Il narcisismo della compliance

Ogni organizzazione – non ha rilievo la dimensione, il fatturato né il settore merceologico – ha la necessità di operare conformemente a molteplici requisiti normativi che, inevitabilmente, devono trovare un punto di equilibrio con le esigenze di business senza alimentare contrapposizioni interne all'organizzazione stessa.

Non é così remoto pensare che il **rispetto di norme** influisca negativamente sull'espansione del business dell'organizzazione. *Compliance manager*, CISO, DPO e *privacy manager*, spesso sono contrapposti a CIO, CSO, *security manager* e *specialist* di ogni genere. Gli uni apparentemente ispirati da un amor morboso per il rispetto aprioristico di norme, regole e regolamenti di ogni sorta; gli altri votati alla sicurezza "del *bit*". Tutte queste figure professionali ricoprono un ruolo fondamentale e decisivo sia per la sopravvivenza delle organizzazioni, che quotidianamente devono fronteggiare attacchi e minacce interne ed esterne sempre più evolute, sia per lo sviluppo del business aziendale, impersonificando un indiscutibile fattore abilitante la crescita.

Non c'è autoreferenzialità nel voler attuare *framework* e modelli di Cybersecurity, come nel voler attuare le *best practice* di settore all'interno della propria azienda. Non c'è autoreferenzialità nel voler implementare i Regolamenti, le norme e le prassi, troppo spesso oggetto solo di studi teorici. Le certificazioni che un'organizzazione decide, su base volontaria, di ottenere anche per distinguersi rispetto *competitor*, non sono finalizzate a sé stesse e dovrebbero essere riconosciute per quel che sono: **un'attestazione di una terza parte**, allo scopo riconosciuta e accreditata per verificare l'aderenza dello *scope* di certificazione, al testo

normativo. Eppure, è così che spesso, nelle relazioni cliente-fornitore, entrano in conflitto i differenti sistemi di gestione delle aziende.

È usuale, nella valutazione di un fornitore, avvalersi di un proprio modello di indagine tecnico-organizzativa, senza voler considerare se questi abbia, per i servizi oggetto di fornitura, già ottenuto una certificazione di terza parte.

La scelta di non voler considerare quanto ottenuto dalla controparte, sovente scade nell'autocompiacimento per il proprio schema di valutazione, nel proprio sistema di *compliance*: da qui il passo verso una **inconsapevole forma di narcisismo** per la propria struttura di valutazione é davvero breve ed estremamente pericoloso.

Il *top management*, che pensa in termini di costi e opportunità, non può non considerare opportunamente l'*effort* derivante dalla duplicazione delle attività di *compliance*, in senso lato, generate per assecondare le differenti e molteplici richieste di clienti e fornitori, di adattarsi a differenti modelli operativi o semplicemente di sottostare a differenti schemi di valutazione.

Sarà capitato ai più di dover rispondere a questionari di "qualificazione del fornitore" in nome di un qualche obbligo normativo o di regolamenti interni.

Spesso non si considera che questa esigenza, assolutamente legittima, potrebbe essere facilmente soddisfatta se venissero opportunamente considerate le certificazioni già possedute dall'organizzazione in esame.

Diversi sono gli studi che dimostrano come una certificazione possa rappresentare **un valido investimento** per l'imprenditore che decide di far crescere la propria azienda. Non bisogna dimenticare che dietro questi riconoscimenti vi sono organismi di certificazione, laboratori di valutazione ed enti di accreditamento che, pur facendo della certificazione il

proprio business, non hanno alcun ragionevole interesse a certificare il falso, essendo poi responsabili per eventuali attestazioni non veritiere.

Un recente rapporto di Accredia[1] mostra quanto sia apprezzabile il ritorno sull'investimento di una certificazione:
"La certificazione accreditata di un sistema di gestione contribuisce a far crescere il fatturato dal 2% al 18%, in funzione dell'ambito di appartenenza e degli standard applicati (qualità, ambiente, sicurezza, ecc.)".

E ancora:
"Le imprese certificate per la UNI EN ISO 9001 registrano ricavi aggiuntivi dell'8,2% e del 17%, rispettivamente nel primo e secondo anno successivi alla certificazione."

Per non vanificare questi investimenti, si dovrebbe riconoscere che l'esistenza di una certificazione, rilasciata sotto accreditamento, da un Organismo di Certificazione (OdC) allo scopo abilitato, in grado di attestare la conformità del sistema, del processo, del prodotto o delle figure professionali rispetto le specifiche esigenze del valutatore, è garanzia adeguata di "qualità" del detentore della certificazione e non serve correre il rischio di effettuare un'ulteriore valutazione, con ogni probabilità approssimativa, che potrebbe quindi risultare in danno qualora non si considerassero le certificazioni in oggetto.

Spesso mi capita di dover rispondere a questionari di valutazione preconfezionati, che non tengono in considerazione l'effettivo servizio reso al Cliente, nei quali è prevista l'esibizione di documenti che, con un pizzico di buon senso, nessuno vorrebbe coscientemente condividere con soggetti esterni: spesso nemmeno con soggetti interni all'organizzazione stessa.

È lecito quindi chiedersi quale sia **il vero valore delle**

certificazioni: che senso abbia investire molte risorse in queste attività se poi nessuno, al di là dell'*auditor*, è disposto ad apprezzare il lavoro fatto.

Un'azienda seria, fondata su sani principi che desidera prosperare, non può pensare alle certificazioni come a un mero atto amministrativo, banalizzandole al punto di ritenere di poter "comprare la certificazione", magari avvalendosi di superficiali consulenti che altro non fanno che replicare sterilmente, quasi come si trattasse di una catena di montaggio, documentazione varia, acquistata o prodotta in forma di "*toolkit*".

Nulla di più sbagliato e deleterio per la crescita aziendale.

Le certificazioni acquisite pensando solo al colore del bollino da esporre sul sito web aziendale, non servono a nulla: non servono a correggere processi aziendali, non servono a migliorare le qualità di un prodotto, non servono a cambiare, in meglio, la mentalità e la cultura aziendale che dovrebbe permeare le menti di manager, dipendenti, collaboratori dell'azienda, finanche clienti e fornitori.

Il cuore del problema sta proprio qui. Non bisogna pensare, stupidamente, che una certificazione o la *compliance* sia affare del solo *compliance manager*, o di figure analoghe, che dotato di uno strabordante narcisismo, trova soddisfazione unicamente in questa attività nelle quale può rispecchiarsi.

Non è possibile pensare che il costante aumento delle richieste di certificazione, spesso plurime all'interno di una singola organizzazione, sia solamente dovuto ai capricci di pochi.

I dati che Accredia mette a disposizione sono eloquenti.

Figura 1: Organizzazioni con una norma certificata negli ultimi 24 mesi. Fonte: Accredia

L’andamento in figura 1 varia significativamente all’aumentare delle norme certificate acquisite da una singola organizzazione.



Figura 2: Organizzazioni con sei norme certificate negli ultimi 24 mesi. Fonte: Accredia

Con una **prospettiva internazionale**, possiamo osservare come le organizzazioni del nostro paese siano molto propense a ricercare certificazioni. Una *survey* condotta da ISO nel 2018[2] ha contato le certificazioni, per settore merceologico, acquisite da organizzazioni sparse in 188 nazioni. Considerando le norme ISO 9001, ISO/IEC 27001, ISO 22301 e ISO/IEC 20000-1, in una graduatoria che conta complessivamente il numero di certificati emessi per norma, il nostro paese è al secondo posto, preceduto dalla Cina. Seguono Germania (terza), Spagna (quinta), Inghilterra (settima), Polonia (decima) e Francia (cinquattottesima).
Riconoscendo dunque che i *Compliance manager*, così come i diffusi C-level, i DPO o i *privacy manager*, i *security manager* e gli *specialist* di ogni genere, sono mossi dalla medesima esigenza di soddisfare gli obiettivi aziendali e non da un endemico e narcisistico bisogno di autoaffermazione (che, a ben vedere, potrebbe risolversi molto più facilmente), occorre affermare oltre ogni ragionevole dubbio il valore distintivo della *compliance* e non cedere alla tentazione di affermare una fantomatica superiorità volendo imporre, senza alcun fondamento razionale, i più diversificati proprietari schemi di valutazione.

In un mondo totalmente interconnesso e intimamente interdipendente, così spesso si sente dire, la **standardizzazione dei processi**, anche quelli di valutazione e certificazione, altro non è che uno dei meccanismi di coordinamento teorizzati da H. Mintzberg[3] a metà degli anni ‘80 del secolo scorso: soltanto, in una scala globale.

Più organizzazioni decidono di certificare le proprie attività, maggiore può essere il mutuo riconoscimento del valore delle stesse, con indubbi vantaggi e risparmi per ogni organizzazione.

Note

[1] Accredia, *Quanto vale la Qualità? Il nuovo studio dell'Osservatorio Accredia*. Luglio 2020

[2] *ISO Survey of certifications to management system standards*. ISO SURVEY 2018

[3] H. Mintzberg, *La progettazione dell'organizzazione aziendale*. Prentice-Hall, 1983

Articolo a cura di **Luciano Quartarone**

https://www.ictsecuritymagazine.com/articoli/il-narcisismo-della-compliance/