AUDIT DA REMOTO

Referente di Schema Ambiente: E. G. Catto

Le disposizioni stabilite dal Governo per contrastare l'emergenza Covid-19 hanno reso impossibile l'effettuazione di Audit da parte di un Team presso la sede delle Organizzazioni.

Per questo motivo risulta opportuno rivedere le procedure ed effettuare gli Audit secondo modalità da remoto per adeguarci ai principi dello smart working.

Per effettuare Audit da remoto è necessario ricorrere alle infrastrutture proprie della tecnologia dell'informazione e della comunicazione.

Le norme internazionali che regolano l'attività di Audit si sono occupate di ICT già da tempo (ICT dall' inglese Information and Communications Technology).

Il documento **IAF MD 4 del 2018 Mandatory Document for the Use of Information and Communication Technology (ICT) for Auditing/Assessment Purposes** ci dà un'ampia panoramica sull'utilizzo di queste tecniche.

Man mano che la tecnologia dell'informazione e della comunicazione diventa più sofisticata, è importante essere in grado di utilizzare le ICT per ottimizzare l'efficacia e l'efficienza dell'audit/valutazione e sostenere e mantenere l'integrità del processo di audit (nel seguito Audit).

Le ICT sono tecnologie per raccogliere, archiviare, recuperare, elaborare, analizzare e trasmettere informazioni. Include software e hardware come smartphone, dispositivi portatili, computer portatili, computer desktop, droni, videocamere, tecnologia indossabile, intelligenza artificiale e altri. L'uso delle ICT può essere appropriato per Audit sia a livello locale che remoto.

Esempi di utilizzo delle ICT durante le attività di Audit possono comprendere, ma non sono limitati a:

- riunioni; mediante strutture di teleconferenza, inclusa la condivisione di audio, video e dati
- audit di documenti e registrazioni mediante accesso remoto, in modo sincrono (in tempo reale) o asincrono (se applicabile)
- registrazione di informazioni e prove mediante registrazioni di video, video o audio
- possibilità di accesso visivo / audio a posizioni remote o potenzialmente pericolose

Gli obiettivi per l'effettiva applicazione delle ICT a fini di Audit sono:

1. fornire una metodologia per l'uso delle ICT sufficientemente flessibile e di natura non prescrittiva per ottimizzare il processo di Audit convenzionale
2. garantire l'esistenza di controlli adeguati a evitare abusi che potrebbero compromettere l'integrità del processo di Audit
3. supportare i principi di sicurezza e sostenibilità

Devono inoltre essere adottate misure per garantire il mantenimento della sicurezza e della riservatezza durante le attività di Audit.

Requisiti di processo
L'organismo deve identificare e documentare i rischi e le opportunità che possono influire sull'efficacia dell'audit per ciascun uso delle ICT alle stesse condizioni, compresa la selezione delle tecnologie, e il modo in cui sono gestite.

Valutazione del rischio
L'auditor deve sempre effettuare una valutazione del rischio in merito all'uso delle ICT prima di ogni audit (utile una check-list da compilare ed allegare ai documenti di audit). Devono essere considerati e documentati i seguenti criteri:

- integrità del processo di Audit e dei suoi risultati
- efficacia ed efficienza dell'Audit, per il raggiungimento dei suoi obiettivi
- rischi per l'obiettività e la validità delle informazioni raccolte
- sicurezza delle informazioni per tutti i soggetti coinvolti nell'Audit
- fattibilità in relazione alla tecnologia selezionata (revisori e clienti)
- ICT condivise e stabili
- buona larghezza di banda per la trasmissione dei dati
- alimentazione affidabile
- continuità e alta qualità del suono/immagine
- competenza ICT delle persone coinvolte

Quando le ICT sono proposte per le attività di audit, la revisione della domanda deve includere un controllo che il cliente e l'organismo di audit dispongano dell'infrastruttura necessaria per supportare l'uso delle ICT proposte.

Considerando i rischi e le opportunità identificati al punto precedente, il piano di audit identifica il modo e la misura in cui le ICT saranno utilizzate a fini di audit per ottimizzarne l'efficacia e l'efficienza mantenendo l'integrità del processo.

Quando si usano le ICT gli Auditor e altre persone coinvolte (ad esempio piloti di droni, esperti tecnici) devono avere la competenza e la capacità di comprendere e utilizzare le tecnologie di informazione e comunicazione impiegate per ottenere i risultati desiderati dell'audit. L'Auditor deve inoltre essere consapevole dei rischi e delle opportunità delle tecnologie di informazione e comunicazione utilizzate e degli impatti che possono avere sulla validità e l'obiettività delle informazioni raccolte.

Se le ICT vengono utilizzate a fini di audit, contribuiscono al tempo di audit totale, ma potrebbe essere necessaria una pianificazione aggiuntiva che potrebbe influire sulla durata totale del processo.
Gli audit da remoto devono essere adeguatamente pianificati, tenendo conto delle loro peculiarità.

La **ISO 19011:2018 al punto A.15 c) Attività di audit virtuali** raccomanda:

- assicurarsi che il gruppo di audit stia utilizzando i protocolli concordati per l'accesso remoto, che comprendono i dispositivi, i software richiesti, ecc.;
- prendere in considerazione gli aspetti di riservatezza e sicurezza, evitando di riprendere persone senza il loro permesso;
- se accade un incidente durante l'accesso remoto, il responsabile del gruppo di audit dovrebbe riesaminare la situazione con l'organizzazione oggetto dell'audit e, se necessario, con il committente dell'audit e raggiungere un accordo circa l'interruzione, riprogrammazione o continuazione dell'audit;
- utilizzare come riferimento planimetrie/diagrammi del sito remoto;
- mantenere il rispetto della privacy durante le pause nelle attività di audit.

Al successivo **punto A.16 Audit di attività e siti virtuali** troviamo poi altre indicazioni:
L'organizzazione oggetto dell'Audit e il gruppo di audit dovrebbero assicurare appropriati requisiti tecnologici per gli Audit virtuali, tra cui:

- inviare in anticipo all'Organizzazione oggetto di audit un elenco dei documenti da rendere disponibili come file per la condivisione sul desktop (o l'invio tramite e-mail;
- chiedere di effettuare la scansione delle registrazioni/documenti non informatizzati per permetterne la condivisione sul desktop;
- condurre verifiche preventive per risolvere eventuali problemi tecnici;
- assicurare che siano disponibili e noti i piani di emergenza (per esempio, l'interruzione dell'accesso, l'utilizzo di tecnologie alternative), prevedendo anche un'estensione del tempo complessivo di audit, se necessario.

La competenza degli auditor dovrebbe comprendere:

- abilità tecniche per l'utilizzo dell'adeguata apparecchiatura elettronica e di altre tecnologie durante l'audit;
- esperienza nella moderazione di riunioni virtuali per la conduzione di audit a distanza.

Nella conduzione della riunione di apertura o nello svolgimento di audit virtuali, l'auditor dovrebbe prendere in considerazione quanto segue:

- valutare i rischi associati agli audit virtuali o a distanza;
- utilizzare planimetrie/diagrammi dei siti remoti come riferimento o ai fini della mappatura delle informazioni elettroniche;
- agevolare la prevenzione di rumori di fondo e di interruzioni;
- chiedere autorizzazione in anticipo per l'acquisizione di schermate video (screen shot), per copiare documenti od ogni tipo di registrazione, prendendo in considerazione gli aspetti di riservatezza e di sicurezza (security);
- assicurare la riservatezza e la privacy durante le pause nelle attività di audit, per esempio silenziando i microfoni o mettendo in pausa le videocamere.

Considerazioni generali
Personale organizzativo e requisiti tecnici

- gli Auditor coinvolti dovrebbero possedere le seguenti caratteristiche:
  - desiderano apprendere e utilizzare il nuovo metodo. Dovrebbero essere tecnologicamente aggiornati;
  - hanno familiarità con l'hardware del cliente utilizzato (ad esempio tablet, fotocamere / webcam) e il software del cliente (strumenti ICT come "WebEx", "GoToMeeting", Skype for Business);
  - dispongono di esperienza di audit sufficienti per utilizzare queste nuove tecniche oltre al loro controllo effettivo;
  - sono anche disposti a "istruire" l'Auditato, promuovendo così questo approccio innovativo.
- l'infrastruttura ICT necessaria è disponibile presso il cliente;
- entrambe le parti (Auditori e Auditato) utilizzano lo stesso software. ICT diversi potrebbero richiedere di più coordinazione;
- la tecnologia di rete del cliente è testata e fornisce una larghezza di banda sufficiente;
- l'Organizzazione valutata e l'Auditor hanno la fiducia reciproca sufficiente per condurre l'audit su questa base;
- questa fiducia viene di solito creata DOPO un audit iniziale (a partire dal primo o dal secondo audit di sorveglianza) o dopo una collaborazione più lunga;
- ci deve essere la consapevolezza che i controlli da remoto possono portare a risultati falsi;
- può esserci solo un numero limitato di partecipanti;
- ci deve essere la consapevolezza che ci si possono aspettare dei limiti tecnici, a

seconda dello strumento utilizzato (ad esempio alcuni strumenti consentono solo cinque webcam alla volta);
- la durata della sessione/colloquio di audit generalmente deve essere di massimo 2 ore. In caso contrario, è necessario programmare interruzioni e/o sessioni aggiuntive.

Aspetti di sicurezza

- tutte le parti interessate sanno che le connessioni via Internet sono meno sicure che durante un audit presso il sito;
- se vengono evidenziati problemi di sicurezza (ad es. Aree riservate o documenti classificati), i controlli da remoto non sono possibili;
- è il cliente/il soggetto auditato che determina il grado di sicurezza richiesto;
- in molte Organizzazioni i dipartimenti di sicurezza richiedono che l'uso degli strumenti per l'acquisizione di immagini sia approvato. Ad esempio, un "permesso di fotografare" specifica esattamente come procedere.

RIFERIMENTI

IAF ID 3: 2011 IAF Informative Document For Management of Extraordinary Events or Circumstances Affecting ABs, CABs and Certified Organizations

IAF MD 4:2018 IAF Mandatory Document for the Use of Information and Communication Technology (ICT for Auditing/Assessment Purposes

IAF MD 5:2019 Determination of Audit Time of Quality, Environmental, and Occupational Health & Safety Management Systems

IAF ID 12:2015 Principles on Remote Assessment

IAF MD 17:2015 Witnessing Activities for the Accreditation of Management Systems Certification Bodies UNI EN ISO 19011:2018 Linee guida per audit di sistemi di gestione

UNI EN ISO/IEC 17021-1:2015 Valutazione della conformità - Requisiti per gli organismi che forniscono audit e certificazione di sistemi di gestione - Parte 1: Requisiti