ESECUZIONE AUDIT DA REMOTO

Copia controllata n._____1_____

Copia non controllata n._____0_____

REV.	DATA	DESCRIZIONE	REDATTO RGQ	APPROVATO DIR
03	23/02/2026	Riesame generale per transizione alla Ed 2024 della ISO/IEC 27006-1	Francesco Lubrano di Scorpaniello	Salvatore Scutiero
02	29/09/2025	Chiusura Osservazione n. 2 Accredia del 11/12/2024	Francesco Lubrano di Scorpaniello	Salvatore Scutiero
01	22/03/2024	Adeguamento alla ISO 27006	Francesco Lubrano di Scorpaniello	Salvatore Scutiero
00	11/3/2020	PRIMA EMISSIONE	Lucia Esca	Francesco Lubrano di Scorpaniello

INDICE

1. SCOPO 3
2 TERMINI E DEFINIZIONI 3
3 MODALITÀ OPERATIVE 3
3.1.1 Apertura dell'Audit di Certificazione: Riunione di apertura 4
3.1.2 Riunione iniziale interna del GA 4
3.1.3 Esecuzione dell'Audit 4
3.1.4 RIunione finale interna del GA 5
3.1.5 Presentazione dell'esito dell'Audit all'organizzazione e chiusura 5
……3.2 Audit sui sistemi SSI 6

1. SCOPO

Lo scopo della presente Istruzione Operativa è fornire criteri omogenei per l'esecuzione di audit a distanza, anche chiamati audit da remoto, in accordo ai requisiti stabiliti dai seguenti documenti:

- IAF MD4 Issue 2 "MANDATORY DOCUMENT FOR THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) FOR AUDITING/ASSESSMENT PURPOSES", secondo le indicazioni del documento IAF ID12:2015 Issue 1 Version 2 "PRINCIPLES ON REMOTE ASSESSMENT" e secondo la ISO 27006:2021.
- IAF MD29:2024 – Requisiti di Transizione per ISO/IEC 27006-1:2024

2. TERMINI E DEFINIZIONI

Si configurano come tecniche di audit a distanza utilizzabili in alternativa o in combinazione una all'altra:

a. Teleconferenze: video e audio, web meeting, comunicazioni interattive basate sul web (es. Skype, Whatsapp, sia attraverso l'utilizzo dei cellulari sia di computer portatili);
b. Accessi da remoto agli applicativi utilizzati in supporto al Sistema di Gestione dell'Organizzazione (SG);
c. Accessi da remoto agli archivi multimediali delle informazioni documentate del SG;
d. Condivisione sincrona o asincrona dei documenti aziendali di sistema.

3. MODALITÀ OPERATIVE

NON È ACCETTABILE CHE:

Lo sviluppo dell'audit avvenga SOLO su base documentale senza interazione con l'organizzazione.

Un audit si svolga SENZA l'intervista del personale dell'organizzazione;

Siano formulate assunzioni sulla base di audit precedentemente svolti o evidenze di audit eseguiti su altri schemi di certificazione.

Il Responsabile del Gruppo di Audit deve definire nel piano di audit:

- Quali componenti del Gruppo di Audit effettueranno l'audit secondo le tecniche di audit a distanza;
- Quali processi potranno essere sviluppati totalmente o parzialmente da remoto;

- I tempi da dedicare ad ogni processo;
- Le tecniche utilizzate;
- I luoghi presso i quali il team di audit svilupperà l'audit.

La segreteria tecnica dovrà essere informata preventivamente, a mezzo email dall'Organizzazione, sulla volontà di eseguire l'audit a distanza. L'organizzazione deve fornire adeguate motivazioni per la richiesta di esecuzione di audit da remoto; il CAB dovrà comunque dare evidenza di aver valutato ed approvato preventivamente le motivazioni addotte dall'Organizzazione oggetto di audit da remoto, comunicando ufficialmente a mezzo mail detta valutazione.
L'eventuale valutazione della fattibilità di un audit da remoto può essere espressa, a suo insindacabile giudizio, anche dal CAB, e comunicata preventivamente all'Organizzazione valutata, purché siano salvaguardate efficacia ed efficienza dell'audit stesso.
Si raccomanda di effettuare una valutazione del rischio che prenda in esame i seguenti fattori:

- Verificare preliminarmente la competenza dell'organizzazione, oltre che di Certifica, coinvolti in un audit a distanza
- Assicurarsi dell'idoneità degli ambienti e dell'efficacia delle infrastrutture presso l'organizzazione a supporto dell'audit in remoto in termini di infrastruttura disponibile sia di Certifica che dell'Organizzazione Cliente
- Settore in cui opera l'Organizzazione Cliente
- Identificare la Tipologia/e di Audit durante il ciclo di Certificazione dall'Audit iniziale all'Audit di Ricertificazione
- Ambito della Certificazione
- Esecuzione precedente di Audit a distanza per il Cliente

Inoltre

- Chiedere in anticipo all'organizzazione l'autorizzazione per l'acquisizione sia di schermate video (screen shot) per copiare documenti od ogni tipo di registrazione sia di documenti inviati mezzo email/chat, tenendo in considerazione gli aspetti di riservatezza e di sicurezza (security);
- Seguire i protocolli concordati con l'organizzazione per l'eventuale accesso remoto;
- Eseguire un collegamento di prova al fine di assicurarsi del corretto funzionamento dei dispositivi e degli strumenti previsti prima dell'inizio dell'audit e risolvere conseguentemente eventuali problemi tecnici;

Qualora si riscontrassero dei problemi tecnici di comunicazione sospendere l'audit fino alla risoluzione degli stessi e, se necessario, prevedere un'estensione del tempo complessivo di audit;

Assicurare la riservatezza e la privacy durante le pause nelle attività di audit, per esempio silenziando i microfoni o mettendo in pausa le videocamere.

Si precisa che la reportistica di audit è quella inviata con l'incarico e resta invariata rispetto a quella utilizzata abitualmente.

Come per gli audit on-site la durata dell'audit di 1 g-u equivale generalmente a 8 ore lavorative.

3.1.1 Apertura dell'Audit di Certificazione: Riunione di apertura

Attività da eseguire tramite collegamento da remoto (es. Skype – Google Meet o metodi alternativi) accertandosi della presenza contemporanea di tutte le figure coinvolte. La conduzione della riunione iniziale segue le normali prassi. Potrebbe essere ritenuto esaustivo documentare tramite screen shot l'inizio e la chiusura della riunione iniziale, dal momento che mediante questa tecnica di cattura dell'immagine si prende evidenza delle persone collegate, dell'ora e del giorno che sono riportate sul monitor del Pc dell'auditor (RGVI) che conduce la riunione.

3.1.2 Riunione iniziale interna del Gruppo di Audit

Al termine della riunione iniziale con l'organizzazione, RGVI chiude il collegamento con l'organizzazione e riunisce i membri del Gruppo di Audit e assegna loro le attività da svolgere e i mandati personali, al fine di lavorare il più possibile separatamente, coinvolgendo persone diverse dell'organizzazione, ed ottimizzare la raccolta di evidenze oggettive.

Se questa riunione avviene tra persone dislocate in luoghi diversi può essere condotta tramite semplice telefonata o oppure in audio conferenza.

3.1.3 Esecuzione dell'Audit

L'organizzazione oggetto dell'audit deve fornire al Gruppo di Audit la massima collaborazione in tutte le fasi di conduzione dell'audit; per tale motivo deve consentire la comunicazione con le risorse dedicate delle aree in cui si svolgono le attività a cui si riferisce lo schema di certificazione ed il campo di applicazione richiesto per la certificazione del proprio sistema di gestione nonché la possibilità di intervistare il personale coinvolto in tali attività/processi/servizi. L'organizzazione deve inoltre garantire che il Gruppo di Audit sia assistito durante l'audit da personale competente dell'organizzazione.

In questa fase l'auditor controlla documenti e dati con le risorse messe a disposizione in remoto dall'azienda.

La valutazione di conformità alla norma di riferimento è condotta dal Gruppo di Audit seguendo i criteri espressi da procedure, regolamenti, modulistica ed istruzioni operative in uso di Certifica srl-

Sarebbe essere ritenuto esaustivo al fine della dimostrazione della correttezza dell'audit da remoto:

Conservare le mail con le richieste di documenti e il relativo riscontro;

Documentare le interviste e immagini dei luoghi dell'organizzazione sottoposti a visita;

Screen shot di eventuali pagine di documenti che non possono essere acquisiti in maniera completa;

Video effettuati con il proprio smartphone (es. WhatsApp) effettuando degli screen shot del video registrato durante le fasi importanti della verifica eliminando dalle registrazioni tutte quelle fasi che possono compromettere la riservatezza.

Ricordiamo che l'audit come da prassi riguarda:

le informazioni e le evidenze circa la conformità a tutti i requisiti della norma di riferimento o di altra normativa cogente applicabile al sistema di gestione dei processi/prodotti/servizi/attività svolte dall'organizzazione;

il monitoraggio, la misurazione, la rendicontazione e il riesame delle prestazioni, con riferimento agli obiettivi delle prestazioni stesse;

il sistema di gestione dell'organizzazione e le prestazioni con riferimento al rispetto delle prescrizioni legali;

la tenuta sotto controllo dei processi dell'organizzazione;

gli audit interni e il riesame della direzione;

la responsabilità della direzione in riferimento alle politiche del cliente;

i collegamenti fra i requisiti normativi, la politica, gli obiettivi ed i traguardi delle prestazioni, tutte le prescrizioni legali applicabili, le responsabilità, la competenza del personale, le attività, le procedure, i dati di prestazioni e le risultanze e le conclusioni degli audit interni;

le modalità di ricezione e il trattamento degli eventuali reclami pervenuti a carico dell'organizzazione;

il continuo miglioramento del sistema di gestione dell'organizzazione.

L'audit potrà essere condotto a più riprese e con un dialogo necessario con l'organizzazione al fine di chiarire eventuali discrepanze o incongruenze, per stabilire il maggior livello di fiducia sull'applicazione del SG da parte dell'Organizzazione.

Accertarsi di essere stati compresi, e di avere dall'altra parte un'organizzazione con la capacità e l'attitudine a condurre la valutazione a distanza nel mezzo/forum scelto della valutazione a distanza.

Tutte le valutazioni a distanza devono essere concluse con un riassunto, una revisione degli eventi del giorno (o dei giorni), questioni di preoccupazione, chiarimenti su questioni, non conformità e aspettative.

Il valutatore dovrebbe avere la possibilità di interrompere la valutazione prima del programma a causa dell'impossibilità di mantenere collegamenti o condizioni soddisfacenti durante l'orario previsto. Questo dovrebbe essere registrato nel rapporto di valutazione.

3.1.4 Riunione finale interna del Gruppo di Audit

Al termine dell'audit, il Gruppo di Audit analizza nel complesso le risultanze, i dati, le evidenze emerse nel corso dell'audit, al fine di decidere in merito all'esito dell'audit di certificazione. Se questa riunione avviene tra persone dislocate in luoghi diversi può essere condotta tramite semplice telefonata o tramite una call conference.

3.1.5 Presentazione dell'esito dell'Audit all'organizzazione e chiusura

Al termine della riunione del Gruppo di Audit, RGVI convoca una conference call con i rappresentanti dell'organizzazione auditata, una "Riunione di chiusura" con l'ordine del giorno come per l'audit in sede:

L'esito dell'audit di certificazione è documentato e comunicato all'organizzazione da RGVI, mediante la compilazione dei report di audit comprensivi dell'identificazione delle conformità e dei rilievi segnalati.

Nel caso in cui l'Organizzazione Cliente disponesse di pochi o nessun sito fisico rilevante, il Rapporto di Audit ed il documento di certificazione dovranno dichiarare che le attività del Cliente vengono svolte da remoto.

Tale rapporto deve essere condiviso con l'organizzazione prima della lettura ufficiale al fine della corretta comprensione dei rilievi. Conservare le email con l'invio del documento e il relativo riscontro.

Entrambe le parti dovrebbero fare del loro meglio per confermare ciò che è stato ascoltato, dichiarato e letto durante tutta la valutazione.

Se non ci sono correzioni da apportare, la "Pagina Iniziale", attestante l'esecuzione dell'audit e la consegna contestuale dei report di audit in formato elettronico, è inoltrata all'organizzazione tramite mail che la sottoscrive, deve essere sottoscritta dai componenti il Gruppo di Audit e dal rappresentante dell'organizzazione per accettazione.

Entrambe le parti devono adottare misure adeguate per salvaguardare la riservatezza dei dati in qualsiasi formato.

Le immagini non reputate necessarie per fornire evidenza dell'effettuazione dell'audit da remoto, in possesso dell'auditor saranno da eliminare definitivamente.

3.2 Audit sui sistemi SGSI.

La ISO 27006 stabilisce che la percentuale massima per le attività di audit condotti da remoto non devono superare il 30% e, nel caso rappresentassero oltre il 30% del tempo di Audit on site, non sarà più necessario ottenere l'approvazione di Accredia (cfr. IAF MD29:2024 paragrafo 2 lettera c). Il GVI dovrà indicare quali processi e attività saranno visionate in modalità ICT e dovrà indicare quali piattaforme verranno utilizzate e registrare poi l'efficacia del collegamento stesso