INDICE

Descrizione della revisione	*Regolamento Tecnico RT-37 rev.01 "Prescrizioni per l'accreditamento con scopo di accreditamento flessibile, Dipartimento Organismi di certificazione ed ispezione".* *Riferimento ad estensione ISO/IEC 27701 e ISO/IEC 27006:2015/Amd 1:2020*

	Reparto	Data	Nome	Firma
Preparazione :	CTSSI	2021-06-21	Antonio Bagiolini	*Documento privo di firme in quanto approvato nel sistema di gestione digitale di TÜV Italia Srl*
Verifica :	T&QM	2021-06-25	Stefano Parini	
Verifica :	RQA	2021-06-25	Luca Boniardi	
Approvazione :	MDBA	2021-06-25	Andrea Coscia	

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 nella data 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 secondo la norma internazionale ISO/IEC 27001, nonché secondo linee guida ad essa riferibili, nell'ambito dello scopo flessibile dell'accreditamento SSI.
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 la certificazione di SGSI sono:

- Norma ISO/IEC 27001:2013 "Information technology – Security techniques – information security management systems - Requirements", o la sua versione italiana UNI CEI EN ISO/IEC 27001:2017, nel seguito considerate equivalenti in termini di descrizione dei requisiti ed identificate come "la Norma".
- Norma ISO/IEC 27006:2015 "Information Technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems"
- Norma ISO/IEC 27006:2015+ISO/IEC 27006:2015/Amd 1:2020 "Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems — Amendment 1"
- Norma UNI CEI EN ISO/IEC 17021-1:2015 "Valutazione della conformità - Requisiti per gli organismi che forniscono audit e certificazione di sistemi di gestione"
- Linea guida ISO/IEC 27002:2013 "Information technology- Security techniques – Code of practice for information security controls", o la sua versione italiana UNI CEI EN ISO/IEC 27002:2017.
- Linea guida ISO/IEC 27017:2015 "Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services".
- Linea guida ISO/IEC 27018:2019 "Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors".
- Norma ISO/IEC/ 27701:2019 "Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines"

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

- Regolamento per l'accreditamento degli Organismi di certificazione ed ispezione RG-01
- Regolamento per l'accreditamento degli Organismi di certificazione del sistema di gestione RG-01-01
- Regolamento Tecnico RT-37 rev.01 "Prescrizioni per l'accreditamento con scopo di accreditamento flessibile, Dipartimento Organismi di certificazione ed ispezione"
- Circolare n. 02/2018 "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"
- Circolare n. 01/2019 "Accreditamento schema di certificazione ISO/IEC 27001:2013 con integrazione delle linee guida ISO/IEC 27017:2015 e ISO/IEC 27018:2014 - Information Technology, Security techniques,
- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors"
- Circolare n.10/2019 "Disposizioni in merito all'accreditamento norma ISO/IEC 27701"
- Altre Disposizioni e Regolamenti in materia di accreditamento
- Per avere un riscontro puntuale delle attività svolte sotto accreditamento ACCREDIA, si può consultare direttamente il sito www.accredia.it oppure il sito https://www.tuvsud.com/it-it, dove è possibile prendere visione del certificato di accreditamento con i relativi allegati.

3. Termini e definizioni

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

- ISO/IEC 27000:2018 "Information technology - Security techniques - Information security management systems - Overview and vocabulary".
- UNI EN ISO 9000:2015 "Sistemi di gestione per la qualità – Fondamenti e terminologia";

- UNI CEI EN 45020:2007: "Normazione ed attività connesse – Vocabolario generale".
- UNI CEI EN ISO/IEC 17000:2005 “Valutazione della conformità - Vocabolario e principi generali”

Gli acronimi impiegati nel testo del presente regolamento particolare sono:
- ISMS (Information Security Management System), equivalente a “Sistema di Gestione per la Sicurezza delle Informazioni” (SGSI)
- SoA (Statement of Applicability) equivalente a “Dichiarazione di Applicabilità” (DdA)

Per le definizioni di:
- Carenza (CA)
- Nonconformità (NC)
- Osservazione (OSS):
- Commento (COM)

si veda il Regolamento generale RGSG.

4. Responsabilità

Vale quanto riportato nel Regolamento Generale RGSG, par. 4.

5. Controllo del regolamento

Il presente regolamento particolare è a disposizione degli interessati sul sito internet https://www.tuvsud.com/it-it . In ogni caso le organizzazioni possono richiederne copia in formato cartaceo o digitale.
Inoltre vale quanto riportato nel Regolamento Generale RGSG, par. 5.

6. Iter di certificazione

6.1 Generalità

Vale quanto riportato nel Regolamento Generale RGSG, par. 6.1, con le seguenti integrazioni:

- La Norma riporta nelle sezioni da 4 a 10 una serie di requisiti obbligatori per gli SGSI, che non possono essere cioè oggetto di esclusione.
- 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 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 10 (comprese), nonché dei controlli 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; 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 17021-1 in edizione vigente, nonché dei Regolamenti emessi da ACCREDIA).

- La certificazione secondo ISO/IEC 27001 può essere integrata dalle linee guida ISO/IEC 27017 e ISO/IEC 27018 su richiesta dell'Organizzazione, nel caso in cui il campo d'applicazione del sistema di gestione preveda l'erogazione di servizi in modalità "cloud", e se vengono trattati dati personali in detta modalità. Si precisa che l'integrazione può riguardare la sola linea guida ISO/IEC 27017 o l'abbinamento con la ISO/IEC 27018, ma non la sola ISO/IEC 27018.
- La certificazione secondo ISO/IEC 27001 può essere inoltre integrata dalla ISO/IEC 27701 estendendo lo scopo di applicazione di quest'ultima al perimetro della gestione della Privacy [Privacy Information Management System]. La Norma, essendo una estensione della ISO/IEC 27001 deve tener conto della interpretazione della stessa alla luce della ISO/IEC 27002. Pertanto, l'applicazione della ISO/IEC 27701 non può essere a sé stante, ma deve appoggiarsi all'applicazione delle Norme citate.
- In particolare tale integrazione può essere eseguita sia in caso di nuova certificazione, sia in presenza di una certificazione ISO/IEC 27001 già in vigore, purché emessa da TÜV Italia (in caso contrario, è richiesto il preventivo trasferimento della stessa a TÜV Italia).

6.2 Modalità di svolgimento degli audit e programma di audit

Vale quanto riportato nel Regolamento Generale RGSG, par. 6.2, con le seguenti integrazioni:

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 documenti che contengano informazioni considerate riservate o sensibili (per esempio informazioni relative al personale, ai clienti, ai fornitori, a proprietà intellettuale, alla sicurezza nazionale); in tale caso 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 concordate.

In caso di sistemi di gestione multipli (riferiti cioè a più di una norma certificabile), l'audit può essere eseguito e condurre al rilascio della certificazione, purché tutti i requisiti della norma di riferimento per gli SGSI siano stati soddisfatti, ed inoltre tutte le informazioni documentate siano disponibili, conformi ai requisiti citati, e siano identificate le interfacce con gli altri sistemi di gestione.

6.3 Avvio dell'iter di certificazione

Vale quanto riportato nel Regolamento Generale RGSG, par. 6.3, con le seguenti integrazioni:

La durata dell'audit, sia che coinvolga un sito singolo, che più siti rientranti nel campo di applicazione del SGSI, sarà determinata da TÜV Italia in base alle prescrizioni della norma di accreditamento ISO/IEC 27006 in edizione vigente.
Per audit multisito e audit integrati si fa riferimento rispettivamente ai documenti IAF MD 1 e IAF MD 11.
In caso di audit i cui criteri sono estesi a linee guida incluse nello scopo di accreditamento flessibile (es.: ISO/IEC 27017 e/o ISO /IEC 27018 e/o 27701), la durata dell'audit sarà determinata anche in base alle Disposizioni Accredia pertinenti.

6.4 Visita preliminare (preaudit)

Vale quanto riportato nel Regolamento Generale RGSG, par. 6.4.

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

Vale quanto riportato nel Regolamento Generale RGSG, par. 6.5, con le seguenti integrazioni:

L'audit di 1° stadio sarà eseguito interamente presso l'Organizzazione.

a) Verifica della documentazione del SGSI (1° fase del 1° stadio)
La verifica della documentazione del SGSI viene eseguita sempre, con le eventuali limitazioni dovute ai motivi di riservatezza di cui al paragrafo 6.2.
Per documentazione del SGSI si intende quanto segue:

- i documenti specificati dalla Norma col termine “informazione documentata” (o “documented information”)
- l'elenco dei requisiti cogenti applicabili nell'ambito del SGSI è integrato al rapporto di stadio 1 (RI02). L'attestazione scritta dell’Organizzazione del rispetto di tali requisiti è resa evidente dalla firma del rapporto di stadio 1.

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.
Si sottolinea inoltre che nei suddetti documenti deve essere chiaramente riportato il campo di applicazione del SGSI, 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 Norma 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:
- requisiti delle sezioni da 4 a 10;
- requisiti del paragrafo A.18.

Per ciascuno di tali requisiti, il SGSI 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 2° stadio; l'eventuale permanere di carenze (CA) della documentazione al momento dell’audit 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.

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, par. 6.6, con le seguenti integrazioni:

Al momento dell'audit di 2° stadio l'ISMS dell'organizzazione deve risultare già operativo; in particolare l'organizzazione deve aver definito obiettivi per la sicurezza delle informazioni misurabili e – ove applicabile - quantificati, deve aver eseguito almeno un riesame della direzione documentato ed un ciclo completo di audit interni secondo i requisiti della sezione 9 della Norma 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 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:

- il top management eserciti la leadership con impegno ed efficacia;
- le esigenze derivanti dalle parti interessate – tra cui gli obblighi normativi - siano adeguatamente tenute in considerazione ed ispirino gli obiettivi per l'information security;
- l'analisi effettuata sui rischi per la sicurezza sia adeguata ai processi dell'organizzazione;
- l'organizzazione abbia stabilito adeguate procedure per l'identificazione, l'esame e la valutazione dei rischi per la sicurezza delle informazioni, e che l'applicazione dei controlli operativi sia coerente con la politica, gli obiettivi ed i target definiti dall'organizzazione stessa;
- la documentazione sia conforme alla norma;
- le misurazioni di efficacia dei controlli siano consistenti.

L'audit è anche volto ad accertare che le interfacce con servizi o attività interamente o parzialmente esterne al campo di applicazione del SGSI siano state considerate e quindi incluse nella valutazione del rischio per la sicurezza delle informazioni.

In caso di certificazione estesa a ISO/IEC 27017 e ISO/IEC 27108, questa può essere rilasciata solo dopo una verifica eseguita presso il sito/i siti interessati dell'organizzazione, e in particolare devono essere verificati tutti i data center presso cui sono dislocati i server che gestiscono il cloud.
Se i Data Center utilizzati per le attività "cloud" sono in outsourcing presso fornitori in possesso di certificazioni ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018 accreditate e riconosciute a livello MLA, si potrà evitare di aggiungere tempo di audit presso tali siti. In tutti gli altri casi, dovrà essere aggiunto tempo per la verifica "de visu" dei siti in outsourcing. Nel caso di siti ove non fosse possibile svolgere un audit diretto (es. fornitori come AWS, AZURE), dovrà essere utilizzato del tempo aggiuntivo presso il sito centrale per la valutazione degli aspetti contrattuali e di controllo operativo con tali fornitori. Questo ultimo requisito è applicabile solamente nel caso di Data Center in possesso di certificazioni TIER III o TIER IV.

In caso di certificazione estesa a ISO/IEC 27701, si dovrà inoltre verificare se l'organizzazione si sottopone periodicamente a vulnerability assessment / penetration test, e con quali modalità.

Non è ammessa l'estensione alla ISO/IEC 27701, per organizzazioni che utilizzano servizi erogati con modalità "cloud", senza il supporto della ISO/IEC 27017:2015 e della ISO/IEC 27018.

6.7 Emissione iniziale della certificazione e successivi rinnovi

Vale quanto descritto nel Regolamento Generale RGSG, par. 6.7, con le seguenti integrazioni:

- Il certificato riporterà il riferimento alla Dichiarazione di Applicabilità (SoA) con la relativa data, edizione e/o revisione.
- Inoltre il certificato dovrà essere riemesso anche in fase di sorveglianza, riportando i nuovi riferimenti al SoA, qualora da quest'ultimo documento emerga che è cambiata la copertura dei controlli di cui all'Appendice A della norma.
- In caso di certificazione estesa a linee guida incluse nello scopo flessibile dell'accreditamento SSI di TÜV Italia (es.: ISO/IEC 27017, ISO/IEC 27018 e ISO/IEC 27701), queste saranno citate nel certificato.

6.8 Audit di sorveglianza

Vale quanto descritto nel Regolamento Generale RGSG, par. 6.8, con le seguenti integrazioni:

Ognuno degli audit di sorveglianza è relativo a parti del SGSI: esso comprende sempre, in linea di principio, alcuni elementi fissi del SGSI secondo la Norma (le sezioni da 4 a 10 ed il paragrafo A.18) 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.

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 9 della Norma 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 per la sicurezza delle informazioni;
- 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;
- eventuali cambiamenti nella copertura dei controlli di cui all'Appendice A della norma, e le conseguenti modifiche alla Dichiarazione di Applicabilità;
- l'implementazione e l'efficacia dei controlli secondo il programma di audit;
- la gestione di reclami proposti dalle parti interessate all'attenzione di TÜV Italia;
- il programma di audit in funzione delle modifiche intervenute (inclusi elementi di contesto, rischi, aspetti legislativi, richieste o segnalazioni dalle parti interessate);
- l'uso appropriato del certificato.

6.9 Audit di rinnovo

Vale quanto descritto nel Regolamento Generale RGSG, par. 6.9.

Inoltre, 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 9 della Norma.

6.10 Audit speciali o audit non programmati o eventuale riduzione del campo di applicazione della certificazione

Vale quanto descritto nel Regolamento Generale RGSG, par. 6.10.

6.10.1 Eventuale riduzione del campo di applicazione della certificazione

TÜV Italia ha il diritto di ridurre il campo di applicazione della certificazione per escludere le parti che non soddisfano i requisiti, qualora l'organizzazione abbia mancato, in modo persistente o grave di rispettare i requisiti della certificazione relativamente a quelle parti di campo di applicazione della certificazione. Tale riduzione sarà congruente con i requisiti della norma utilizzata per la certificazione.

7. Registro delle organizzazioni certificate

Vale quanto descritto nel Regolamento Generale RGSG, par. 7.

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

Vale quanto descritto nel Regolamento Generale RGSG, par. 8.
Per i sistemi di gestione certificati solo in accordo alla Norma, il marchio applicabile, salvo aggiornamenti, è il seguente:

Nota: nel caso di ulteriori certificazioni di sistema di gestione ottenute con TÜV Italia potrà essere inviato – se disponibile - un marchio specifico che faccia riferimento anche agli altri schemi per i quali si è conseguita la certificazione.

9. Sospensione della certificazione

Vale quanto descritto nel Regolamento Generale RGSG, par. 9.

10. Ritiro / annullamento della certificazione

Vale quanto descritto nel Regolamento Generale RGSG, par. 10.

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

Vale quanto descritto nel Regolamento Generale RGSG, par. 11.
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.
- Rivalutazione del rischio per la sicurezza delle informazioni.
- Valutazione delle interazioni con altri elementi del SGSI

12. Documentazione o informazioni documentate del sistema di gestione e relativa accessibilità per le verifiche di TÜV Italia srl

Vale quanto descritto nel Regolamento Generale RGSG, par. 12.
Inoltre si sottolinea che qualora le informazioni contenute nella documentazione di sistema e nei rapporti di verifica siano tali da non poter essere distribuite in forma controllata a TÜV Italia o a soggetti terzi, 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, par. 13.

14. Modifiche alle regole del sistema di certificazione

Vale quanto descritto nel Regolamento Generale RGSG, par. 14.

15. Prescrizioni particolari per organizzazioni già certificate da altro organismo

Vale quanto descritto nel Regolamento Generale RGSG, par. 15.

16. Riservatezza

Vale quanto descritto nel Regolamento Generale RGSG, par. 16.

17. Ricorsi (o Appelli)

Vale quanto descritto nel Regolamento Generale RGSG, par. 17.

18. Reclami nei confronti di TÜV Italia

Vale quanto descritto nel Regolamento Generale RGSG, par. 18.

19. Contenziosi

Vale quanto descritto nel Regolamento Generale RGSG, par. 19.

20. Condizioni economiche

Vale quanto descritto nel Regolamento Generale RGSG, par. 20.