo con i requisiti del Cliente e con le politiche aziendali,
- sono stati sviluppati tali processi,
- sono stati effettuati e registrati monitoraggi e misure dei processi e dei prodotti rispetto alle politiche, agli obiettivi ed ai requisiti per il prodotto.

2.2.2 Disporre di un Manuale che:

- definisca lo scopo/campo di applicazione del Sistema di Gestione della Security, descriva i principali processi e le loro interazioni e contenga o richiami le relative procedure documentate.

  La descrizione dei processi e delle loro interazioni deve essere estesa a tutti quelli sviluppati dall'Organizzazione (anche a processi affidati all'esterno) necessari alla realizzazione di un determinato prodotto/servizio, determinanti ai fini della capacità del prodotto/servizio stesso di soddisfare i requisiti applicabili.

Tale descrizione può avvenire in vario modo:

- Descrizioni
- Diagrammi di flusso o logigrammi
- Tabelle o matrici
- Altro

- prenda in considerazione i requisiti della Norma e fornisca una descrizione, anche breve, delle risorse e dei procedimenti posti in atto per assicurare la conformità a tali requisiti,
- specifichi la gestione della politica della security,
- contenga una adeguata descrizione dell'Organizzazione aziendale.

2.2.3 Disporre di adeguate procedure:

- Per l'identificazione e la valutazione dei rischi della security e la gestione degli stessi,
- per l'identificazione e l'implementazione delle necessarie misure di gestione,
- per la gestione dell'addestramento degli adetti.

2.3

I requisiti di cui al punto 2.2 sono verificati dal RINA, attraverso un processo di audit iniziale composto da due stage:

Audit stage 1 - RINA generalmente effettua un audit sul sito.
Audit stage 2 - RINA effettua un audit sul sito.

Le peculiarità dell'audit iniziale sono dettagliate nel capitolo successivo.

CAPITOLO 3
CERTIFICAZIONE INIZIALE

3.1

Le Organizzazioni che desiderino ottenere la certificazione del loro Sistema di Gestione Security devono fornire al RINA i dati essenziali della loro Organizzazione e relative attività svolte e la localizzazione del Sito/i, inviando l'apposito modulo "Questionario Informativo" compilato in tutte le sue parti (disponibile sul sito web www.rina.org), sulla base dei quali viene formulata dal RINA un'offerta economica.

In particolare, l'Organizzazione deve comunicare al RINA:

- eventuali elementi della norma di riferimento che ritiene non siano applicabili alla sua Organizzazione o che necessitino di interpretazione o di adattamento, indicandone chiaramente i motivi;
- informazioni concernenti tutti i processi affidati all'esterno utilizzati dall'Organizzazione che influenzano la conformità ai requisiti;
- numero di siti permanenti e temporanei oggetto della certificazione e le relative attività svolte;

Tali informazioni sono richieste allo scopo di verificare preventivamente l'applicazione di alcuni requisiti della norma e di predisporre un'offerta economica adeguata.

Le Organizzazioni, in caso di accettazione dell'offerta economica, formalizzano la richiesta di certificazione inviando al RINA lo specifico modulo allegato all'offerta, indicando la norma di riferimento e, se del caso, altro documento normativo di riferimento, secondo il quale è richiesta la certificazione.

Al ricevimento della richiesta di certificazione e dei relativi allegati, e dopo loro esame preliminare per verificarne la completezza, il RINA invia all'Organizzazione per iscritto la conferma di accettazione della richiesta stessa.

La richiesta dell'Organizzazione, nella quale è espressamente richiamato il presente Regolamento e la relativa accettazione da parte del RINA formalizzano contrattualmente il rapporto tra il RINA e l'Organizzazione e l'applicabilità del presente Regolamento.

Il contratto stipulato tra il RINA e l'Organizzazione comprende:

- l'audit iniziale composto da due stage e il rilascio del certificato;
- i successivi audit di sorveglianza e di ricertificazione
- eventuali servizi aggiuntivi specificati nell'offerta.

Il RINA comunica all'Organizzazione i nomi dei tecnici qualificati incaricati dell'effettuazione dell'audit stage1 e l'audit stage2; l'Organizzazione può fare obiezione sulla nomina di tali tecnici, giustificandone i motivi.

Durante l'audit iniziale l'Organizzazione deve poter dimostrare che il Sistema di Gestione sia pienamente operante da almeno tre mesi e di applicare effettivamente il Sistema stesso e le relative procedure documentate.

3.2

Unitamente alla richiesta di certificazione, o successivamente alla stessa, l'Organizzazione dovrà rendere disponibile al RINA la seguente documentazione:

- manuale di gestione della security (ultima revisione valida);
- elenco delle procedure interne rilevanti ai fini della security;
- copia del certificato di iscrizione alla Camera di Commercio o documento equivalente, quale evidenza dell'esistenza dell'Organizzazione e dell'attività effettuata;
- organigramma del Sistema di Gestione dell'Organizzazione;
- pianta del Sito/Siti;
- ultimo Riesame della Direzione;
- pianificazione Audit Interni;
- elenco delle principali leggi e/o regolamenti applicabili al prodotto/servizio fornito;
- elenco dei cantieri in corso, con descrizione delle attività ivi espletate.

Il RINA può richiedere a sua discrezione, per esame, anche altri documenti, oltre quelli indicati in precedenza, giudicati importanti ai fini della valutazione del Sistema di Gestione Security.

La documentazione di cui sopra è valutata dal RINA per conformità alla norma di riferimento ed ai requisiti del presente Regolamento.

3.3

La finalità dell'audit di stage 1 è di:

- sottoporre ad audit la documentazione del Sistema di Gestione della Security del cliente;
- valutare la localizzazione e le condizioni particolari del sito del cliente e intraprendere uno scambio d'informazioni con il personale del cliente al fine di stabilire il grado di preparazione per l'audit stage 2;
- riesaminare lo stato e la comprensione del cliente riguardo i requisiti della norma, con particolare riferimento all'identificazione di prestazioni chiave o di aspetti, processi, obiettivi e funzionamento significativi del Sistema di Gestione della Security;
- raccogliere le informazioni necessarie riguardanti il campo di applicazione del Sistema di Gestione, i processi e la/e localizzazione/i del cliente, compresi i relativi aspetti legali e regolamentati e la conformità ad essi;
- riesaminare l'assegnazione di risorse per l'audit stage 2 e concordare con il cliente i dettagli dell'audit stage 2;
- mettere a fuoco la pianificazione dell'audit stage 2, acquisendo una sufficiente conoscenza del Sistema di Gestione della Security e delle attività nel sito del cliente, con riferimento ai possibili aspetti significativi;

- valutare se gli audit interni e il riesame da parte della direzione siano stati pianificati ed eseguiti e che il livello di attuazione del Sistema di Gestione della Security fornisca l'evidenza che il cliente è pronto per l'audit stage 2.

Al termine dell'audit stage 1 è consegnata all'Organizzazione copia del rapporto di audit stage1, sul quale sono tra l'altro riportate le eventuali osservazioni riscontrate incluse quelle che potrebbero essere classificate come non conformità durante l'audit di stage 2.

Le azioni intraprese dall'Organizzazione per la risoluzione di tali osservazioni sono, generalmente, verificate durante l'audit stage 2 di cui al punto 3.4.

In presenza di osservazioni ritenute particolarmente significative, a giudizio dei tecnici che hanno effettuato l'audit, può essere richiesta la loro completa risoluzione prima dell'audit stage2 presso l'Organizzazione.

Normalmente l'audit stage 1 sarà effettuato direttamente presso il sito/i dell'Organizzazione stessa.

3.4

L'audit stage 2 presso l'Organizzazione è effettuato, a buon esito dell'audit stage 1 "on-site" di cui al punto 3.3, al fine di verificare la corretta attuazione del Sistema di Gestione Security.

RINA invia all'Organizzazione, prima dell'effettuazione dell'audit stage 2 presso il sito/i, un piano di audit dove è riportata, in dettaglio, la descrizione delle attività e delle disposizioni per la conduzione dell'audit.

Qualora le attività da verificare siano svolte su più siti operativi, l'audit è svolto secondo criteri previamente stabiliti e comunicati dal RINA all'Organizzazione.

L'audit stage 2 è effettuato sulla base del rapporto di audit stage 1 e dei seguenti documenti predisposti dall'Organizzazione nella revisione aggiornata:

- manuale del Sistema di Gestione della Security,
- questionario informativo compilato dall'Organizzazione,
- elenco delle procedure interne della scurity,
- altri documenti del Sistema di Gestione della Security.

Essenzialmente l'audit stage 2 consiste in:

- una riunione iniziale con i tecnici dell'Organizzazione per concordare le finalità e le modalità dell'audit stesso a conferma di quanto previsto dal piano di audit;

- una verifica della messa in atto di efficaci azioni di adeguamento relativamente alle osservazioni emerse durante l'audit stage1;
- un sopralluogo del Sito/i dell'Organizzazione per verificare la conformità del Sistema di Gestione Security ai documenti di riferimento e la sua completa attuazione;
- una riunione finale per illustrare l'esito dell'indagine.

3.5

Al termine dell'audit stage 2 è consegnata all'Organizzazione copia del rapporto di audit, sul quale sono tra l'altro riportate le eventuali non conformità (rilievi di tipo "A"), osservazioni (rilievi di tipo "B") sull'applicazione del Sistema di Gestione della Security e raccomandazioni (rilievi di tipo "C") riscontrate.
L'Organizzazione può annotare sue eventuali riserve od osservazioni, in merito ai rilievi espressi dai tecnici del RINA, su un apposito spazio del rapporto di audit.
Il contenuto di tale rapporto è successivamente confermato dal RINA tramite una comunicazione scritta.
In assenza di comunicazione scritta da parte del RINA il rapporto si ritiene confermato dopo tre giorni lavorativi della sua consegna all'Organizzazione.

L'Organizzazione, dopo aver analizzato le cause delle eventuali non conformità segnalate sul rapporto di cui sopra, deve proporre al RINA, entro la data indicata sul rapporto stesso, i necessari trattamenti delle non conformità nonché le necessarie azioni correttive ed i tempi previsti per la loro attuazione.
È prevista la possibilità di usufruire della "Member Area" sul sito web RINA (www.rina.org) per l'invio delle proposte di trattamento e azione correttiva con successiva accettazione da parte del RINA.
L'Organizzazione, infatti, può proporre gli eventuali trattamenti e azioni correttive compilando gli appositi moduli direttamente nella "Member Area" sul sito web RINA (www.rina.org).[1]

L'accettazione di tali proposte e dei tempi previsti per l'attuazione è comunicata per iscritto dal RINA all'Organizzazione.

3.6

In presenza di non conformità[2] il processo di certificazione è sospeso; nel caso di altri rilievi, la cui numerosità, a giudizio del gruppo di audit sia tale da pregiudicare il

[1] In caso di impossibilità di accesso ad internet, l'Organizzazione potrà compilare copia cartacea della modulistica utilizzata ed inviarla all'Ufficio RINA di pertinenza.

[2] Si intendono non conformità:
- la totale assenza di considerazione di uno o più requisiti della norma di riferimento,
- il mancato rispetto di uno o più requisiti del presente Regolamento,
- una situazione tale da provocare una grave deficienza del sistema di gestione, o da ridurre la sua capacità ad assicurare il controllo degli aspetti/impatti sulla security e/o il rispetto della legislazione.

corretto funzionamento del Sistema, il processo di certificazione è ugualmente sospeso.
In tali casi, entro tre mesi, il RINA può effettuare un audit supplementare finalizzato ad accertare la corretta applicazione delle azioni correttive proposte; a buon esito di tale audit il processo di certificazione è ripreso.
L'audit supplementare può essere effettuato sul sito o su base documentale in base alla tipologia delle azioni correttive da verificare a giudizio del team di audit.

Qualora il suddetto termine sia superato, il Sistema di Gestione Security dell'Organizzazione deve essere sottoposto a completo riesame entro un termine di sei mesi dalla data del rilievo.

Trascorso il suddetto periodo di sei mesi senza conclusione positiva della valutazione, il RINA può considerare chiusa la pratica di certificazione, addebitando i tempi e le spese sostenute sino a quel momento. In tali casi l'Organizzazione che desidera proseguire con la certificazione del RINA deve presentare una nuova richiesta e ripetere l'iter certificativo.

I suddetti termini temporali possono in casi particolari essere variati su richiesta motivata dell'Organizzazione, a giudizio del RINA.

3.7

A completamento, con esito favorevole, degli accertamenti e previa convalida da parte dell'apposito Comitato del RINA, è rilasciato, per il Sistema di Gestione Security in esame, un Certificato di conformità (il cui fac simile è disponibile sul sito www.rina.org) con validità di tre anni.

La validità del certificato è subordinata al risultato dei successivi audit di sorveglianza annuali ed alla ricertificazione triennale del Sistema di Gestione Security.

La periodicità e l'estensione dei successivi audit per il mantenimento della certificazione sono stabiliti dal RINA caso per caso mediante l'elaborazione di un programma triennale di audit, che è inviato all'Organizzazione.
Per il dettaglio sulla gestione e validità dei certificati di conformità rilasciati da RINA si veda il successivo capitolo 6.

. situazioni che potrebbero causare serie carenze nel sistema di gestione della security o che riducano le la sua capacità di controllare gli aspetti/impatti dell'ambiente esetrno e/o gli adempimenti previsti dalla normativa cogente.

CAPITOLO 4
MANTENIMENTO DELLA CERTIFICAZIONE

4.1

L'Organizzazione deve mantenere la conformità del proprio Sistema di Gestione Security alla Norma di riferimento.

4.2

L'Organizzazione deve tenere registrazioni degli eventuali reclami e delle relative azioni correttive intraprese e deve renderle disponibili al RINA unitamente alle azioni correttive intraprese durante gli audit periodici.

4.3

Il RINA effettua audit periodici sul Sistema di Gestione Security al fine di valutare il mantenimento della conformità ai requisiti della Norma di riferimento.

Gli audit per il mantenimento della certificazione si dividono in due tipologie:

- audit di sorveglianza, con periodicità di regola almeno annuale.
  - Si effettua una valutazione parziale a campione sul Sistema di Gestione della Security.
- audit di ricertificazione (vedere capitolo 5);
  Il Sistema di Gestione della Security deve essere rivalutato nella sua interezza con periodicità triennale.

4.4

Gli audit di sorveglianza sono condotti presso il sito/i dell'Organizzazione, secondo un programma triennale che consenta di verificare, nell'arco dei tre anni, almeno una volta, ogni punto relativo alle prescrizioni contenute nella norma di riferimento secondo cui il Sistema di Gestione Security è stato certificato.

Durante gli audit di sorveglianza saranno comunque presi in considerazione i seguenti aspetti:

a) audit interni ed i riesami da parte della direzione;

b) un riesame delle azioni intraprese a seguito delle non conformità identificate durante il precedente audit;

c) il trattamento dei reclami;

d) l'efficacia del Sistema di Gestione riguardo il conseguimento degli obiettivi;

e) l'avanzamento delle attività pianificate mirate al miglioramento continuo;

f) il controllo operativo continuo;

g) il riesame di ogni cambiamento.

La descrizione delle attività e delle disposizioni per la conduzione dell'audit di sorveglianza presso il sito/i è riportato, in dettaglio, nel piano di audit di sorveglianza che RINA invia all'Organizzazione prima dell'effettuazione dell'audit stesso.

4.5

Deve essere effettuato almeno un audit di sorveglianza con periodicità non superiore ai 12 mesi e la data entro la quale devono essere effettuati gli audit è riportata sul programma di audit triennale inviato all'Organizzazione.
Tale programma può essere modificato dal RINA sulla base dei risultati degli audit di sorveglianza precedenti.

Eventuali scostamenti degli audit di sorveglianza oltre tali limiti temporali, dovuti a giustificati motivi, devono essere concordati preventivamente con il RINA e devono comunque essere recuperati al primo audit successivo.

In ogni caso la data del primo audit di sorveglianza, successivo alla certificazione iniziale dovrà essere fissata entro dodici mesi dalla data finale dell'audit stage2.

4.6

Il RINA si riserva inoltre di effettuare audit aggiuntivi rispetto a quelli previsti dal programma triennale, annunciati o non annunciati, presso l'Organizzazione:
nel caso gli pervengano reclami o segnalazioni, ritenute particolarmente significative, relative alla non rispondenza del Sistema di Gestione Security ai requisiti della norma di riferimento e al presente Regolamento
in relazione a cambiamenti intervenuti nell'Organizzazione
ad Organizzazioni cui è stata sospesa la certificazione.

In caso di rifiuto, senza valide motivazioni, da parte dell'Organizzazione, il RINA può avviare l'iter di sospensione della certificazione.

Nel caso in cui i reclami e le segnalazioni siano ritenute giustificate dal RINA, il costo dell'effettuazione dell'audit aggiuntivo è a carico dell'Organizzazione.

4.7

Le date di esecuzione degli audit di sorveglianza sono concordate con l'Organizzazione con adeguato anticipo e ad essa ufficialmente confermate tramite una comunicazione scritta.

I nominativi dei tecnici qualificati incaricati all'effettuazione all'audit sono preventivamente comunicati dal RINA all'Organizzazione, la quale può fare obiezione sulla loro nomina, giustificandone i motivi.

4.8

Per le modalità di comunicazione dell'esito dell'audit si rimanda al precedente punto 3.5.

La validità del certificato è confermata, a seguito dell'esito positivo dell'audit di sorveglianza.

4.9

In presenza di non conformità maggiori o di altri rilievi, la cui numerosità a giudizio del gruppo di audit sia tale da pregiudicare il corretto funzionamento del Sistema, l'Organizzazione è sottoposta ad un audit supplementare entro i tempi stabiliti dal RINA, in relazione all'importanza delle non conformità stesse e, comunque, non oltre tre mesi dal termine dell'audit di sorveglianza.
Nel caso le non conformità non siano risolte entro i tempi stabiliti o qualora le non conformità rilevate siano tali da non assicurare il controllo degli aspetti/impatti ambientali e delle normative di legge applicabili, il RINA può sospendere la certificazione sino a che le non conformità stesse non siano state corrette e comunque in accordo con quanto previsto dal punto 10.1.

Tutte le spese relative ad eventuali audit aggiuntivi conseguenti a carenze del Sistema di Gestione Security sono da considerarsi a carico dell'Organizzazione.

CAPITOLO 5
RICERTIFICAZIONE

5.1

In occasione dell'audit di ricertificazione del Sistema di Gestione Security, previsto ogni tre anni, l'Organizzazione deve contattare il RINA, con anticipo di circa tre mesi rispetto alla data prevista sul programma di audit triennale in suo possesso, ed inviare una copia aggiornata e compilata in tutte le sue parti del Questionario Informativo (disponibile sul sito web www.rina.org) al fine di poter pianificare l'attività e concordare la data di esecuzione dell'audit ricertificazione.
La data di esecuzione dell'audit ricertificazione, concordata con l'Organizzazione con adeguato anticipo, è ad essa ufficialmente confermato tramite una comunicazione scritta.

I nominativi dei tecnici qualificati incaricati dell'effettuazione dell'audit sono preventivamente comunicati dal RINA all'Organizzazione, la quale può fare obiezione sulla loro nomina, giustificandone i motivi.

5.2

L'audit di ricertificazione ha come scopo quello di confermare il mantenimento della conformità e dell'efficacia del Sistema di Gestione nel suo complesso e si basa principalmente su un audit in sito da effettuarsi, di regola, con gli stessi criteri dell'audit stage2.

In particolare, l'audit di ricertificazione comprende un audit in sito che prende in considerazione, tra l'altro i seguenti aspetti:

a) l'efficace interazione tra i processi del Sistema di Gestione della Security;
b) l'efficacia del sistema di gestione nella sua globalità alla luce di cambiamenti interni ed esterni;
c) la dimostrazione dell'impegno a mantenere l'efficacia e l'aggiornamento del Sistema di Gestione della Security.
d) se l'operatività del sistema di gestione contribuisce al conseguimento della politica e degli obiettivi dell'organizzazione;

La descrizione delle attività e delle disposizioni per la conduzione dell'audit di ricertificazione presso il sito/i è riportato, in dettaglio, nel piano di audit di ricertificazione che RINA invia all'Organizzazione prima dell'effettuazione dell'audit stesso.

5.3

A seguito dell'esito positivo dell'audit di ricertificazione il gruppo di audit presenta al RINA la proposta di ricertificazione dell'Organizzazione ai fini della riemissione del certificato di conformità.

Il certificato di conformità è riemesso da RINA a seguito dell'esito positivo dell'esame della suddetta proposta dell'Organizzazione.
La conferma dell'approvazione da parte di RINA della ricertificazione con conseguente rilascio del certificato è inviata per iscritto all'Organizzazione.

Per il dettaglio sulla gestione e validità dei certificati di conformità rilasciati da RINA si veda il successivo capitolo 6.

5.4

L'iter di ricertificazione deve necessariamente concludersi, con esito positivo, prima della data di scadenza della certificazione riportata sul certificato che non può essere prorogata da parte di RINA.

Di conseguenza l'audit di ricertificazione si deve concludere positivamente in tempo utile per permettere l'approvazione da parte di RINA della proposta di ricertificazione e la conseguente riemissione del certificato entro la suddetta data (almeno un mese prima della data di scadenza riportata sul certificato).

Qualora un'Organizzazione non ottemperi alle tempistiche suddette e che quindi non ottenga la riemissione del certificato entro i termini di scadenza dello stesso, la relativa certificazione deve ritenersi scaduta a partire dal giorno successivo alla data di scadenza riportata sul certificato.
L'Organizzazione che, dopo la data di scadenza del certificato, intenda nuovamente accedere alla certificazione, deve presentare una nuova domanda seguendo, di regola, l'intero iter previsto per la certificazione iniziale.

5.5

In presenza di non conformità maggiori o di altri rilievi, la cui numerosità a giudizio del gruppo di audit sia tale da pregiudicare il corretto funzionamento del Sistema, l'Organizzazione deve necessariamente applicare, in modo efficace, i relativi trattamenti e/o azioni correttive prima della data di scadenza del certificato di conformità.

Ciò implica che RINA dovrà effettuare l'audit supplementare per la verifica dellla chiusura di tali non conformità in tempo utile per la successiva emissione del certificato.
I tempi stabiliti entro i quali RINA deve effettuare l'audit supplementare sono comunicati all'Organizzazione sul rapporto di audit di ricertificazione.
L'audit supplementare può essere effettuato sul sito o su base documentale in base alla tipologia delle azioni correttive da verificare a giudizio del team di audit.

Tutte le spese relative ad eventuali audit supplementari conseguenti a carenze del Sistema di Gestione Security sono da considerarsi a carico dell'Organizzazione.

CAPITOLO 6
GESTIONE DEI CERTIFICATI DI CONFORMITA'

6.1

Il certificato di conformità rilasciato da RINA ha una validità di tre anni a partire dalla data di approvazione della proposta di certificazione iniziale o di ricertificazione da parte del RINA

Sul Certificato sono, tra l'altro, chiaramente riportate eventuali attività, presenti nel/i sito/i oggetto di certificazione, ma escluse dal campo di applicazione del Sistema di Gestione Security.

6.2

Dal momento del rilascio del certificato da parte di RINA, copia originale dello stesso e del relativo programma triennale di audit è reso disponibile all'Organizzazione sulla "Member Area" del sito web RINA (www.rina.org).
In caso di impossibilità di accesso ad internet, l'Organizzazione potrà richiederne copia originale in formato cartaceo all'Ufficio RINA di pertinenza.

6.3

La validità del certificato, nell'arco del triennio di validità, è subordinata al risultato dei successivi audit di sorveglianza.

A buon esito di ciascun audit di ricertificazione, come riportato al precedente capitolo 5, è riemesso il certificato di conformità.

La validità del certificato può essere sospesa, revocata o rinunciata in accordo a quanto previsto al Capitolo 10 e 11.

RINA pubblica e mantiene aggiornati direttamente sul proprio sito web www.rina.org:

- l'elenco delle Organizzazioni certificate;
- lo stato di validità dei certificati emessi indicando per ciascun certificato lo stato valido, sospeso o non valido;
- le copie dei certificati in corso di validità.

Su richiesta RINA fornisce informazioni sullo stato della certificazione.

CAPITOLO 7
MODIFICA DELLA CERTIFICAZIONE E COMUNICAZIONE CAMBIAMENTI

7.1

L'Organizzazione in possesso della certificazione può richiedere una modifica o estensione della stessa presentando una nuova richiesta di certificazione, corredata dalla documentazione di cui al punto 3.2 debitamente aggiornata. Il RINA si riserva di esaminare caso per caso le richieste e di decidere le modalità di valutazione ai fini del rilascio di una nuova certificazione, in conformità a quanto previsto dalle "CONDIZIONI GENERALI DI CONTRATTO PER LA CERTIFICAZIONE DI SISTEMI, PRODOTTI E PERSONALE" ed alla norma ISO 28003:2007.

7.2

L'Organizzazione deve comunicare tempestivamente a RINA eventuali cambiamenti intervenuti su aspetti che possono influenzare la capacità del Sistema di Gestione di continuare a soddisfare i requisiti della norma utilizzata per la certificazione.
Queste disposizioni riguardano, per esempio, variazioni relative:

a) allo stato legale, commerciale, organizzativo o alla proprietà;
b) all'organizzazione e alla gestione, (ad es. responsabili chiave o personale tecnico, processo decisionale);
c) agli indirizzi di contatto ed ai siti;
d) al campo di applicazione delle attività coperte dal Sistema di Gestione certificato;
e) a cambiamenti significativi del Sistema di Gestione e dei processi.

Il RINA si riserva di effettuare audit aggiuntivi presso l'Organizzazione nel caso le modifiche comunicate siano ritenute particolarmente significative ai fini del mantenimento della conformità del Sistema di Gestione Security ai requisiti della norma di riferimento e al presente Regolamento ovvero di revisionare le condizioni economiche per l'eventuale modifica del contratto.

CAPITOLO 8
PARTICOLARITA' PER ORGANIZZAZIONI MULTISITO

8.1

Generalmente, tutti i siti dell'organizzazione saranno verificati, eventuali differenze nel calcolo dei giorni uomo, rispetto a quanto stabilito nell'ANNEX A della norma ISO 28003:2007, saranno giustificati, attraverso un approccio di risk management definito da RINA che terrà in considerazione il settore e/o le attività, la tipologia e la dimensione dei siti da valutare, le eventuali variazioni locali applicabili al Sistema di Gestione della Security, nonché l'utilizzo temporaneo di eventuali siti operanti sotto il Sistema di Gestione della security.

Qualora un'Organizzazione operi su più siti permanenti, tutte le funzioni attinenti al Sistema di Gestione della Security siano gestite da una sede centrale e sia richiesta un'unica certificazione, le attività di audit possono essere espletate per campionamento dei siti sottoposti ad audit, purché:

- la catena di fornitura dei servizi forniti da tutti i siti e tutte le attività siano sostanzialmente gli stessi e siano svolti in pieno accordo con gli stessi metodi e procedure;
- sia implementato un Sistema di Gestione della Security comune a tutti i siti e che l'Organizzazione abbia implementato, quando necessario, le azioni correttive in ogni suo sito;
- le minacce per la security siano le medesime per ogni sito operativo. L'Organizzazione abbia implementato una valutazione del rischio per ogni sito e abbia messo in atto opportune misure di controllo;
- almeno le seguenti attività siano gestite dalla sede centrale dell'Organizzazione:
  - riesame della Direzione;
  - implementazione degli obiettivi e dei programmi di gestione;

- valutazione delle necessità di addestramento;
- controllo della documentazione e delle sue modifiche;
- valutazione dei reclami, incidenti, azioni correttive e preventive;
- pianificazione /esecuzione degli audit interni e valutazione dei loro risultati;

- Prima dell'audit iniziale da parte del RINA, l'organizzazione abbia effettuato un audit interno ad ogni sito ed abbia verificato, dopo la chiusura delle eventuali azioni correttive, la sua conformità alla norma di riferimento. L'organizzazione dovrebbe essere in grado di dimostrare, tramite opportune registrazioni, l'efficacia dei controlli in ogni sito inclusi quelli non soggetti agli audit dell'organismo di certificazione.

8.2

Il RINA rilascia un singolo certificato con il nome e l'indirizzo della sede centrale dell'Organizzazione. In allegato o sul certificato stesso è emesso un elenco di tutti i siti a cui si riferisce il certificato.

All'organizzazione può essere rilasciato uno stralcio del certificato per ciascun sito coperto dalla certificazione, a condizione che esso contenga lo stesso scopo o un suo sotto-elemento ed includa un riferimento chiaro al certificato principale.

8.3

Per eventuali non conformità rilevate in un singolo sito durante gli audit, l'Organizzazione deve valutare se le stesse sono relative a carenze imputabili a più siti e se del caso, deve adottare azioni correttive sia presso la sede centrale che presso gli altri siti.

8.4

Sulla base delle informazioni fornite dall'Organizzazione il RINA stabilisce il piano di campionamento applicabile sia per l'audit iniziale che per gli audit di sorveglianza e di ricertificazione. Sul programma triennale di audit è indicato il numero di siti oggetto di campionamento per ogni audit programmato.

CAPITOLO 9
TRASFERIMENTO DI CERTIFICATI ACCREDITATI

9.1

Qualora un'Organizzazione, con certificazione per i Sistemi di Gestione della Security in corso di validità rilasciata da un altro Organismo di certificazione, presenti domanda di certificazione, il RINA prevede procede come segue:

- l'analisi documentale come riportato al paragrafo 3.2 del presente Regolamento;

- il riesame dei rapporti dei precedenti audit condotti dall'Organismo accreditato che ha rilasciato la certificazione precedente;
- l'eventuale audit presso l'Organizzazione, il cui grado di estensione dipende dallo stato di conformità e di validità della certificazione rilasciata in precedenza.

L'Organizzazione deve inoltre comunicare al RINA:

- le motivazioni della richiesta di trasferimento della certificazione
- eventuali osservazioni o segnalazioni pervenute dalle autorità nazionali o locali preposte
- eventuali reclami ricevuti e relative azioni intraprese

Il contratto tra il RINA e il richiedente è gestito con le stesse modalità riportate al paragrafo 3.1, in funzione dell'estensione dell'attività di audit.

A completamento con esito favorevole dell'attività sopra riportata, è rilasciato, per il Sistema di Gestione Security in esame, un Certificato di Conformità che, di regola, mantiene la scadenza già stabilita dall'Organismo che ha emesso la precedente certificazione.

In generale, anche per l'effettuazione degli audit di sorveglianza e di ricertificazione del Sistema è mantenuta la programmazione già stabilita dall'Organismo che ha emesso la precedente certificazione.

CAPITOLO 10
SOSPENSIONE, RIPRISTINO E REVOCA DELLA CERTIFICAZIONE

10.1

La validità del Certificato di conformità può essere sospesa in accordo a quanto previsto dalle "CONDIZIONI GENERALI DI CONTRATTO PER LA CERTIFICAZIONE DI SISTEMI, PRODOTTI E PERSONALE" e nei seguenti casi specifici:

- se l'Organizzazione non consente che siano condotti gli audit di sorveglianza o di ricertificazione alle frequenze richieste;
- se sono riscontrate nel Sistema di Gestione Security delle non conformità maggiori non risolte entro i tempi stabiliti dal RINA;
- se l'Organizzazione non ha rispettato i termini fissati per la comunicazione delle azioni correttive, a seguito di non conformità segnalate sul rapporto di audit;
- se l'Organizzazione ha effettuato importanti ristrutturazioni interne al Sito/i, si trasferisce in un altro sito/i senza segnalare tali varianti al RINA;

- se l'Organizzazione ha apportato al suo Sistema di Gestione Security modifiche rilevanti che non siano state accettate dal RINA;
- in presenza di importanti ristrutturazioni dell'Organizzazione non comunicate al RINA;
- per rifiuto od ostacolo alla partecipazione agli audit di osservatori di un Ente di Accreditamento;
- per l'evidenza che il Sistema di Gestione Security non assicura il rispetto delle leggi e regolamenti cogenti applicabili alle attività e/o al sito/i;
- riscontro di eventuali giustificati e gravi reclami pervenuti al RINA.

L'Organizzazione può inoltre richiedere al RINA, giustificandone i motivi, la sospensione della certificazione per un periodo in generale non superiore a sei mesi e comunque non oltre la data di scadenza del certificato.

La sospensione è notificata per iscritto all'Organizzazione, precisando le condizioni per il ripristino della certificazione ed il termine entro il quale devono essere attuate.

La sospensione della validità del Certificato decorre dalla data dell'invio della notifica ed è resa pubblica dal RINA direttamente sul sito web www.rina.org come previsto al punto 6.3.

10.2

Il ripristino della certificazione è subordinato all'accertamento dell'eliminazione delle carenze che avevano causato la sospensione stessa mediante un audit approfondito che verifichi la rispondenza del Sistema di Gestione Security a tutti i requisiti della norma di riferimento.

Esso è notificato per iscritto all'Organizzazione e reso pubblicamente noto dal RINA attraverso il sito web www.rina.org come previsto dal punto 6.3.

10.3

Il mancato soddisfacimento entro il termine prescritto delle condizioni di cui al punto 10.2 causa la revoca del Certificato di conformità.

La revoca del Certificato di conformità può essere decisa in accordo a quanto previsto dalle "CONDIZIONI GENERALI DI CONTRATTO PER LA CERTIFICAZIONE DI SISTEMI, PRODOTTI E PERSONALE" e nei seguenti casi specifici:

- quando si verifichino circostanze, quali quelle citate al punto 10.1 per la sospensione, che siano giudicate particolarmente gravi;
- se l'Organizzazione sospende le sue attività o servizi oggetto del Sistema di Gestione Security certificato per un periodo in generale superiore a sei mesi;
- qualora l'Organizzazione non accetti le nuove condizioni economiche stabilite dal RINA per l'eventuale modifica del contratto;

- nel caso di organizzazione multi-sito, qualora la sede centrale o uno dei siti non rispetti i criteri necessari per il mantenimento del certificato;
- per ogni altro serio motivo, a giudizio del RINA

L'avvenuta revoca del Certificato di Conformità è notificata per iscritto all'Organizzazione ed è resa pubblicamente nota dal RINA secondo quanto previsto dal punto 6.3.

L'Organizzazione che dopo la revoca intenda nuovamente accedere alla certificazione, deve presentare una nuova domanda seguendo l'intero iter.

CAPITOLO 11
RINUNCIA ALLA CERTIFICAZIONE

L'Organizzazione certificata può inviare una formale comunicazione di rinuncia alla certificazione al RINA, prima della scadenza del Certificato, incluso il caso in cui l'Organizzazione stessa non voglia o non possa adeguarsi alle nuove istruzioni impartite dal RINA.
RINA, al momento della ricezione di tale comunicazione, avvia l'iter per rendere lo stato del certificato non valido.
In generale, entro un mese dalla data della avvenuta comunicazione, RINA aggiorna lo stato di validità del certificato.

CAPITOLO 12
CONDIZIONI CONTRATTUALI

Per le condizioni contrattuali trovano applicazione le disposizioni contenute nel documento RINA "CONDIZIONI GENERALI DI CONTRATTO PER LA CERTIFICAZIONE DI SISTEMI, PRODOTTI E PERSONALE", nell'edizione in vigore.

Pubblicazione: NC/C 64
Edizione Italiana

RINA Società per azioni
Via Corsica, 12 - 16128 Genova - Italia
Tel. +39 01053851 - Fax: +39 0105351000
www.rina.org

Regolamenti tecnici