Appendice A

Gestire gli auditor

Amor, ch'a nullo amato amar perdona,
mi prese del costui piacer sì forte,
che, come vedi, ancor non m'abbandona.

Dante Alighieri, *Inferno* Canto V

Questo libro non approfondisce come programmare, pianificare e condurre un audit, né come riportare le evidenze e le risultanze di audit. Per comprendere veramente come si gestiscono gli audit si consiglia di leggere libri dedicati a questo argomento [35], partecipare a corsi di formazione e, soprattutto, affiancare persone esperte durante gli audit.

Il rapporto con le persone da intervistare è spesso complesso perché vi è sempre un misto di timore e cautela da parte sia dell'auditor sia delle persone dell'organizzazione oggetto dell'audit. Raramente si tratta di un rapporto conflittuale, ma richiede comunque cautela.

Un auditor si trova spesso in imbarazzo a dover affrontare persone sconosciute, nei confronti delle quali deve erogare un servizio che richiede una certa durezza. Ciascun auditor impara con il tempo a gestire questi rapporti, anche in funzione del proprio carattere e delle proprie attitudini; alcuni si dimostrano molto distaccati, altri più amabili, altri molto rigorosi.

Quando un'organizzazione incontra un auditor, il timore, la curiosità, il rispetto professionale e i dubbi sulle sue competenze sono elementi tra loro conflittuali che rendono non sempre semplice il rapporto e, anzi, molto stancante, anche quando l'audit si svolge in modo sereno e senza che siano rilevate non conformità o punti di attenzione.

Questo è vero anche per l'auditor: tutto il giorno è seguito da persone attente a ogni suo movimento e a ogni sua domanda, ha sempre il dubbio di essere inadeguato e timoroso delle reazioni degli intervistati se venissero rilevate delle non conformità.

Il timore di inadeguatezza dell'auditor è determinato dalla consapevolezza di non essere pienamente competente su tutti i campi di indagine, mentre le persone intervistate sono invece molto competenti nel loro settore. Un auditor di sicurezza delle informazioni deve poter discutere di sicurezza fisica, sicurezza dei sistemi, sicurezza della rete, sicurezza delle applicazioni; non può conoscere in

modo approfondito tutti questi temi, anche considerando le numerose tecnologie disponibili.

Spesso, soprattutto agli inizi di un audit, le persone intervistate possono avere dei dubbi sulle competenze dell'auditor perché fa domande o affermazioni non sempre pertinenti. Può anche far sorridere quando chiede spiegazioni su argomenti ritenuti banali da parte degli operatori. Si deve però tener conto che un auditor, se non è interno, ha rapporti con tante organizzazioni, ciascuna con il proprio gergo e le proprie tecnologie.

Questa appendice tratta di come gestire un auditor, tema quasi mai trattato da testi, convegni o altro. Si fa riferimento agli auditor esterni, ma alcune regole sono applicabili anche a quelli interni. Inoltre, quanto detto non è sempre applicabile quando l'auditor è un rappresentante di un'Autorità pubblica o delle Forze dell'ordine.

Per illustrare come gestire un auditor, si considerano le sue quattro nature: ospite, partner, fornitore e... auditor.

A.1 L'auditor è un ospite

Come per ogni ospite dell'organizzazione, è buona norma offrire all'auditor caffè e acqua e chiedere se ci sono problemi in merito al condizionamento o riscaldamento dell'eventuale stanza messa a sua disposizione.

L'auditor, quando opera presso l'organizzazione, non è nel proprio ufficio e quindi, se questo non presenta conflitti con le regole dell'organizzazione, è comune cortesia mettergli a disposizione una connessione a Internet (oltre alle regole da seguire, come per ogni altro ospite) e permettergli di fare qualche fotocopia, purché pertinente lo scopo della visita.

Per gli auditor devono essere osservate le misure di sicurezza applicabili agli ospiti e, per esempio, devono essere sempre accompagnati.

Se l'auditor è un esterno, in particolare di un organismo di certificazione, ed è da solo, è buona norma organizzare un pranzo. Se l'attività è lunga, si può ridurre questo impegno alla prima giornata; se l'attività è di uno o due giorni, è opportuno organizzare il pranzo tutti i giorni.

Si consiglia di chiedere a metà mattinata se vuole "accompagnarci per pranzo", in modo che tutti possano organizzarsi convenientemente. Alcuni auditor rifiutano per evitare conflitti di interesse (anche se spesso sono in trasferta con rimborso spese), altri accettano volentieri. Spesso un pranzo permette all'auditor di cogliere meglio il lato umano dell'organizzazione e la sua *cultura*.

L'organizzazione non deve pagare per forza il pasto, soprattutto se vi sono regole o codici etici da applicare. In ogni caso, è meglio chiarire subito con l'auditor la cosa. È anche opportuno chiedere all'auditor se ha problemi particolari, in modo da non andare in un posto "solo pesce" se non può mangiarlo.

Il pranzo non deve essere troppo lungo, perché si è lì per ragioni di lavoro, ma neanche un panino al bar in piedi. Un posto veloce, decoroso e vicino alla sede dove si sta svolgendo l'audit permette di non perdere tempo e di rendere piacevole il pasto.

Si evitino posti lontani o "da provare" proprio per il giorno dell'audit. Alcuni, in particolare se normalmente devono osservare una dieta, colgono l'occasione dell'audit per una mangiata pantagruelica: anche questo va evitato.

Ogni perdita di tempo la pagano tutti: l'audit deve essere completato e se il pranzo è lungo, l'audit si concluderà più tardi, senza soddisfazione per alcuno.

Se l'auditor è in trasferta, si dovrebbe aiutarlo a trovare un buon hotel e segnalargli il modo migliore per raggiungere la sede dell'audit. Può anche essere organizzata una cena con le stesse regole di cui sopra. Non è però obbligatorio. Certamente, se alcuni rappresentanti dell'organizzazione sono in trasferta e devono cenare al ristorante, allora è una buona idea coinvolgere anche l'auditor.

A.2 L'auditor è un partner

Una delle cose più pericolose è raccontare bugie a un auditor, soprattutto perché potrebbe accertare la verità e poi mettere in discussione qualunque altra successiva affermazione.

Quelle più comuni riguardano l'impossibilità tecnica di fare qualcosa (per esempio, sui sistemi Linux creare utenze personali con gli stessi privilegi di *root*), con il risultato che l'auditor potrebbe anche sentirsi offeso se invece conosce la tecnologia in questione.

È anche importante evitare scuse come "non abbiamo risorse": l'auditor potrebbe riportare la lamentela alla Direzione, con potenziali ricadute negative su chi l'ha fatta perché ritenuto incapace di gestire i processi con le risorse messe a disposizione. Inoltre questa scusa è nota per essere la più diffusa; un auditor ha avuto modo di rispondere "è un vostro problema di organizzazione" e di scrivere una non conformità.

È meglio evitare contestazioni, inventando scuse improbabili, quando l'auditor ha ragione. In questi casi, l'atteggiamento corretto è: accettare il rilievo ed, eventualmente, cercare di dimostrare che si tratta di cosa non grave.

L'auditor è un partner e quindi è sempre possibile segnalargli aree su cui potrebbe contribuire maggiormente. È necessario tuttavia stare attenti e non segnalare aree di non conformità tali da compromettere il risultato dell'audit. Per esempio, gli si può chiedere di affrontare argomenti su cui la consapevolezza e attenzione delle persone coinvolte è ridotta.

È sempre una buona tecnica, se adottata con sincerità, chiedere chiarimenti su come interpretare alcuni requisiti oggetto dell'audit: l'auditor si sente coinvolto per le sue competenze e può metterle a disposizione di qualcuno.

Altra buona tecnica è fargli vedere le novità rispetto all'ultimo audit o i progetti innovativi, purché gestiti in modo adeguato: spesso gli auditor vedono sempre le stesse cose, seppure differenti e in ambienti diversi; le novità fanno sempre piacere.

Una cortesia riguarda la documentazione: se è molta e in formato elettronico, è opportuno stamparne qualche esempio, oppure permettergli di consultarla con un PC dedicato. È sempre molto frustrante dover esaminare delle procedure (anche numerose o molto lunghe) senza poterlo fare in autonomia.

Per la pianificazione dell'audit è opportuno cercare di collaborare con l'auditor, soprattutto se l'organizzazione è grande e gruppi diversi si occupano di cose simili (per esempio, per la conduzione dei sistemi Windows e Unix) o le attività sono svolte in sedi diverse e lontane tra loro (molte grandi organizzazioni sono il frutto di acquisizioni e incorporazioni, con il risultato di avere molte sedi e gruppi di lavoro diversi). Si dovrebbe quindi indicare all'auditor le potenziali

difficoltà relative al tempo da dedicare ad alcuni spostamenti o alla scorretta pianificazione delle attività.

Esempio A.2.1. Un auditor potrebbe pianificare due ore per la verifica della conduzione dell'infrastruttura informatica. Se questa è effettuata da più funzioni dell'organizzazione, bisognerebbe segnalarglielo, in modo che possa modificare il piano in modo appropriato. In caso contrario, l'auditor potrebbe trovarsi in difficoltà a chiudere l'audit nei tempi previsti.

Alcuni ritengono che una pianificazione scorretta possa essere utile a perdere tempo. In realtà si rischia di costringere l'auditor e le persone coinvolte nell'audit a fare tardi e non poter affrontare serenamente l'impegno.

Se l'auditor lo permette, è possibile collaborare alla scrittura del rapporto, in modo che i termini utilizzati e alcuni riferimenti siano facilmente comprensibili a tutte le parti interessate, inclusa la Direzione. Ovviamente, questo non implica l'opportunità di modificare il risultato finale dell'audit.

A.3 L'auditor è un fornitore

L'auditor, se esterno, è veramente un fornitore. Anche l'auditor interno può essere visto come fornitore interno. Per questo, è giusto pretendere la qualità del servizio.

Il primo parametro riguarda il rispetto dei tempi: bisogna chiedere di ricevere con congruo anticipo il regolamento dell'audit e il piano di audit, in modo da garantire la presenza delle persone da coinvolgere senza doverle bloccare oltre il necessario. Inoltre, se non ci sono contrattempi e il piano è stato concordato tra le parti in modo collaborativo e non sono emerse non conformità, se l'auditor prolunga gli incontri oltre l'orario stabilito, deve essere invitato a terminarli.

Durante l'audit, al termine di ogni incontro è opportuno chiedere di esplicitare se ha rilevato qualcosa, in modo che la illustri e fornisca i necessari chiarimenti. Bisogna chiedere chiarimenti fino a quando non si è capito il rilievo, ovviamente evitando di prendere in giro l'auditor e manifestare una falsa incapacità di comprensione per perdere tempo.

Non bisogna aver paura di contraddire un auditor. Per esempio, se vuole che siano verificati i PC dei visitatori all'ingresso della sede e si ritiene inutile questa misura, bisogna spiegargli le proprie motivazioni (spesso collegate alla valutazione del rischio) e non accettare passivamente ogni sua richiesta.

Può essere necessario pretendere il rispetto dei tempi anche dopo la conclusione dell'audit, in particolare relativamente ai tempi di consegna del rapporto. Spesso, quando si riceve il rapporto dopo molto tempo la conclusione dell'audit, se è scritto in modo molto sintetico, è difficile interpretarlo correttamente e avviare le opportune azioni correttive a fronte delle non conformità rilevate.

Bisogna evitare di fare da segretario dell'auditor, per esempio prenotando treni o aerei come potrebbe fare autonomamente via web.

A.4 L'auditor è un auditor

La raccomandazione di essere sinceri deve essere bilanciata con la necessità di non dire proprio tutto.

Regola base: fare in modo che tutto il personale, compresa la Direzione, sia preparato all'audit, anche grazie a simulazioni svolte in precedenza.

Le simulazioni vanno fatte con largo anticipo rispetto all'audit, in modo da condividere i punti da evitare o da adeguare. Le persone che parteciperanno all'audit dovranno essere molto collaborative in questa fase. Alcuni, anche se non hanno mostrato interesse durante le fasi preparatorie, presi da entusiasmo, raccontano all'auditor cose mai segnalate in precedenza ai consulenti o agli auditor interni, con ovvi effetti negativi.

D'altra parte bisogna evitare di falsificare le attività: se durante l'anno non si è fatto nulla per essere conformi ai criteri di audit bisognerebbe chiedersi se non si sono fatti degli errori nella progettazione e pianificazione del proprio sistema di gestione. È pratica comune riesaminare e correggere in anticipo i documenti che l'auditor, presumibilmente, analizzerà, esattamente come si riassetta la casa prima di ricevere degli ospiti. Ma non è ammissibile trovarsi nella necessità di creare dal nulla procedure e registrazioni come dei villaggi Potëmkin o delle ombre cinesi azionate da Fantozzi.

Esempio A.4.1. Una forma interessante di falsificazione delle attività è l'attuazione di misure di sicurezza solo per l'auditor: controllo del computer all'ingresso, indisponibilità della wi-fi, eccetera. Spesso queste false misure sono evidenti perché l'auditor vede altri visitatori trattati in modo diverso e, a quel punto, è costretto a scrivere una non conformità.

Quando si affronta un audit è anche necessario comprendere le esigenze degli auditor: devono vedere esempi delle attività oggetto di audit e quindi bisogna evitare di raccontare processi e controlli di sicurezza solo a voce. È imbarazzante per l'auditor dover continuare a chiedere delle *evidenze* e continuare ad ascoltare solo parole (anche se il termine *auditor* deriva proprio dal latino "ascoltare"); in questi casi l'incontro potrebbe concludersi in ritardo o con delle non conformità.

Da evitare frasi come "Questo documento l'ho messo da qualche parte nella e-mail": le registrazioni vanno tenute sotto controllo e opportunamente archiviate; il fatto che siano reperibili solo in una casella di posta rappresenta una non conformità.

L'auditor non conosce in modo approfondito le mansioni di ciascuno e potrebbe cercare di affrontare un argomento con la persona sbagliata. In questo caso è bene imparare a rispondere "Vorrei non rispondere su questo argomento perché di competenza di altri" e indicare a chi rivolgersi. Alcuni cercano di rispondere come se fossero interrogati a scuola su un argomento che non hanno studiato, con prevedibili risultati negativi.

Se qualcuno è in difficoltà a capire o rispondere a una domanda, deve chiedere aiuto ai colleghi o collaboratori: l'audit è una valutazione dell'organizzazione ed è la "organizzazione" a dover rispondere, non una singola persona. Questa regola ha le sue eccezioni: è previsto che ciascuno sappia reperire e interpretare la politica per la sicurezza delle informazioni e le procedure applicabili alle sue mansioni (non è però previsto che siano recitate a memoria).

Molti accompagnatori tendono ad assumersi la responsabilità dei risultati dell'audit e a intervenire su tutti gli argomenti. Anche questo è un atteggiamento da evitare: se l'audit è stato preparato correttamente, è giusto che dimostrino fiducia nelle persone e le lascino rispondere. In alcuni casi, però, la persona intervistata potrebbe cedere al panico, anche se ingiustificato, e in questo caso l'accompagnatore dovrebbe intervenire per aiutare. Un'altra occasione di aiuto si presenta quando l'auditor e gli intervistati hanno difficoltà a comprendersi a vicenda perché utilizzano gerghi tra loro diversi.

Bisogna ricordare che l'auditor pone molte domande perché soprattutto intende capire i processi e non ha alcuna intenzione di affliggere i propri interlocutori.

Purtroppo, alcune organizzazioni assegnano al personale obiettivi sul numero di rilievi dell'audit. Questa è una pratica scorretta perché, oltre a rendere gli audit conflittuali, prevede di assegnare obiettivi al lavoro dell'auditor e quindi si potrebbe avere una non conformità perché gli obiettivi non sono appropriati.