
 Italia	REGOLAMENTO PARTICOLARE PER LA CERTIFICAZIONE DEI SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI Pag. 1 di 9	RSSI	3 ^a Ediz.	Rev.00
---	--	------	----------------------	--------

INDICE

1. Scopo ed entrata in vigore
2. Campo di applicazione
3. Termini e definizioni
4. Responsabilità
5. Controllo del regolamento
6. Iter di certificazione
 - 6.1 Generalità
 - 6.2 Modalità di svolgimento degli audit
 - 6.3 Avvio dell'iter di certificazione
 - 6.4 Visita preliminare (preaudit)
 - 6.5 Audit di 1° stadio (Esame iniziale della documentazione + visita iniziale)
 - 6.6 Audit di 2° stadio (per la verifica iniziale del sistema di gestione, o audit per la certificazione)
 - 6.7 Emissione iniziale della certificazione e successivi rinnovi
 - 6.8 Audit di sorveglianza
 - 6.9 Audit di rinnovo
 - 6.10 Audit non programmati
7. Registro delle organizzazioni certificate
8. Modalità di riferimento alla certificazione - Uso del certificato e del marchio
9. Sospensione della certificazione
10. Ritiro / annullamento della certificazione
11. Gestione dei reclami e delle segnalazioni da parte delle organizzazioni clienti e dalle parti interessate
12. Controllo della documentazione del sistema di gestione SGSI e dei rapporti di verifica del TÜV Italia srl
13. Modifiche al sistema di gestione
14. Modifiche alle regole del sistema di certificazione
15. Prescrizioni particolari per organizzazioni già certificate da altro organismo
16. Riservatezza
17. Ricorsi (o Appelli)
18. Reclami nei confronti di TÜV Italia
19. Contenziosi
20. Allegati

00	01-09-11	Nuova edizione	 D. DIOMEDE	 P. MERENDA
N°DI REV.	DATA	DESCRIZIONE DELLA REVISIONE	VERIFICA FIRMA DI CTSSI	APPROVAZIONE FIRMA DI DCMS

 Italia	<p style="text-align: center;">REGOLAMENTO PARTICOLARE PER LA CERTIFICAZIONE DEI SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI</p> <p style="text-align: center;">Pag. 2 di 9</p>	<p style="text-align: center;">RSSI</p>	<p style="text-align: center;">3^a Ediz.</p>	<p style="text-align: center;">Rev.00</p>
---	--	--	---	--

1. Scopo ed entrata in vigore

Scopo di questo documento è integrare il Regolamento Generale per la Certificazione dei Sistemi di Gestione (RGSG) adottato da TÜV Italia s.r.l. (nel seguito denominata TÜV Italia), ai fini specifici della certificazione dei sistemi di gestione per la Sicurezza delle informazioni (SGSI o, in modo del tutto equivalente in inglese, ISMS).

Il presente regolamento entra in vigore a 30 giorni dalla data di emissione riportata in intestazione.

2. Campo di applicazione

Questo regolamento si applica alle attività di certificazione di sistemi di gestione per la sicurezza delle informazioni (SGSI) svolte sotto accreditamento ACCREDIA.

Il presente regolamento viene applicato da TÜV Italia in maniera uniforme e imparziale per tutte le organizzazioni che utilizzano i servizi di certificazione erogati da TÜV Italia; in particolare non vengono poste in atto condizioni di tipo finanziario o condizioni indebite di altra natura; inoltre l'accesso alla certificazione non è condizionato dalle dimensioni dell'organizzazione o dall'appartenenza ad una particolare associazione o ad un gruppo e neppure dal numero di organizzazioni già certificate.

Esso non pregiudica l'applicabilità di altri regolamenti inerenti ulteriori schemi certificativi per cui l'organizzazione risulti certificata da TÜV Italia e/o da altri Organismi di Certificazione.

Le normative applicabili come riferimento per gli SGSI sono:

- la norma ISO/IEC 27001:2005 "Information technology – Security techniques – information security management systems - Requirements" ; o la sua versione italiana UNI CEI ISO/IEC 27001:2006 "Tecnologia delle informazioni tecniche di sicurezza- sistema di gestione per la sicurezza delle informazioni – Requisiti", nel seguito considerate equivalenti in termini di descrizione dei requisiti.
- La linea guida ISO/IEC 27002:2005 (in precedenza rilasciata come ISO /IEC 17799:2005) "Information technology- Security techniques – Code of practice for information security management".
- La linea guida ISO/IEC 27005:2008 "Information technology — Security techniques — Information security risk management".
- La linea guida ISO/IEC 27006:2007 "Information Technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems"
- La norma nazionale UNI CEI EN ISO/IEC 17021:2011 "Valutazione della conformità - Requisiti per gli organismi che forniscono audit e certificazione di sistemi di gestione"

Inoltre sono riferimento obbligatorio i documenti emessi da ACCREDIA e reperibili nel sito www.accredia.it:


- Eventuali Regolamenti Tecnici
- Regolamento per l'accreditamento degli Organismi di certificazione RG 01
- Disposizioni in materia di accreditamento emesse da ACCREDIA / SINCERT

3. Termini e definizioni

La terminologia utilizzata nel presente regolamento è in accordo alle seguenti norme:

- ISO/IEC 27000:2009 "Information technology - Security techniques - Information security management systems - Overview and vocabulary"
- UNI EN ISO 9000:2005 "Sistemi di gestione per la qualità – Fondamenti e vocabolario".
- UNI CEI EN 45020:2007 "Normazione ed attività connesse – Vocabolario generale".
- ISO/IEC 17000:2004 "Conformity assessment - Vocabulary and general principles".

Gli acronimi impiegati nel testo del presente regolamento sono:

 Italia	<p align="center">REGOLAMENTO PARTICOLARE PER LA CERTIFICAZIONE DEI SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI</p> <p align="center">Pag. 3 di 9</p>	<p align="center">RSSI</p>	<p align="center">3^a Ediz.</p>	<p align="center">Rev.00</p>
---	--	-----------------------------------	--	-------------------------------------

- ISMS (Information Security Management System) = Sistema di Gestione per la Sicurezza delle Informazioni (SGSI)
- SoA (Statement of Applicability) = Dichiarazione di Applicabilità

Per la definizione di:

- Carezza (CA)
- Nonconformità (NC)
- Osservazione (OSS):
- Commento (COM)

si veda il Regolamento generale RGSG.

4. Responsabilità

Il presente regolamento descrive in dettaglio le responsabilità che l'organizzazione e TÜV Italia devono assolvere nel corso del rapporto contrattuale relativo alle attività di certificazione in accordo allo standard UNI CEI ISO/IEC 27001:2006.

Si segnala che le organizzazioni clienti di TÜV Italia sono autorizzate a creare un link sulla home page del sito Web di TÜV Italia, il cui indirizzo è www.TUV.it.

5. Controllo del regolamento

Il presente regolamento particolare è a disposizione degli interessati sul sito internet www.tuv.it.

In ogni caso le organizzazioni possono richiederne copia cartacea.

Inoltre, in caso di revisione del regolamento, tutte le organizzazioni che hanno in essere un contratto di certificazione vengono informate dell'esistenza della nuova versione.

Le modifiche che vengono apportate al regolamento nelle sue versioni successive (a seguito di nuove revisioni) sono evidenziate con le seguenti modalità:

- il testo revisionato e/o aggiuntivo viene scritto in carattere corsivo (*italics*)
- il testo annullato e non sostituito è segnalato con {testo annullato}

Nel caso di nuove edizioni, poiché i cambiamenti sono significativi, non viene evidenziata la modifica, ma fa testo l'intero contenuto del documento.


6. Iter di certificazione

6.1 Generalità

L'iter di certificazione dei sistemi di gestione adottato dal TÜV Italia è descritto nel Regolamento generale RGSG.

Nello svolgimento dell'iter di certificazione, occorre tenere presenti le seguenti particolari considerazioni e prescrizioni:

- La norma UNI CEI ISO/IEC 27001:2006 riporta nelle sezioni da 4 a 8 (comprese) una serie di requisiti obbligatori per gli SGSI, che non possono essere cioè oggetto di esclusione.
- Invece nell'Appendice A (normativa) (dedicata ai controlli ed ai relativi obiettivi di controllo, denominata "Annex A" nella versione originale della norma) essa riporta l'elenco dei possibili controlli da impiegare nell'ambito dello specifico SGSI, in funzione dei risultati dei processi di valutazione e di trattamento dei rischi; pertanto i controlli descritti nell'Appendice A non sono tutti obbligatori per tutti gli SGSI, ma vanno selezionati dall'organizzazione responsabile del SGSI utilizzando criteri documentati che tengano presente le proprie reali esigenze; quindi i controlli ritenuti realmente necessari e dunque "obbligatori" nell'ambito dello specifico SGSI vengono identificati a cura dell'organizzazione nel SoA, dove devono essere riportate e giustificate eventuali esclusioni.
- Da quanto sopra deriva che TÜV Italia, quale organismo di certificazione degli SGSI, ha il compito di valutare la documentazione ed attuazione di tutti i requisiti delle sezioni da 4 a 8 (comprese), del par. A.15 e degli altri paragrafi

 Italia	REGOLAMENTO PARTICOLARE PER LA CERTIFICAZIONE DEI SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI Pag. 4 di 9	RSSI	3^a Ediz.	Rev.00
---	--	-------------	----------------------------	---------------

dell'Appendice A" che l'organizzazione ha dichiarato applicabili nel SoA; TÜV Italia si riserva la facoltà di giudicare l'adeguatezza delle scelte operate dall'organizzazione

- Nell'esecuzione delle proprie verifiche TÜV Italia esamina inoltre l'esistenza e la congruenza dei collegamenti tra i diversi elementi del SGSI quali: la politica, i risultati della valutazione dei rischi, gli obiettivi generali e di dettaglio, le strategie di trattamento dei rischi, le responsabilità, i programmi, le procedure, i riesami interni sulla sicurezza, ecc.
- Per quanto concerne il rispetto dei requisiti cogenti (per disposizione di leggi, regolamenti, direttive, ecc.), il principio generale è che il mantenimento e la valutazione della conformità ai suddetti requisiti cogenti ricadono sotto la responsabilità dell'organizzazione che gestisce l'ISMS e che ne rilascia apposita attestazione a TÜV Italia (vedere modulo RLI); TÜV Italia si limita ad eseguire verifiche a campione per acquisire fiducia che l'ISMS sia efficace sotto questo punto di vista e che – nell'eventualità di non conformità rispetto ai requisiti cogenti – l'organizzazione metta in atto idonee azioni correttive.
- Può accadere che l'organizzazione gestisca reti di informazioni che ricadono sotto il controllo di un unico SGSI ma che siano ramificate in luoghi geografici diversi, ossia in più siti; in tale situazione TÜV Italia può emettere un unico certificato, ma si riserva la decisione di verificare ogni singolo sito o campionarne alcuni e verificare solo questi (TÜV Italia prende tale decisione sulla base delle apposite prescrizioni e raccomandazioni degli standard ISO/IEC 27006 e ISO/IEC 17021:2011, nonché degli RT e RG emessi da ACCREDIA).

6.2 Modalità di svolgimento degli audit

Le modalità di svolgimento dell'audit sono descritte nel Regolamento generale RGSG, cui si aggiunge quanto segue:

L'organizzazione, all'atto della richiesta di certificazione, è tenuta a comunicare se intende avvalersi della facoltà di negare al team di audit l'accesso a registrazioni che contengano informazioni considerate riservate o sensibili (per esempio informazioni relative al personale, ai clienti ed ai fornitori); in tale caso, però, il TÜV Italia valuterà se le informazioni cui può avere accesso sono sufficienti ai fini della valutazione del SGSI; se non lo fossero, l'organizzazione ed il TÜV Italia devono raggiungere – ove possibile – un accordo sulle modalità di accesso a tutte le informazioni indispensabili per la valutazione del SGSI; se l'accordo non può essere raggiunto, l'iter di certificazione non viene iniziato. Detto accordo può consistere nel fatto che l'organizzazione autorizzi il team di audit ad accedere ad informazioni, riservate o sensibili, solo per il tempo dell'audit e in base a modalità specificate.

6.3 Avvio dell'iter di certificazione

L'iter di certificazione viene avviato con l'emissione della conferma d'ordine da parte di TÜV Italia. Vale inoltre quanto descritto nel Regolamento Generale RGSG.

6.4 Visita preliminare (preaudit)

Vale quanto descritto nel paragrafo 6.4 del Regolamento Generale RGSG.

6.5 Audit di 1° stadio (Esame iniziale della documentazione + visita iniziale)

Vale quanto descritto nel Regolamento Generale RGSG.


Inoltre si aggiunge quanto segue :

a) Verifica della documentazione del SGSI (1° fase del 1° stadio)

La verifica della documentazione del SGSI viene eseguita sempre.

Per documentazione del SGSI si intende quanto segue:

- i documenti specificati dalla ISO/IEC 27001 al par. 4.3.1
- l'elenco dei requisiti cogenti applicabili nell'ambito del SGSI, integrato dall'attestazione scritta del rispetto di tali requisiti rilasciata dall'organizzazione (vedere modulo RLI allegato).

 Italia	<p align="center">REGOLAMENTO PARTICOLARE PER LA CERTIFICAZIONE DEI SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI</p> <p align="center">Pag. 5 di 9</p>	<p align="center">RSSI</p>	<p align="center">3^a Ediz.</p>	<p align="center">Rev.00</p>
---	--	-----------------------------------	--	-------------------------------------

Tra i documenti specificati nella norma vi sono, in particolare, i documenti relativi alla valutazione ed al trattamento dei rischi, la Dichiarazione di Applicabilità, le policy e le procedure per la sicurezza delle informazioni. Per la redazione della Dichiarazione di Applicabilità, è allegato al presente regolamento l'apposito modulo SoA, che rappresenta un facsimile con tutte le informazioni indispensabili da riportare nella dichiarazione stessa. Per la redazione dell'elenco dei requisiti cogenti e della attestazione di conformità ad essi, è invece allegato al presente regolamento l'apposito modulo RLI.

Si sottolinea inoltre che nei suddetti documenti deve essere chiaramente riportato il campo di applicazione dell'ISMS, nonché il suo "perimetro" fisico (sedi dell'organizzazione incluse nel SGSI) e logico (sistemi e utenze coperte dal SGSI pur se fisicamente non nelle sedi). Eventuali interfacce / interazioni con servizi o attività non completamente inclusi nel campo di applicazione devono essere individuate e comprese nella valutazione dei rischi (per esempio questo potrebbe essere il caso di computer o sistemi di telecomunicazioni condivisi con altre organizzazioni). L'esame della documentazione è volto ad accertare che essa sia innanzitutto completa ossia soddisfi tutti i requisiti della ISO/IEC 27001:2005 e del presente regolamento; inoltre la documentazione deve essere chiara, ossia non deve lasciare adito a dubbi interpretativi, deve essere congruente tra le sue varie parti e deve essere facilmente leggibile.

b) Visita iniziale (2° fase del 1° stadio)

La visita iniziale viene eseguita sempre e consiste in una verifica in campo presso il sito (o i siti) dell'organizzazione. Essa consente innanzitutto a TÜV Italia di meglio comprendere:

- la dimensione e le caratteristiche del SGSI dell'organizzazione;
- il suo grado di idoneità ad affrontare l'iter di certificazione;
- l'applicabilità di norme e requisiti legislativi relativi alla sicurezza delle informazioni;
- il tipo di esperienza richiesta al team incaricato dell'audit di 2° stadio;
- l'entità delle risorse necessarie per svolgere l'audit di 2° stadio.

Inoltre la visita iniziale consente all'organizzazione di approfondire i seguenti aspetti (qualora non già risolti ad esempio in occasione dell'eventuale preaudit di cui al par. 6.4):

- dettagli dell'iter di certificazione;
- programmazione più precisa dei tempi necessari per giungere alla certificazione;
- definizione esatta del campo di applicazione del SGSI;
- identificazione di eventuali carenze nella attuazione del SGSI.

Per conseguire le suddette finalità, durante la visita iniziale il team di audit valuta il grado di soddisfacimento dei seguenti punti fondamentali della norma ISO/IEC 27001:2005:


- requisiti delle sezioni da 4 a 8;
- requisiti del paragrafo A.15.

Per ciascuno di tali requisiti, l'ISMS deve risultare attuato e devono essere disponibili le corrispondenti registrazioni.

L'esito dell'esame della documentazione è riportato, assieme ai risultati della visita iniziale, in un apposito rapporto, emesso a conclusione dell'audit di 1° stadio. Copia del rapporto viene consegnata anche all'organizzazione; se necessario, esso può essere illustrato al cliente in occasione di un incontro diretto col cliente stesso. Qualora l'attuazione del SGSI risulti carente, il cliente ne viene informato tramite il suddetto rapporto.

Nel caso l'esame della documentazione abbia evidenziato carenze (CA) queste dovranno essere corrette dall'organizzazione prima dell'audit di 2° stadio; l'eventuale permanere di carenze (CA) della documentazione al momento dell'audit di 2° stadio impedirà l'emissione immediata del certificato e renderà necessaria l'effettuazione di un postaudit.

TÜV Italia effettuerà un riesame del rapporto di 1° stadio per decidere se ci sono le condizioni per procedere con l'audit di 2° stadio, e per verificare la necessità di competenze particolari per il team di audit di 2° stadio. Inoltre, qualora emergano scostamenti rispetto a quanto comunicato dall'organizzazione in sede di formulazione offerta, TÜV Italia si riserva di valutare la necessità di modificare la propria offerta economica.

 Italia	<p style="text-align: center;">REGOLAMENTO PARTICOLARE PER LA CERTIFICAZIONE DEI SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI</p> <p style="text-align: center;">Pag. 6 di 9</p>	<p style="text-align: center;">RSSI</p>	<p style="text-align: center;">3^a Ediz.</p>	<p style="text-align: center;">Rev.00</p>
---	--	--	---	--

6.6 Audit di 2° stadio (per la verifica iniziale del sistema di gestione, o audit per la certificazione)

Vale quanto descritto nel Regolamento Generale RGSG.

In aggiunta si precisa che:

L'audit per la certificazione si svolge sempre in campo (ossia presso il/i sito/i dell'organizzazione), entro max 6 mesi e minimo 7 giorni dall'avvio dell'audit di 1° stadio

Inoltre al momento di tale audit l'ISMS dell'organizzazione deve risultare già operativo; in particolare l'organizzazione deve aver definito obiettivi per la sicurezza delle informazioni misurabili e – ove possibile - quantificati, deve aver eseguito almeno un riesame della direzione documentato ed un ciclo completo di audit interni secondo i requisiti della sezione 6 della ISO/IEC 27001:2005 e, infine, deve rispettare le prescrizioni dei paragrafi 8 e 11 del presente regolamento.

L'audit viene effettuato sulla base di un piano di audit concepito in modo tale da tenere conto dell'esito delle attività già svolte (audit di 1° stadio), dando rilevanza agli elementi del SGSI risultati più significativi (valutazione dei rischi per la sicurezza delle informazioni e relativa consistenza dei risultati, selezione degli obiettivi di controllo e dei controlli basati sui risultati di valutazione dei rischi, riesame dell'efficacia del sistema SGSI e misura dell'efficacia dei controlli, implementazione dei controlli, etc.) ; pertanto il piano comprende, in linea di principio, tutti i requisiti della norma di riferimento, ma può anche non includere quei requisiti che sono risultati attuati in modo completamente soddisfacente nel corso dell'audit di 1° stadio.

Tale piano viene anticipato all'organizzazione prima dell'audit.

L'audit per la certificazione ha lo scopo di accertare che il SGSI sia messo in pratica in accordo alla relativa documentazione (policy, procedure, istruzioni, SoA, requisiti di legge, eventuali altri requisiti cogenti, programmi, ecc.) e in maniera efficace, e soddisfi quindi i requisiti della norma di riferimento.

Inoltre il team di audit ha l'obiettivo di verificare che:

- l'analisi effettuata sulle minacce alla sicurezza sia adeguata ai processi dell'organizzazione;
- l'organizzazione abbia stabilito adeguate procedure per l'identificazione, l'esame e la valutazione delle minacce agli asset, vulnerabilità ed impatti, e che la relativa applicazione sia congrua con la politica, gli obiettivi ed i target definiti dall'organizzazione stessa;
- le misurazioni di efficacia dei controlli siano consistenti.

6.7 Emissione iniziale della certificazione e successivi rinnovi

Vale quanto descritto nel Regolamento Generale RGSG.


Il certificato riporterà anche il riferimento al SoA con la relativa data, edizione e/o revisione.

L'emissione della certificazione comporta automaticamente il permesso per l'organizzazione di utilizzare il certificato stesso ed il marchio rilasciato da TÜV Italia, in accordo con le modalità descritte al par. 8 del presente regolamento, unitamente a quanto indicato nel Regolamento Generale RGSG.

6.8 Audit di sorveglianza

Vale quanto descritto nel Regolamento Generale RGSG.

Ognuno degli audit di sorveglianza è relativo a parti del SGSI: esso comprende sempre, in linea di principio, alcuni elementi fissi del SGSI secondo ISO/IEC 27001:2005 (le sezioni da 4 a 8 ed il paragrafo A.15) più ulteriori elementi; tuttavia, nel caso degli eventuali audit di sorveglianza "aggiuntivi" (rif. Paragrafo 6.10 presente documento), gli elementi fissi citati possono non essere oggetto di verifica a giudizio del team di audit; comunque complessivamente gli audit di sorveglianza del triennio coprono almeno una volta l'intero SGSI.

 Italia	<p style="text-align: center;">REGOLAMENTO PARTICOLARE PER LA CERTIFICAZIONE DEI SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI</p> <p style="text-align: center;">Pag. 7 di 9</p>	<p style="text-align: center;">RSSI</p>	<p style="text-align: center;">3^a Ediz.</p>	<p style="text-align: center;">Rev.00</p>
---	--	--	---	--

Al momento di tale audit l'ISMS dell'organizzazione deve dare evidenza dell'esecuzione del riesame della direzione e di un ciclo di audit interni secondo i requisiti della sezione 6 della ISO/IEC 27001:2005 con una frequenza almeno annuale.

Inoltre come minimo, oltre a quanto stabilito nel RGSG, l'audit di sorveglianza ha l'obiettivo di riesaminare :

- l'efficacia del SGSI con riferimento al raggiungimento degli obiettivi stabiliti nella politica SGSI;
- il funzionamento delle procedure per la valutazione periodica della conformità legislativa e normativa;
- le azioni intraprese a fronte di situazioni non conformi rilevate nel precedente audit;
- la gestione di reclami proposti dalle parti interessate all'attenzione di TÜV Italia;
- il programma di audit in funzione delle modifiche intervenute (inclusi asset, vulnerabilità, impatti, aspetti legislativi, richieste o segnalazioni da parti interessate);
- l'uso appropriato del certificato.

6.9 Audit di rinnovo

Vale quanto descritto nel paragrafo 6.9 del Regolamento Generale RGSG.

Al momento di tale audit l'ISMS dell'organizzazione deve dare evidenza dell'esecuzione del riesame della direzione e di un ciclo di audit interni secondo i requisiti della sezione 6 della ISO/IEC 27001:2005 con una frequenza almeno annuale.

6.10 Audit non programmati

Vale quanto descritto nel Regolamento generale RGSG.

7. Registro delle organizzazioni certificate

Vale quanto descritto nel Regolamento Generale RGSG, cui si aggiunge quanto segue:


La sottoscrizione del contratto di certificazione costituisce per TÜV Italia l'autorizzazione per la pubblicazione nel registro dei dati relativi all'organizzazione (salvo che questa ne faccia esplicito divieto a TÜV Italia con apposita comunicazione scritta).

8. Modalità di riferimento alla certificazione - Uso del certificato e del marchio

Vale quanto descritto nel Regolamento Generale RGSG.

Per i sistemi di gestione certificati solo in accordo in accordo alla Norma ISO/IEC 27001:2005, il marchio applicabile, salvo aggiornamenti, è il seguente:



 Italia	<p style="text-align: center;">REGOLAMENTO PARTICOLARE PER LA CERTIFICAZIONE DEI SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI</p> <p style="text-align: center;">Pag. 8 di 9</p>	<p style="text-align: center;">RSSI</p>	<p style="text-align: center;">3^a Ediz.</p>	<p style="text-align: center;">Rev.00</p>
---	--	--	---	--

Nota: nel caso di ulteriori certificazioni di sistema di gestione ottenute con TÜV Italia s.r.l. verrà inviato un marchio specifico che farà riferimento anche agli altri schemi per i quali si è conseguita la certificazione.

9. Sospensione della certificazione

Vale quanto descritto nel Regolamento Generale RGSG.

10. Ritiro / annullamento della certificazione

Vale quanto descritto nel Regolamento Generale RGSG.

11. Gestione dei reclami e delle segnalazioni da parte delle organizzazioni clienti e dalle parti interessate

Vale quanto descritto nel Regolamento Generale RGSG.

Inoltre nello specifico l'organizzazione dovrà evidenziare nella propria procedura di gestione dei reclami le modalità operative relative a:

- Eventuali comunicazioni alle autorità, se richiesto dall'ambito regolamentato.
- Ripristino della conformità
- Prevenzione delle ricorrenze
- Valutazione e mitigazione di qualsiasi incidente relativo alla sicurezza delle informazioni e del suo impatto associato
- Assicurare interazioni soddisfacenti con altri elementi del SGSI
- Verificare l'efficacia dei rimedi/misure correttive adottate

12. Controllo della documentazione del sistema di gestione SGSI e dei rapporti di verifica del TÜV Italia srl

In generale vale quanto descritto nel Regolamento Generale RGSG, ed in particolare si sottolinea che qualora le informazioni contenute nella documentazione siano tali da non poter essere distribuite in forma controllata a TÜV Italia, l'organizzazione è tenuta a comunicare formalmente a TÜV Italia le motivazioni per cui non è possibile effettuare tale distribuzione controllata.

13. Modifiche al sistema di gestione

Vale quanto descritto nel Regolamento Generale RGSG.

L'organizzazione certificata deve informare preventivamente TÜV Italia di qualsiasi modifica sostanziale intenda apportare al proprio SGSI (relativa ad esempio al campo di applicazione, alla Dichiarazione di Applicabilità, all'organizzazione per la sicurezza, alla documentazione sotto controllo di cui al precedente paragrafo 12, ecc.).


TÜV Italia valuta la reale necessità di effettuare, a causa di tali modifiche, un audit addizionale non programmato (vedere par.6.10), eventualmente accompagnato da una revisione del certificato, o di avviare direttamente un iter di certificazione ex-novo.

La non osservanza di tali condizioni può comportare la sospensione del certificato (vedere par.9).

Naturalmente può accadere che sia la stessa organizzazione certificata che, al verificarsi di una o più delle situazioni descritte al primo capoverso, richieda a TÜV Italia una revisione del proprio certificato.

Anche in questo caso TÜV Italia valuta la reale necessità di effettuare, a causa delle modifiche apportate, un audit addizionale non programmato (vedere par. 6.10) o di avviare un iter di certificazione ex-novo.

In tutti i casi i certificati revisionati vengono rilasciati su parere favorevole del comitato di approvazione.

 Italia	<p style="text-align: center;">REGOLAMENTO PARTICOLARE PER LA CERTIFICAZIONE DEI SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI</p> <p style="text-align: center;">Pag. 9 di 9</p>	<p style="text-align: center;">RSSI</p>	<p style="text-align: center;">3^a Ediz.</p>	<p style="text-align: center;">Rev.00</p>
---	--	--	---	--

14. Modifiche alle regole del sistema di certificazione

TÜV Italia ha la facoltà di modificare il proprio sistema di certificazione descritto nel presente regolamento e/o nel Regolamento Generale RGSG (si veda RGSG). In tal caso, però, TÜV Italia consente alle organizzazioni già certificate di presentare osservazioni alle modifiche proposte.

TÜV Italia, una volta decise le modifiche da apportare, specifica la data di entrata in vigore delle modifiche stesse e le conseguenti azioni richieste alle organizzazioni, accordando loro un ragionevole lasso di tempo per adeguarsi.

Qualora un'organizzazione non possa o non voglia adeguarsi a tali nuove regole, TÜV Italia procede al ritiro / annullamento della certificazione (vedere par. 10).

15. Prescrizioni particolari per organizzazioni già certificate da altro organismo

Un'organizzazione avente il sistema di gestione e, in particolare, un sistema di gestione per la sicurezza delle informazioni già certificato da altro organismo di certificazione accreditato, può richiedere anche la certificazione del TÜV Italia.

Vale quanto descritto nel Regolamento Generale RGSG.

16. Riservatezza

Vale quanto descritto nel Regolamento Generale RGSG.

17. Ricorsi (o Appelli)

Vale quanto descritto nel Regolamento Generale RGSG.

18. Reclami nei confronti di TÜV Italia

Vale quanto descritto nel Regolamento Generale RGSG.

19. Contenziosi

Qualora venga avviato un contenzioso con TÜV Italia srl, il foro competente in via esclusiva è quello di Milano.

20. Allegati

Nel presente regolamento sono citati alcuni moduli con la loro sigla identificativa.

Tali moduli sono di seguito allegati:

allegato 1	modulo RLI
allegato 2	modulo SoA

TIMBRO DELL' AZIENDA

Spett.le
TÜV Italia Srl

DICHIARAZIONE DI CONFORMITA' AI REQUISITI COGENTI

(rilasciata in accordo al regolamento di TÜV Italia per la certificazione di SGSI)

L'elenco completo di tutte le leggi, i decreti ed i regolamenti applicabili alla sicurezza delle informazioni gestite nell'ambito del nostro sistema per la sicurezza delle informazioni (SGSI) è il seguente:

- 1.
- 2.
- 3.
- 4.
- 5.

Ecc. ecc.

Dichiariamo inoltre di rispettare tutte le leggi, i decreti ed i regolamenti sopraelencati.

Data: _____

Firma: _____

FACSIMILE

DICHIARAZIONE DI APPLICABILITA' (SoA)

(Edizione XX – Revisione YY del GG/MM/AA)

Identificazione dell'organizzazione:

Campo di applicazione dell'SGSI:

<i>Elenco dei controlli secondo l'allegato "A" della ISO/IEC 27001:2005</i>	<i>Selezionato</i>		<i>Motivazioni della selezione o non selezione di ciascun controllo</i>
	SI'	NO	
<i>Eventuali note integrative:</i> <ul style="list-style-type: none">••			
<i>Eventuali controlli addizionali rispetto a quelli dell'allegato "A" della ISO/IEC 27001:2005 e loro scopo:</i> <ul style="list-style-type: none">••			

Data: _____ Luogo: _____

Firma del responsabile dell'SGSI dell'organizzazione:
