

L'AUDIT A DISTANZA.**ESEMPIO APPLICATIVO DI ANALISI DEI RISCHI E DELLE OPPORTUNITÀ
DI UN AUDIT REMOTO**

Paolo Calveri - Ispettore Accredia e Delegato italiano in ISO nel Comitato ISO/PC 302 per la revisione della norma UNI EN ISO 19011:2018 "Linee guida per audit di sistemi di gestione"

Ringrazio Marco Cibien - Funzionario tecnico UNI ed Esperto delegato presso ISO/TMBG/JTCG-TF 14 "Revision of the High Level Structure for MSS", per il contributo dato agli aspetti di natura terminologica e di coerenza con i riferimenti tecnico-normativi pertinenti

Sommario

Spunti di riflessione	2
Introduzione e campo di applicazione	3
1. Fonti e riferimenti	3
2. Definizioni applicabili	3
3. Flusso operativo di un audit remoto	4
4. Applicazione pratica del <i>risk based approach/thinking</i> per un audit remoto	5
4.1 Interazione iniziale e valutazione preliminare	6
4.2 Contesto dell'organizzazione e contesto dell'audit	7
4.3 Analisi di rischi e opportunità e decisione di fattibilità dell'audit remoto	14
4.4 Elementi rilevanti del piano e del rapporto di audit remoto	19
5. Conclusioni	21

Spunti di riflessione

Lo scorso aprile il tema dell'audit a distanza è stato trattato da UNI e Accredia sui rispettivi mezzi di comunicazione per presentare il documento "L'audit a distanza. Considerazioni generali, modalità di gestione e spunti operativi"¹ al quale ci ricollegiamo per affrontare gli aspetti più operativi.

Questa "seconda parte", tenendo salde le dovute premesse "teoriche" e i riferimenti normativi già citati nel precedente documento, vuole entrare nel dettaglio pratico fornendo una guida su come poter approcciare l'analisi dei rischi e delle opportunità di un audit remoto.

In coerenza con le norme ISO di sistemi di gestione (ISO MSSs - *Management Systems Standards*) di ultima generazione, basate sull'approccio dei concetti evolutivi riconducibili all'HLS (*High Level Structure*²) si fornisce nel seguito un esempio di modello sperimentale di stima di rischi e opportunità associati all'audit remoto.

Riflettendo su come enfatizzare il concetto che, in generale, la "buona teoria" possa ritenersi davvero tale quando sia ben allineata all'aspetto pratico che tratta, viene naturale pensare al Boeing 777, noto per essere il primo aereo di linea progettato interamente al computer:

"... ci sono 5.000 ingegneri che progettano un aeroplano. È molto difficile per questi ingegneri coordinarsi con pezzi di carta bi-dimensionali o per un progettista che sta progettando un condotto per l'aria condizionata andare da uno che è nelle Strutture e dire: Bene, ecco il mio condotto, si inserisce bene nella tua struttura?

È molto difficile con disegni bi-dimensionali. Perciò, alla fine, ricorriamo a prototipi (fisici) e, onestamente, anche alla linea di assemblaggio finale per terminare l'integrazione. Ed è molto costoso. Ci troviamo un aeroplano che è molto difficile da costruire. La prima volta che le parti si mettono assieme è nella linea di assemblaggio. E non combaciano. Così abbiamo un costo tremendo di rilavorazione sui primi aeroplani, per essere davvero sicuri che tutte le parti combacino correttamente ...".

Chief Engineer, Boeing 777

Fonte: Sabbagh, 1996

¹ Rispettivamente: <https://bit.ly/UNIAuditadistanza> e <https://bit.ly/ACCREDIAuditadistanza>

² ISO/IEC Directives, Part 1, Consolidated ISO Supplement, 2020 Annex SL (normative) Proposals for management system standards, Appendix 2 (normative) High level structure, identical core text, common terms and core definitions.

Introduzione e campo di applicazione

Questo documento è focalizzato su un'applicazione pratica dell'approccio basato sul rischio (*risk-based approach/thinking*) nella pianificazione e conduzione di un audit remoto.

L'ambito operativo del documento utilizza come fonti principali, sempre nei termini descritti, in riferimento al documento già pubblicato a fine aprile 2020 "L'audit a distanza. Considerazioni generali, modalità di gestione e spunti operativi", le seguenti norme:

- UNI EN ISO 19011:2018, "Linee guida per audit di sistemi di gestione";
- UNI CEI 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";
- UNI ISO 31000:2018, "Gestione del rischio - Linee guida".

Inoltre, vengono puntualizzati i seguenti aspetti:

- il modello proposto, pur realizzato per essere coerente con i riferimenti tecnico-normativi ISO pertinenti, in relazione al *risk based approach/thinking*, non è intrinsecamente l'unico applicabile;
- l'utilizzo a cui il modello si è ispirato è prettamente quello legato al mondo del *Conformity assessment*, in particolare agli audit di certificazione di sistemi di gestione; può essere ragionevolmente esteso ad altri tipi di applicazioni che si fondano sui principi generali di audit, come espressi nella norma UNI EN ISO 19011:2018;
- la modalità e i parametri di calcolo della significatività del contesto e dei livelli di rischio sono in fase di validazione, trattandosi di un modello sperimentale la cui valenza, per ora, è prettamente di metodo, senza alcuna pretesa di rigore scientifico. Nei mesi a venire potranno essere proposti i risultati della sperimentazione in atto.

1. Fonti e riferimenti

Si rimanda al documento "L'audit a distanza. Considerazioni generali, modalità di gestione e spunti operativi" (aprile 2020, nel seguito denotato come "documento precedente") punto 1.

I calcoli associati al modello proposto sono effettuati su un "classico" foglio di calcolo elettronico. A tal scopo, possono ovviamente essere utilizzati applicativi analoghi, disponibili in rete e non necessariamente legati a licenze e/o abbonamenti.

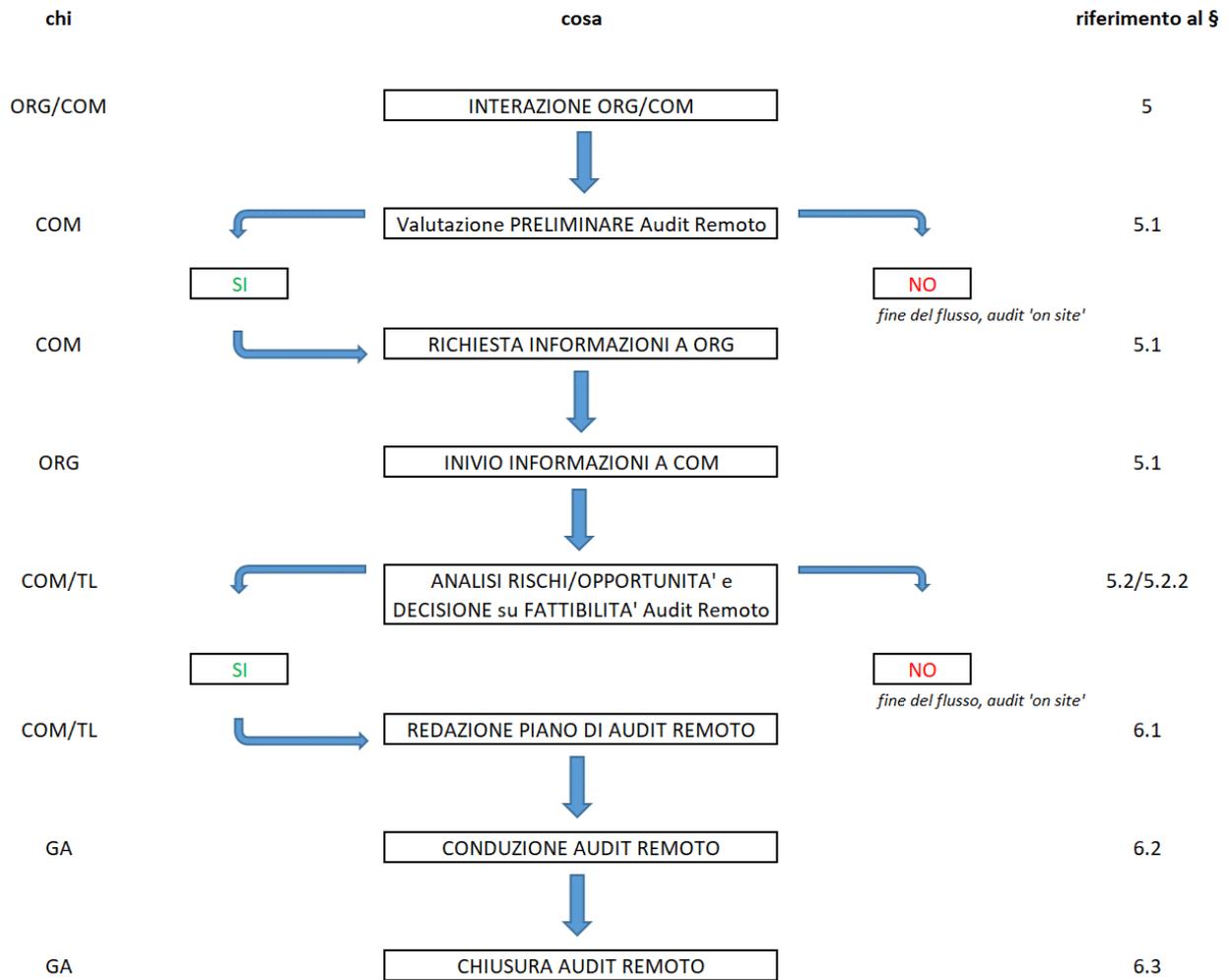
2. Definizioni applicabili

Si rimanda al documento "L'audit a distanza. Considerazioni generali, modalità di gestione e spunti operativi" (aprile 2020), punto 2.

3. Flusso operativo di un audit remoto

Riallacciandoci ai concetti già espressi nell'allegato 1 del documento precedente, si ripropone lo schema decisionale di un audit remoto, espresso nel seguente flow chart:

FLOW CHART OPERATIVO DI UN AUDIT REMOTO (totale/parziale)



LEGENDA:

- COM = committente dell'audit
- ORG = organizzazione oggetto di audit
- TL = team leader del gruppo di audit
- GA = gruppo di audit

4. Applicazione pratica del risk based approach/thinking per un audit remoto

Viene proposto nel seguito, a titolo di esempio applicativo, dunque a carattere non necessariamente esaustivo e/o esclusivo, una modello per determinare il livello di rischio accettabile nel processo di audit remoto.

La metodologia presentata è da ritenersi "sperimentale", nel senso che il modello di calcolo dei livelli di rischio associati al processo di audit remoto è tuttora in fase di affinamento e validazione su casi pratici. In ogni caso, si puntualizza che la valenza del modello è quella di percorrere analiticamente l'approccio all'audit remoto attraverso i seguenti passi:

- analisi del **contesto** (sia dell'organizzazione oggetto di audit, sia del processo di audit stesso);
- rilevazione di elementi di **significatività del contesto** e stima del loro **impatto sui rischi** di audit;
- correlazione di tali elementi in una matrice di rischio che considera i **principi di audit**;
- stima dei **livelli di rischio** e della media generale, per poter poi intervenire riportando le stime dei valori a un livello accettabile.

Il risultato finale del modello, enfatizzando i rischi maggiormente impattanti su efficacia ed efficienza di audit, potrà permettere una decisione consapevole circa la fattibilità dell'audit remoto, mantenendo alta l'attenzione sui fattori che altrimenti, se fuori controllo, potrebbero inficiare le conclusioni stesse dell'audit.

Il *tool* rende agevole la compilazione dei dati necessari alla stima finale del livello di rischio. La prima maschera è la seguente:



Nello specifico, si tratta di un'applicazione pratica secondo le logiche dell'HLS, e, più in particolare, dell'approccio basato sul rischio (*risk based approach/thinking*) per una prima certificazione secondo la norma UNI ISO 45011:2018 di un'organizzazione del settore IAF39, con scopo richiesto della certificazione "Servizio di trasporto rifiuti". Viene quindi ripercorso schematicamente il processo decisionale per l'eventuale audit remoto, totale o parziale, a partire dall'esame della domanda già effettuato a cura del rispettivo CAB.

4.1 Interazione iniziale e valutazione preliminare

Come riportato nel documento precedente (vedi punto 1), una prima interazione tra il committente dell'audit e l'organizzazione oggetto di audit permette una **valutazione preliminare di fattibilità dell'audit remoto**. In particolare, si possono raccogliere le seguenti informazioni, evidenziando gli elementi favorevoli e sfavorevoli per l'effettuazione dell'audit stesso:



INTERAZIONE INIZIALE committente / organizzazione oggetto di audit

COMPILARE DOPO INTERAZIONE INIZIALE CON L'ORGANIZZAZIONE		note (VERDE = punto favorevole, ROSSO = punto NON favorevole)
INTERAZIONE INIZIALE SI/NO per step successivo	<p>aspetti che possono rendere FAVOREVOLE un audit remoto:</p> <p>Aspetti peculiari legati al processo/i da auditare con gli strumenti ICT (per es., opportunità emergenti nell'uso a distanza di localizzatori, droni, strumenti di realtà aumentata, ecc.);</p> <p>Elevato numero di siti con processi simili con comprovata e maturata esperienza da parte del committente dell'audit nella valutazione da remoto di processi a basso rischio;</p> <p>Il committente dell'audit ha disponibile auditor con familiarità con l'organizzazione oggetto dell'audit e con i suoi processi, avendo già auditato il sito 'fisico' della stessa;</p> <p>Aspetti logistici particolari (restrizioni per motivi di sicurezza o per altre esigenze specifiche);</p> <p>Motivazioni personali non prevedibili o sopraggiunte nuove priorità di pianificazione;</p> <p>Impossibilità (o inopportunità) di chiusura di precedenti audit 'on site';</p> <p>Impossibilità di effettuare in tempi ragionevoli visite di follow up di audit 'on site' già effettuati.</p>	<p>non particolari per la sola Fase 1, situazione di emergenza (alternativa era spostare audit, in ogni caso Fase 2 on site più avanti)</p> <p>monosito per uffici, esperienza specifica del TL nel settore. Per il controllo operativo comunque prevista Fase 2 on site</p> <p>è prima certificazione, ma vedi sopra per TL</p> <p>si, emergenza Covid-19</p> <p>NA</p> <p>NA</p> <p>NA</p>
	<p>aspetti che possono rendere SFAVOREVOLE un audit remoto:</p> <p>In fase di valutazione/certificazione iniziale o per estensioni significative di scopo di certificazione (processi e/o siti);</p> <p>Quando è importante assistere direttamente ai processi realizzativi, soprattutto in schemi di certificazione ad alto rischio (Es: verifica cantieri per ISO 9001 settore 28, ISO 45001, ISO 14001)</p> <p>Quando il Sistema di Gestione dell'organizzazione oggetto di audit ha presentato varie non conformità per un periodo di tempo significativo*;</p> <p>Quando non sono state effettuati audit 'on site' per un periodo di tempo significativo*.</p>	<p>prima certificazione. Ma in essere SdG già certificato per ambiente e qualità.</p> <p>controllo operativo da verificare ON SITE, eventuale audit remoto solo per Fase 1 (vedi anche disposizioni Accredia mar20 DCG/2020), entro 6 mesi Fase 2 on site</p> <p>NA</p> <p>NA</p>

Possono essere effettuate ulteriori considerazioni relative alla situazione di emergenza richiamate nel documento IAF ID3:2011:

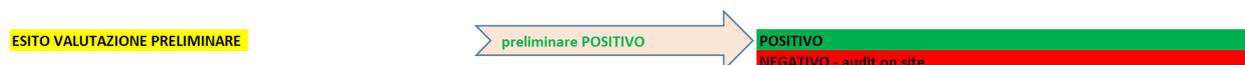
altre valutazioni in relazione a §3 di IAF ID3:2011

AMBITO: In presenza di eventi o circostanze eccezionali occorrerebbe informarsi preliminarmente sull'operatività dell'organizzazione che sta vivendo la situazione contingente, anche per valutare la possibilità di mantenimento della valutazione in essere. Per esempio, potrebbero essere raccolte e gestite le informazioni in merito a:

Piano e criteri per il ripristino di una situazione 'normale';	NA (azienda in attività per tipo di settore, necessità contingente per la comunità)
Tempo massimo di possibile utilizzo dei metodi di valutazione 'da remoto' prima dell'eventuale sospensione o ritiro della certificazione;	NA
Eventuali modifiche ai piani di supervisione dell'organizzazione, valutandole caso per caso e in conformità con le procedure del committente dell'audit;	NA
Garantire che eventuali deviazioni dai requisiti e dalle procedure applicate in regime 'normale' siano giustificate e ricondotte alla situazione contingente;	NA
Ristabilire il ripristino delle attività di sorveglianza/ricertificazione una volta possibile accedere di nuovo al luogo interessato.	NA

In

In funzione delle informazioni descritte, può essere fornito un ESITO della valutazione:



In tal caso, con esito POSITIVO, vengono richieste all'organizzazione ulteriori informazioni per poter poi effettuare l'analisi di contesto/rischi/opportunità:

STEP SUCCESSIVO (se positiva valutazione preliminare)

		informazioni da chiedere all'organizzazione	RIPORTARE SOTTO I DATI FORNITI DALL'ORGANIZZAZIONE
elementi di INGRESSO per ANALISI del CONTESTO	Procedure/istruzioni dell'organizzazione oggetto di audit in relazione alla riservatezza di dati e all'uso di strumenti ICT con interazione di personale esterno (per es., ;	Non presenti particolari procedure in relazione alla riservatezza per l'utilizzo di strumenti ICT, si rimanda all'impegno di riservatezza stabilito a livello contrattuale con l'ente	
	Planimetrie del sito dell'organizzazione;	Allegate	
	Gli strumenti ICT ritenuti più appropriati dall'organizzazione oggetto di audit, compreso la piattaforma di comunicazione preferita;	Hangouts, Skype o Zoom in alternativa	
	Eventuali restrizioni tecniche, legali o contrattuali applicabili per l'organizzazione oggetto di audit;	Nessuna	
	Elenco del personale e dei processi diretti ed indiretti attivi alle date e agli orari di presunta effettuazione dell'audit remoto (compreso le informazioni su indisponibilità totale o parziale del personale, turni, fusi mail e cellulari: xxxxxx/xxxxxx orari, ecc.);	Supporto di 2 persone per tutti i processi gestionali dell'organizzazione – xxxxxx/xxxxxx	
	Competenze relative all'uso degli strumenti ICT delle persone oggetto di possibili interviste;	Buone per le persone che si occupano degli aspetti gestionali dell'organizzazione, previsto supporto per le altre persone	
	Disponibilità in formato elettronico, eventualmente anche preliminarmente all'audit, della documentazione del Sistema di Gestione e possibilità di condivisione di schermi remoti (reciprocamente permettono la condivisione degli schermi tra organizzazione e gruppo di audit);	La documentazione verrà inviata a mezzo mail; e le piattaforme indicate tra organizzazione e gruppo di audit;	
	Riferimento della persona/e dell'organizzazione tecnicamente competente/i per la valutazione preliminare dell'opportuna modalità di gestione della comunicazione da remoto;	La persona che segue i SdG (xxxxx)	
	Possibilità di effettuare tour virtuali degli uffici e reparti oggetto di valutazione.	Sì, con smartphone e/o computer portatile	

4.2 Contesto dell'organizzazione e contesto dell'audit

A seguito della valutazione preliminare di fattibilità, può essere effettuata l'analisi del contesto dell'organizzazione oggetto di audit (*auditee*) e del processo di audit, da cui deriva – secondo le logiche dell'HLS e secondo il nuovo principio di audit di "approccio basato sul rischio" (UN EN ISO 19011:2018, punto 4, g)) – l'analisi dei rischi e delle opportunità.

Il metodo proposto segue lo schema seguente:

dati iniziali dell'organizzazione

NOTE iniziali	prima certificazione. Già in essere SdG ambiente e qualità (con altro OdC)
nome organizzazione	XXXXX SPA
norma di riferimento e settori IAF	UNI ISO 45001: 2018, IAF 39

Si riportano le indicazioni iniziali di compilazione:

Seguire le **istruzioni riportate di seguito** per attribuire ai campi in verde le soglie di significatività dei fattori del contesto dell'organizzazione e del processo di audit. E' possibile modificare per ogni campo i rischi ad esso collegati (vedi sotto elenco rischi secondo § 5.3 della UNI EN ISO 19011:2018.

- 1 per ogni campo verde scegliere la relativa *soglia di significatività* (medù a tendina)
- 2 verificare se coerenti le *corrispondenze tra singolo campo e rischio* (lettere da a) ad h); possono essere scelti più di un rischio
- 3 valutare i calcoli finali delle medie delle significatività del contesto e dove ho maggiore *significatività tra organizzazione e processo di audit*

Ora dovranno essere attribuite le soglie di significatività ai fattori del contesto.

Identificazione dei fattori interni ed esterni del contesto dell'organizzazione e del processo di audit³

In verde si trovano i campi per i quali verrà attribuito un valore di **significatività del contesto**:

descrizione generale organizzazione (info generiche preparatorie all'audit)

ORGANIZZAZIONE OGGETTO DELL'AUDIT	scopo organizzazione
	note certificato
	siti fisici
	processi affidati all'esterno
	lavoro su turni, compreso notturno
	visura camerale
	fattori int/ext (componente fisica, sociale, economica)
	fisica - ambiente naturale/artificiale
	sociale - Aspetti culturali/etici/di sicurezza e protezione/pubblico interesse/fattori demografici
	economica - competizione/reddività/prestazioni/gestione rete di fornitura/partnership/trategie di mercato/gestione economico-finanziaria
parti interessate rilevanti (vedi anche scopo e contesto)	

³ La schematizzazione proposta è ispirata ai Quaderni della Qualità, UNI, N. Gigante, in particolare il Quaderno 2, "Fattori del contesto e parti interessate".

fattori dell'audit

auditor

auditor - comportamento (emotività, attitudine, grado di coinvolgimento)

auditor - esperienza (anzianità di lavoro e esperienza nel settore, gestione tempo e altre variabili)

auditor - conoscenza (formazione di base e successivo mantenimento/miglioramento/estensione)

strumenti e regole di audit

strumenti - appropriatezza del campione (processi campionati, rilevanza dei processi e delle attività correlate, robustezza degli elementi di conformità, grado di dettaglio dell'indagine, documenti, persone intervistate, ecc.)

strumenti - tecniche di audit (osservazioni dirette/indirette, da remoto/on site e relativi strumenti ICT)

oggetto dell'audit

oggetto dell'audit - appropriatezza del campione (processi campionati, rilevanza dei processi e delle attività correlate, robustezza degli elementi di conformità, grado di dettaglio dell'indagine, documenti, persone intervistate, ecc.)

PROCESSO DI AUDIT oggetto dell'audit - accessibilità ai dati (collaborazione e trasparenza auditee, fruibilità dei dati e delle informazioni, accessibilità fisica o virtuale dei siti)

interazione auditor/oggetto dell'audit

interazione auditor/oggetto di audit - interlocutori non appropriati (gestione dei processi comunicativi pre/post audit inadeguata)

interazione auditor/oggetto di audit - comportamenti inappropriati dell'audit team (puntualità, atteggiamento, aspetti etici, ecc.)

fattori ambientali

fattori ambientali - interferenze attive o passive degli auditor sull'ambiente con effetti su comportamento delle persone e sulla conduzione dei processi dell'auditee

fattori ambientali - fattori climatici (pottenziale impatto sulla rappresentatività di quanto osservato)

fattori ambientali - legati all'ambiente 'culturale' (attribuendo valenze improprie a quanto osservato, oppure giustificando situazioni di oggettiva non conformità)

fattori ambientali - condizionamento degli auditor derivanti da soggezione psicologica o pregiudizio negativo dell'auditor

fattori ambientali - interferenza, in presenza o meno, di soggetti esterni al processo di audit (consulenti, osservatori di entrambe le parti, altro)

parti interessate rilevanti (vedi anche scopo e contesto)

Processi critici (rilevanti ai fini dell'audit)

Concetto di significatività dei fattori del contesto associata ai rischi dell'audit

Facendo riferimento ai rischi del programma di audit (ragionevolmente estendibili al piano di audit) espressi nel punto 5.3 della UNI EN ISO 19011:2018, il metodo proposto collega con delle soglie di significatività i fattori del contesto ad uno o più rischi.

Nello specifico, si riepilogano con le rispettive lettere i rischi del punto 5.3 della UNI EN ISO 19011:2018:

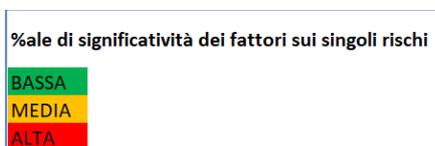
- a pianificazione, per esempio errata definizione di pertinenti obiettivi di audit ed errata determinazione dell'estensione, numero, durata, siti e programmazione temporale degli audit;
- b risorse, per esempio, concedendo tempo, dotazioni e/o formazione insufficienti per sviluppare il programma di audit o per condurre un audit;
- c selezione del gruppo di audit, per esempio insufficiente competenza complessiva per condurre gli audit in modo efficace;
- d comunicazione, per esempio inefficace comunicazione esterna/interna, inefficaci canali/processi di comunicazione;
- e attuazione, per esempio inefficace coordinamento degli audit all'interno del programma di audit, o mancata considerazione della sicurezza e riservatezza delle informazioni;
- f controllo delle informazioni documentate, per esempio inefficace determinazione delle informazioni documentate richieste dagli auditor e dalle parti interessate rilevanti, incapacità di proteggere adeguatamente le registrazioni dell'audit per dimostrare l'efficacia del programma stesso;
- g monitoraggio, riesame e miglioramento del programma di audit, per esempio, inefficace monitoraggio degli esiti del programma di audit;
- h disponibilità e cooperazione da parte dell'organizzazione oggetto dell'audit e disponibilità delle evidenze da campionare.

Per esempio, rispetto al fattore "lavoro su turni, compreso notturno", relativo al contesto dell'organizzazione, la nota dell'esempio è che il lavoro viene effettuato solo sul turno centrale, quindi può essere scelto dal menu a tendina la corrispondente soglia di significatività, con la logica riportata a seguire. Il modello calcola automaticamente i valori medi (vedi il prospetto di significatività riportato nel seguito).

OGGETTO DELL'AUDIT	Note interpretative per DETERMINARE la SIGNIFICATIVITA' del CONTESTO	INSERIRE I COMMENTI PER L'AUDIT SPECIFICO	BASSA - MEDIA - ALTA	*
descrizione generale organizzazione (info generiche preparazione all'audit)		situazione contingente per COVID-19, vedi specifiche disposizioni con effetti sul 'distanziamento sociale'; 15 persone, supporto ext di consulenza sui SOG e RSP, disponibili per interazioni preliminari e documenti vari.		
scopo e settore IAF dell'organizzazione*	Vedi IAF MD5:2019 e categorie di rischio/complessità	Servizio di trasporto rifiuti	MEDIA	x
note su tipo di audit	sovveglianza = BASSA, rinnovo/estensione = MEDIA, nuova certificazione = ALTA	nuova certificazione. Prevedere Fase 2 'on site' entro 6 mesi da Fase 1.	MEDIA	x
siti fisici	monosito = BASSA, più siti con processi non significativi = MEDIA, più siti con processi significativi = ALTA	unico sito con uffici in XXXX	BASSA	x
processi affidati all'esterno	no = BASSA, si e processi poco significativi = MEDIA, si e processi significativi = ALTA	NO (tutti dipendenti)	BASSA	x
lavoro su turni, compreso notturno	centrale/1 turno = BASSA, 2 turni = MEDIA, 3 turni (notturno) = ALTA	2 turni, no notturno	MEDIA	x
visura camerale		vedi doc specifico	BASSA	
fattori int/ext (componente fisica, sociale, economica)	considerare i fattori elencati sotto: fisica - ambiente naturale/artificiale sociale - Aspetti culturali/etici/di sicurezza e protezione/pubblico interesse/fattori demografici economica - competizione/reddività/prestazioni/gestione rete di fornitura/partnership/strategie di mercato/gestione economico-finanziaria	vedi doc di SOG ricevuti, visura, scopo, sito, ambiente circostante	MEDIA ALTA	
parti interessate rilevanti (vedi anche scopo e contesto)	considerare i fattori legati alle parti interessate rilevanti	clienti (tutti pubblici), consumatori e cittadini, azionisti, dipendenti, fornitori, autorità legislative (sicurezza e ambiente), collettività, aziende pubbliche e private limitrofe e vicinato (vedi anche fattori int/ext, visura, scopo, sito e ambiente circostante)	MEDIA	

La percentuale di significatività dei fattori del contesto, parametrizzabile, segue questo criterio, che aumenta, minimizza o resta invariata a seconda della scelta dell'opzione.

Tale soglia di significatività dei fattori di contesto può essere parametrizzata sulla base del giudizio professionale del singolo lead auditor (o di chi effettua l'analisi di rischi e opportunità di audit) ovvero sulla base un approccio statistico strutturato⁴. L'esempio proposto adotta la classica "logica semaforica":



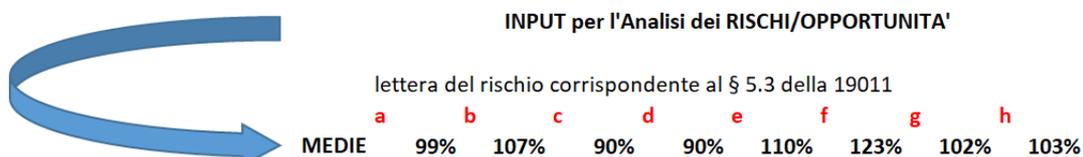
La tabella che associa la significatività dei fattori del contesto con i vari rischi è la seguente (rispettivamente, per il contesto dell'organizzazione e per il contesto del processo di audit); inoltre, è reso evidente che NON verranno effettuate consecutivamente le Fasi 1 e Fase 2, in conformità con le disposizioni recenti applicabili. Quindi, la decisione di fattibilità dell'audit remoto riguarderà solo la Fase 1.

⁴ Vedi anche i possibili futuri sviluppi del modello, Conclusioni

CAMPI CON COLORAZIONE VERDE CHIARO = contributo a significatività del contesto			Significatività dei FATTORI	impatto su rischi:								significatività rischi:							
Note interpretative per DETERMINARE la SIGNIFICATIVITA' del CONTESTO		INSERIRE I COMMENTI PER L'AUDIT SPECIFICO	BASSA - MEDIA - ALTA	a	b	c	d	e	f	g	h	a	b	c	d	e	f	g	h
fattori dell'audit																			
auditor																			
auditor - comportamento (emotività, attitudini, grado di coinvolgimento)	considerare le caratteristiche del gruppo di audit	no evidenza di problematiche precedenti	BASSA	x	x														
auditor - esperienza (anzianità di lavoro e esperienza nel settore, gestione tempo e altre variabili)	considerare le caratteristiche del gruppo di audit	esperienza specifica nel settore (vari audit e su diversi schemi)	MEDIA	x					x										
auditor - conoscenza (formazione di base e successivo mantenimento/miglioramento/estensione)	considerare le caratteristiche del gruppo di audit	formazione continua in essere, vari schemi e ruoli diversi	BASSA	x	x			x											
strumenti e regole di audit	considerare i fattori elencati sotto:	vedi sotto	ALTA	x	x			x											
	strumenti - appropriatezza del campione (processi campionati, rilevanza dei processi e delle attività correlate, robustezza degli elementi di conformità, grado di dettaglio dell'indagine, documenti, persone intervistate, ecc.)	prevedere in Fase 1 soprattutto doc di SdG e conformità, anche formazione (rischio alto), presenza RSPP da riunione iniziale																	
	strumenti - tecniche di audit (osservazioni dirette/indirette, da remoto/on site e relativi strumenti ICT)																		
oggetto dell'audit	considerare i fattori elencati sotto:	doc di sistema ricevuti preliminarmente, favorevoli a parte in remoto	ALTA	x		x		x	x										
	oggetto dell'audit - appropriatezza del campione (processi campionati, rilevanza dei processi e delle attività correlate, robustezza degli elementi di conformità, grado di dettaglio dell'indagine, documenti, persone intervistate, ecc.)																		
	oggetto dell'audit - accessibilità ai dati (collaborazione e trasparenza auditee, fruibilità dei dati e delle informazioni, accessibilità fisica o virtuale dei siti)																		
interazione auditor/oggetto dell'audit	considerare i fattori elencati sotto:	avuta già interazione con persone dell'organizzazione	MEDIA	x	x			x											
	interazione auditor/oggetto di audit - interlocutori non appropriati (gestione dei processi comunicativi pre/post audit inadeguata)																		
	interazione auditor/oggetto di audit - comportamenti inappropriati dell'audit team (puntualità, atteggiamento, aspetti etici, ecc.)																		
fattori ambientali	considerare i fattori elencati sotto:	da ritenere con ALTA significatività per tipologia di attività e gli altri fattori	ALTA	x		x		x											
	fattori ambientali - interferenze attive o passive degli auditor sull'ambiente con effetti su comportamento delle persone e sulla conduzione dei processi dell'auditee																		
	fattori ambientali - fattori climatici (potenziale impatto sulla rappresentatività di quanto osservato)																		
	fattori ambientali - legati all'ambiente 'culturale' (attribuendo valenze improprie a quanto osservato, oppure giustificando situazioni di oggettiva non conformità)																		
	fattori ambientali - condizionamento degli auditor derivanti da soggezione psicologica o pregiudizio negativo dell'auditor																		
	fattori ambientali - interferenza, in presenza o meno, di soggetti esterni al processo di audit (consulenti, osservatori di entrambe le parti, altro)																		
parti interessate rilevanti (vedi anche scopo e contesto)	considerare le parti interessate rilevanti	organizzazione, dipendenti, comunità (dopo Fase 2), OdC, fornitori e clienti dell'organizzazione, autorità legislative	MEDIA							x									
Processi critici (rilevanti ai fini dell'audit)	considerare gli eventuali processi critici	Fase 1, analisi informazioni documentate di SdG, verifica aspetti legislativi (anche Covid-19), interazione dell'organizzazione con le parti interessate ext (aspetti ambientali) e int (rischio biologico ed operativi-macchine)	ALTA	x				x	x										
				valori medi								105%	114%	80%	100%	130%	130%	103%	115%
				valore medio SIGNIFICATIVITA' - CONTESTO del processo di audit								110%							

Il risultato finale delle stime delle soglie di significatività dei fattori del contesto correlate ai rischi può essere quindi riportato nel prospetto seguente, in cui viene fatta la media dei 2 contesti:

Valori medi contesto ORGANIZZAZIONE	92%	100%	100%	80%	90%	115%	100%	90%
Valori medi contesto del processo di AUDIT	105%	114%	80%	100%	130%	130%	103%	115%

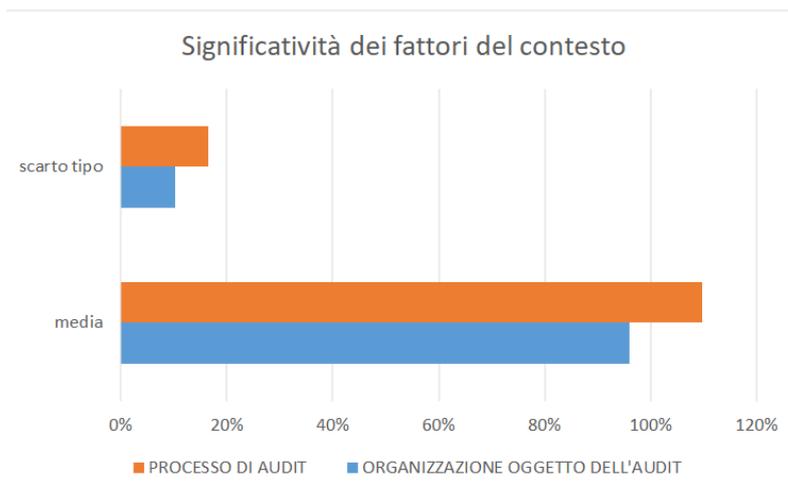


Inoltre, avendo calcolato separatamente per contesto di organizzazione e processo di audit i valori delle soglie di significatività (single e medie) e i rispettivi scarti tipo (*standard deviation*), il modello propone la sintesi dei risultati come da grafico seguente⁵:

Sintesi di significatività dei fattori del contesto

	media	scarto tipo
ORGANIZZAZIONE OGGETTO DELL'AUDIT	96%	10%
PROCESSO DI AUDIT	110%	17%

valore medio SIGNIFICATIVITA' - CONTESTO dell'organizzazione	96%
valore medio SIGNIFICATIVITA' - CONTESTO del processo di audit	110%
scarto tipo SIGNIFICATIVITA' - CONTESTO dell'organizzazione	10%
scarto tipo SIGNIFICATIVITA' - CONTESTO del processo di audit	17%



Nel caso trattato, si evidenzia una maggior significatività dei fattori legati al contesto del processo di audit, sia per i valori medi, sia per gli scarti tipo (*standard deviation*). Questi dati potranno orientare gli auditor a porre ancora maggiore attenzione al processo di audit.

A questo punto, è possibile stimare il livello di rischio complessivo dell'audit.

⁵ Come già anticipato e ribadito anche nelle Conclusioni, i parametri e le formule del modello sono da ritenersi, per ora, sperimentali.

4.3 Analisi di rischi e opportunità e decisione di fattibilità dell'audit remoto

Come riportato nel documento precedente (punto 5.2.2 Analisi di rischi e opportunità dell'audit remoto), l'analisi dei rischi e delle opportunità permette di valutare un livello accettabile di rischio come input alla decisione consapevole circa la fattibilità dell'audit, mantenendo il focus su efficacia ed efficienza del processo di audit stesso.

Nel modello proposto, i fattori di significatività del contesto precedentemente valutati vengono ora utilizzati per procedere con la stima del livello complessivo di rischio dell'audit stesso.

Riferimento per l'analisi dei rischi: ISO/IEC 17021-1 § 4.8 e 9.4 e contributo analitico della UNI EN ISO 19011, § 5.3

significatività dei FATTORI del CONTESTO (organizzazione e audit)

S _c	elenco rischi (UNI EN ISO 19011, §5.3)		evidenziati quelli più significativi per audit remoto (totale/parziale)		P	G	Rischio R ₀	Rischio R
99%	a	pianificazione, per esempio errata definizione di pertinenti obiettivi di audit ed errata determinazione dell'estensione, numero, durata, siti e programmazione temporale degli audit;			1	3	3,0	3,0
107%	b	risorse, per esempio, concedendo tempo, dotazioni e/o formazione insufficienti per sviluppare il programma di audit o per condurre un audit;			1	3	3,0	3,2
90%	c	selezione del gruppo di audit, per esempio insufficiente competenza complessiva per condurre gli audit in modo efficace;			1	3	3,0	2,7
90%	d	comunicazione, per esempio inefficace comunicazione esterna/interna, inefficaci canali/processi di comunicazione;			2	3	6,0	5,4
110%	e	attuazione, per esempio inefficace coordinamento degli audit all'interno del programma di audit, o mancata considerazione della sicurezza e riservatezza delle informazioni;			2	3	6,0	6,6
123%	f	controllo delle informazioni documentate, per esempio inefficace determinazione delle informazioni documentate richieste dagli auditor e dalle parti interessate rilevanti, incapacità di proteggere adeguatamente le registrazioni dell'audit per dimostrare l'efficacia del programma stesso;			2	4	8,0	9,8
102%	g	monitoraggio, riesame e miglioramento del programma di audit, per esempio, inefficace monitoraggio degli esiti del programma di audit;			1	3	3,0	3,1
103%	h	disponibilità e cooperazione da parte dell'organizzazione oggetto dell'audit e disponibilità delle evidenze da campionare.			2	3	6,0	6,2
media							4,8	5,0

probabilità
gravità
R₀ = valutazione livello di rischio
R = valutazione livello di RISCHIO calcolato con la significatività del CONTESTO

In particolare, per l'audit remoto, sono stati evidenziati i rischi prevalenti, ossia quelli associati alle lettere: c), d), e), f) ed h).

Inoltre, si specificano le lettere delle formule:

- P = probabilità del verificarsi dell'evento;
- G = gravità/impatto delle conseguenze derivanti;
- R₀ = P * G, valutazione del livello di rischio (senza il contributo dei fattori del CONTESTO);
- R = R₀ * S_c, valutazione livello di RISCHIO calcolato moltiplicando R₀ per la significatività del CONTESTO.

Come si vede dall'esempio, non vi sono grosse variazioni dei rischi tranne che per il rischio f) (*controllo delle informazioni documentate, per esempio inefficace determinazione delle informazioni documentate richieste dagli auditor e dalle parti interessate rilevanti, incapacità di proteggere adeguatamente le registrazioni dell'audit per dimostrare l'efficacia del programma stesso*) che da **ARANCIO = 8** diventa **ROSSO = 9,8**.

Le scale delle probabilità e delle gravità degli eventi associati ai rischi sono:

scala PROBABILITA' P	
improbabile	Indica scarsissima probabilità del verificarsi dell'evento per la mancanza della presenza oggettiva del rischio in esame. Non sono noti episodi già verificatisi. Assenza di criteri oggettivi nell'individuazione del livello delle probabilità. Il verificarsi dell'evento susciterebbe incredulità.
occasionale	Indica la scarsa possibilità del verificarsi dell'evento. Sono noti rarissimi episodi già verificatisi o che sarebbero potuti accadere. Scarsa presenza di criteri oggettivi nell'individuazione del livello delle probabilità. Il verificarsi dell'evento ipotizzato susciterebbe grande sorpresa.
probabile	Indica la possibilità concreta del verificarsi dell'evento. È noto qualche episodio associato al verificarsi dell'evento. Presenza di criteri oggettivi nell'individuazione del livello delle probabilità. Il verificarsi dell'evento ipotizzato susciterebbe una moderata sorpresa.
molto probabile	Si sono già verificati episodi correlati all'evento in situazioni operative simili. Alta presenza di criteri oggettivi nell'individuazione del livello delle probabilità.

scala GRAVITA' G	
lieve	Evento di scarsa entità , con conseguenze facilmente contenibili.
media	Evento di media entità , che permette un'agevole gestione nel corso dell'audit.
grave	Evento di grave entità , che impatta l'efficienza e lo svolgimento dell'audit.
gravissima	Evento di grave entità , che impatta fortemente efficacia ed efficienza dell'audit con coinvolgimento del committente e potenziale sospensione dell'audit stesso.

I colori associati ai rischi seguono la legenda seguente, con la rispettiva matrice 4x4 (spesso denominata *risk map* o *heat map*):

$$R = P \times G$$

R = indice del rischio;
 P = probabilità del verificarsi dell'evento;
 G = gravità/impatto delle conseguenze derivanti.

R = VALUTAZIONE RISCHIO RANGE

MOLTO BASSO	1-2
BASSO	3
MEDIO	4-9
ALTO	9-16

P				
4	8	12	16	
3	6	9	12	
2	4	6	8	
1	2	3	4	
				G

Una volta calcolato il rischio R – che, come più volte ricordato, tiene conto della significatività del contesto dell'organizzazione oggetto di audit e del processo di audit stesso –, il modello proposto **collega tali valori ai principi di audit**, introducendo il coefficiente S' di significatività del rischio e incrociando i rischi delle lettere da a) ad h) ai principi indicati nella UNI EN ISO 19011:2018 e nella ISO/IEC 17021-1:2015; il modello prevede quindi, a seconda della sensibilità del singolo lead auditor (o di chi effettua l'analisi di rischi e opportunità di audit), di correlare il singolo rischio a uno o più principi di audit attribuendogli una maggior significatività, in modo da poter eventualmente incrementare il valore del rischio stesso e rendendo evidente anche visivamente e numericamente l'opportunità di attuare delle azioni di mitigazione.

Nel prospetto seguente si trova la matrice della significatività dei rischi, associata ai principi e il nuovo valore di rischio R':

Come si nota, l'introduzione della significatività dei rischi, nel nostro caso, ha permesso di enfatizzare la "rilevanza" associata ai rischi d) ed f) che, evidentemente, dovranno essere oggetto di approfondimento e gestione per non compromettere efficacia ed efficienza di audit.

- rischio d) (comunicazione, per esempio inefficace comunicazione esterna/interna, inefficaci canali/processi di comunicazione) correlato ai principi della UNI EN ISO 19011:2018 della presentazione imparziale e dell'approccio basato sull'evidenza;
- rischio f) (controllo delle informazioni documentate, per esempio inefficace determinazione delle informazioni documentate richieste dagli auditor e dalle parti interessate rilevanti, incapacità di proteggere adeguatamente le registrazioni dell'audit per dimostrare l'efficacia del programma stesso) correlato al principio della ISO/IEC 17021:2015 della riservatezza.

Il risultato di queste valutazioni porta ad una stima di rischi per così dire "maggiorati" per l'audit remoto, che possono alzare i valori di rischio anche oltre quelli della tabella iniziale (vedi matrice P*G). Il tal modo, sarà ora possibile formalizzare schematicamente delle azioni di trattamento e mitigazione dei rischi (in coerenza, ad esempio, con il framework proposto dalla UNI ISO 31000:2018, punto 3.1, nota 3), permettendo di riportare le stime dei livelli di rischio entro valori più accettabili:

R' (rischio con significatività) R' = prodotto R*S	AZIONI SUI RISCHI				DESCRIZIONE AZIONE	nuova probabilità dopo AZIONE di MITIGAZIONE	R'' (rischio calcolato dopo azione) R'' = R'*Cr
	EVITARE	TRASFERIRE	MITIGARE	ACCETTARE			
3,0			X			1	3,0
3,2			X			1	3,2
2,7			X			1	2,7
7,8		X			uso ICT consueto/accortezze sia su piano audit sia audit report, prove tecniche preliminari	1	3,9
6,6		X			accortezza operativa di gestione delle informazioni nella conduzione dell'audit	1	3,3
16,9		X			ricevimento in anticipo vari doc di SdG, conferma policy x registrazioni e uso dati	1	8,5
3,1			X			1	3,1
6,2		X			verifica preliminare vari doc di sistema, puntualizzazione per rispetto ruoli	1	3,1
media						media	3,8

Il nuovo rischio calcolato, finale, sarà R'', evidentemente ridotto in funzione delle eventuali azioni di trattamento (mitigazione) e delle aggiornate probabilità corrispondenti al rischio specifico⁶.

Come si vede, le azioni di mitigazione attuate sui rischi "ARANCI" e "ROSSI" riducono il valore medio da 6,2 a 3,8, quindi ad un livello accettabile, secondo il seguente criterio:

livello di RISCHIO R''	AZIONE DI CONTENIMENTO
MOLTO BASSO	Nessuna azione specifica, redazione AUDIT PLAN
BASSO	Nessuna azione specifica, redazione AUDIT PLAN con focus sui valori di rischio più alti
MEDIO	Focus rischi su AUDIT PLAN e monitoraggio durante conduzione audit degli aspetti correlati alle fonti di rischio
ALTO	Predisposizione di azioni sui rischi, SCONSIGLIATO L'AUDIT con le condizioni attuali, da ricercare soluzioni alternative

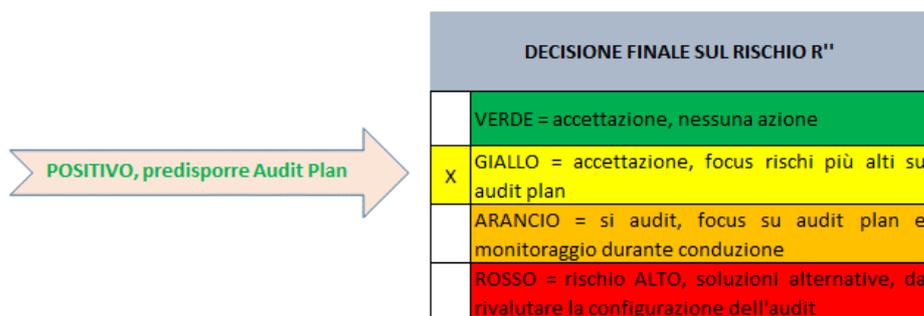
Rimangono in ogni caso "sotto osservazione" eventuali rischi ancora "rossi" dopo le azioni di mitigazione; questo permetterà agli auditor di monitorare gli aspetti correlati a tali rischi durante la conduzione dell'audit.

Si sottolinea che a seguito delle azioni sui rischi più rilevanti sono stati considerati possibili rischi emergenti, per questo caso non rilevati (vedi sotto).

EVENTUALI RISCHI EMERGENTI DOPO LE AZIONI SUI RISCHI

Non rilevati.

Inoltre, il modello permette la formalizzazione della decisione consapevole di fattibilità dell'audit per la sola Fase 1, come già rilevato nell'analisi del contesto, vedi sotto:



Per quanto riguarda le opportunità, sempre in coerenza con il documento precedente, il riferimento rimane il punto 5.3 della UNI EN ISO 19011:2018. Il modello proposto permette, parallelamente alla gestione e valutazione dei rischi, di rilevare eventuali opportunità associate all'audit remoto.

⁶ l'attuale revisione del modello prevede l'aggiornamento delle sole probabilità, seppure le logiche della UNI ISO 31000:2018 prevedano che le azioni di trattamento possano eventualmente anche incidere sulla gravità del rischio

Nel caso specifico, sono evidenziate le seguenti:

elenco opportunità (§5.3 UNI EN ISO19011:2018)	sottolineate quelli più significativi per audit remoto (totale/parziale)	descrizione opportunità perseguibili
	1 permettere la conduzione di audit multipli all'interno di una sola visita; 2 <u>minimizzare i tempi e le distanze di viaggio per raggiungere il sito;</u> 3 adeguare il livello di competenza del gruppo di audit al livello di competenza richiesto per raggiungere gli obiettivi dell'audit; 4 <u>allineare le date degli audit alle disponibilità del personale chiave dell'organizzazione oggetto dell'audit.</u>	x perseguibile, anche in relazione a situazione contingente x perseguibile, coordinamento con le persone dell'auditee con varie interviste e campionamenti da remoto
altre opportunità	5 <u>migliorare efficacia ed efficienza di audit.</u>	x perseguibile, sono disponibili preliminarmente vari documenti del SdG, potendo effettuare valutazioni prima della riunione iniziale. Inoltre, maggior flessibilità per le interviste del personale coinvolto

4.4 Elementi rilevanti del piano e del rapporto di audit remoto

Ribadendo quanto già espresso nei punti 6.1 e 6.2 del documento precedente (vedi 6.1 Redazione del piano di audit remoto e 6.3 Conclusioni, chiusura e rapporto dell'audit remoto), si riportano sinteticamente, a titolo esemplificativo, le evidenze descritte nella documentazione pertinente. Resta inteso che le informazioni proposte dovrebbero essere aggiunte a quelle già previste.

Le informazioni elencate nel seguito possono essere riportate, rispettivamente, nel piano e nel rapporto di audit (l'esempio riportato è generico, non necessariamente riferibile al caso presentato nelle pagine precedenti).

Piano di audit

Nel piano di audit potrebbero essere riportate le indicazioni seguenti:

- **Piattaforma di comunicazione:** per l'intero campionamento dei processi, MicroXXX Teams, come concordato, versione mobile su smartphone per il tour virtuale dei reparti operativi; in caso di caduta linea, comunicazione via SkyXXX con computer/smartphone o "classica" con cellulare;
- **Pause con disconnessione:** orientativamente 10min/ora di audit (a parte pause pranzo);
- Attività con esigenze di **interruzione della comunicazione:** tempo del team di audit per analisi dei dati, sono evidenziate in verde nel piano di audit;
- **Gestione dei dati** eventualmente acquisiti: screenshot di videate, registrazioni audio/video, ecc. NON saranno effettuati se non dietro richiesta motivata e relativa ed eventuale autorizzazione; in tal caso, i dati saranno eliminati entro 5gg lavorativi dalla data della delibera/decisione di certificazione o della conferma del mantenimento della certificazione;
- Eventuali **problematiche nell'interazione remota:** in caso di evidenti difficoltà tecnico/operative, l'audit potrebbe essere sospeso e riprogrammato, totalmente o in parte.

Rapporto di audit

Nel rapporto di audit potrebbero essere riportate le indicazioni seguenti:

- L'audit di sorveglianza secondo la norma XXXXXXXXXX effettuato per l'organizzazione XXXXXX è stato condotto, con il criterio del campionamento dei processi, seguendo il piano di audit previsto;
- L'audit è stato effettuato completamente in remoto, secondo i **protocolli di comunicazione concordati** (vedi piano di audit), con condivisioni reciproche degli schermi dei computer e nel **rispetto delle policy di riservatezza applicabili**. Nel corso dello svolgimento dell'attività di audit **NON sono stati effettuati screenshot, né registrazioni audio o video** da parte del team di audit; risulta un **comportamento "simmetrico"** anche da parte delle persone intervenute nell'audit per conto dell'organizzazione;
- Gli **strumenti ICT** utilizzati sono stati: rispettivi computer del gruppo di auditor e delle persone intervistate per conto dell'organizzazione con reciproca condivisione dei monitor, secondo i processi riportati nel piano di audit, con annesse webcam, cuffie e microfoni, smartphone;
- Non si sono verificate **problematiche di comunicazione** nell'uso degli strumenti ICT previsti, né si rilevate **inefficienze e/o perdite di tempo** dovute al collegamento con le varie persone coinvolte.
- Tenendo conto del momento contingente e della situazione di operatività parziale delle attività dell'organizzazione **sono stati effettuati tour virtuali solo di alcuni reparti operativi**, potendo comunque campionare i documenti previsti ed effettuare le interviste alle persone, secondo il piano di audit. Si è inoltre avuta **visione in riunione iniziale e finale tramite webcam di parte degli uffici della direzione e dell'area commerciale**, essendone i responsabili collegati in remoto dal sito operativo.
- **L'efficacia nel raggiungimento degli obiettivi di audit non è stata inficiata dall'uso degli strumenti ICT**. Inoltre, al termine delle raccolte delle evidenze oggettive dei processi campionati, **la comprensione delle informazioni scambiate è stata reciprocamente confermata**, compreso i rilievi e le conclusioni dell'audit.

5. Conclusioni

L'obiettivo di questo documento operativo, che si collega a quello precedentemente pubblicato, è rendere disponibile una guida pratica di applicazione delle logiche riferibili all'HLS e alla UNI EN ISO 19011:2018, con specifico riferimento all'applicazione dell'approccio basato sul rischio (*risk-based approach/thinking*) e alla conseguente valutazione dei rischi e alle opportunità associabili agli audit da remoto, in particolare, di terza parte.

Viene ribadito che il modello proposto:

- ha una sua natura "sperimentale" e intrinsecamente non esaustiva, essendo la sua finalità quella di proporre uno strumento pratico per tenere sotto controllo i fattori di maggior possibile impatto sull'efficacia ed efficienza dell'audit remoto;
- con i dovuti adattamenti, potrebbe essere ragionevolmente applicato anche ad audit tradizionali in presenza;
- a oggi viene già utilizzato da vari auditor per diverse tipologie di audit, norme e settori; pertanto, una volta disponibile un campione sufficientemente significativo di "casi di studio", eventualmente con ulteriori e significativi contributi, lo step successivo potrebbe essere quello di affinare e validare lo strumento.