Nuova versione della ISO 19011 sugli audit

A luglio 2018 è stata pubblicata la nuova versione dello standard internazionale ISO 19011 dal titolo “Guidelines for auditing management systems”. In contemporanea sono state approvate le versioni europea EN ISO 19011 e italiana UNI EN ISO 19011 (“Linee guida per audit di sistemi di gestione”).

Lo standard è dedicato agli audit di prima e seconda parte (audit interni e ai fornitori o ad altre parti esterne interessate), ma è applicabile anche agli audit di certificazione. Come dice il titolo, lo standard riguarda i sistemi di gestione (in particolare quelli descritti da standard quali ISO 9001 e ISO/IEC 27001), però può essere utilizzato come utile riferimento per altri audit, per esempio quelli richiesti dal GDPR.

Questo breve articolo non ha l’intenzione di descrivere completamente la norma, ma solo fornirne alcuni elementi. Se ne consiglia la lettura, in quanto di (relativa) facile lettura.

Le novità

Questa è la terza edizione dello standard (le versioni precedenti erano del 2002 e 2011), resa necessaria dall’approccio basato sul rischio previsto dalle ultime versioni degli standard ISO per i sistemi di gestione.

Nella premessa della versione inglese sono riassunte le novità:

- aggiunta, tra i principi dell’audit, dell’approccio basato sul rischio;
- ampliamento della guida sulla gestione del programma di audit, includendo considerazioni sui rischi;

- ampliamento della guida sulla conduzione degli audit, in particolare sulla loro pianificazione;
- ampliamento dei requisiti generali per le competenze degli auditor;
- miglioramento della terminologia per renderla più orientata ai processi;
- rimozione dei requisiti specifici per le competenze degli auditor (in quanto riportati da altri standard);
- estensione dell'Appendice A (guida di dettaglio) per inserire i nuovi concetti relativi al contesto, leadership and commitment, audit virtuali, conformità e filiera di fornitura.

I principi degli audit

Sin dalla prima edizione, la norma riporta i principi degli audit. Come sopra indicato, è stato aggiunto l'ultimo della lista che segue:

- Integrità (onestà e responsabilità): il fondamento della professionalità;
- Presentazione imparziale: obbligo di riferire in modo veritiero e accurato;
- Dovuta professionalità: l'applicazione di diligenza e giudizio nel corso dell'attività di audit;
- Riservatezza: sicurezza delle informazioni;
- Indipendenza: la base per l'imparzialità dell'audit e l'obiettività delle conclusioni dell'audit;
- Approccio basato sull'evidenza (o "sulle prove"): il metodo razionale per raggiungere conclusioni dell'audit affidabili e riproducibili in un processo di audit sistematico;
- Approccio basato sul rischio (risk-based approach): un approccio all'audit che considera rischi e opportunità.

Il programma di audit

La norma ruota intorno al concetto di “programma di audit”, definito come “Disposizioni per un insieme di uno o più audit pianificati per un arco di tempo definito e orientati verso uno scopo specifico”.

Il programma di audit è spesso inteso come l’insieme degli audit da condurre in un arco temporale pluriennale (solitamente 3 anni, alcune volte anche 5). Esso include ulteriori informazioni, tra cui: gli obiettivi dell’audit, il campo di applicazione degli audit, la frequenza dei singoli audit, le procedure e i criteri (ossia gli standard di riferimento per condurre le valutazioni) da seguire. Il programma di audit deve essere strutturato considerando il contesto in cui dovranno essere condotti gli audit e i relativi rischi.

I rischi relativi al programma di audit includono: l’errata determinazione dell’estensione, numero, durata, siti e programmazione temporale degli audit; dotazioni o competenze insufficienti del responsabile del programma, degli auditor o del gruppo di audit nel suo complesso; inefficaci canali di comunicazione; mancata considerazione della sicurezza delle informazioni; carenze di disponibilità e cooperazione da parte dell’organizzazione oggetto dell’audit.

Il programma deve determinare le risorse umane e materiali per condurre gli audit. In particolare le competenze degli auditor e delle persone coinvolte nel programma, incluso lo stesso responsabile del programma.

La norma specifica poi le attività necessarie all’attuazione del programma di audit (per esempio comunicare il programma alle parti interessate, coordinare temporalmente gli audit, fornire le risorse necessarie e selezionare gli auditor, assegnare il ruolo di lead auditor per ogni singolo audit) e, infine, al suo riesame e miglioramento, in quanto anche il

programma di audit deve essere soggetto al ciclo PDCA.

Conduzione di un audit

Ogni singolo audit previsto dal programma di audit va realizzato.

Per questo la norma descrive le attività necessarie, tra cui:

- contatto con l'organizzazione oggetto dell'audit;
- riesame delle informazioni documentate;
- pianificazione;
- assegnazione di ruoli e responsabilità a guide e osservatori;
- riunione di apertura;
- comunicazione durante l'audit;
- raccolta e verifica delle informazioni (con anche esempi pratici);
- produzione delle risultanze dell'audit (ossia valutazione delle prove raccolte durante l'audit);
- riunione di chiusura;
- preparazione e distribuzione del rapporto di audit (in Italia solitamente il rapporto è consegnato nel corso della riunione di chiusura, ma questo non succede in molti altri Paesi);
- conduzione di eventuali audit straordinari (per esempio in caso di non conformità gravi).

Rischi da considerare relativi alla conduzione di un audit includono: il mancato raggiungimento degli obiettivi di audit a causa di una pianificazione scorretta; la potenziale influenza negativa degli auditor in materia di salute e sicurezza sul lavoro, ambiente e qualità (per esempio, contaminazione di una camera bianca).

Competenze degli auditor

Il capitolo 7 della ISO 19011 è dedicato alle competenze

generali degli auditor. La descrizione delle competenze tecniche specifiche sono demandate ad altre norme. Per esempio, per quanto riguarda la ISO/IEC 27001, alla ISO/IEC 27007 per gli audit di prima e seconda parte e alla ISO/IEC 27006 per gli audit degli organismi di certificazione.

Va detto che i requisiti sulle competenze degli audit sono eccessivi e prevedono capacità e competenze impossibili da trovare in un'unica persona.

Importante è il paragrafo intitolato "Acquisizione della competenza di auditor" perché ricorda che la partecipazione ad un corso o ad un programma di formazione non è condizione né necessaria né sufficiente per ottenere le competenze richieste. Purtroppo negli anni, in quanto più facile da richiedere e verificare, si è affermata la prassi di specificare un numero determinato di ore di corso e di giornate di esperienza per poter considerare competente una persona.

Guida di dettaglio

La norma si chiude con un'appendice con maggiori dettagli su alcune attività di audit (per esempio sulla filiera di fornitura).

Articolo a cura di: **Cesare Gallotti**

L'articolo Nuova versione della ISO 19011 sugli audit proviene da ICT Security Magazine.

https://www.ictsecuritymagazine.com/articoli/nuova-versione-della-iso-19011-sugli-audit/