Compliance e Organizzazione

CESARE GALLOTTI

INDICE: 1. Introduzione – 2. Compliance e Organizzazione - 3. Le norme ISO 9001 e ISO/IEC 27001 – 4. Approccio per processi - 5. Approccio sistemico – 6. Attribuzione delle responsabilità - 7. Leadership - 8. Miglioramento continuo - 9. Le norme ISO - 10. Conclusioni - 11. Appendice: carta di Pescara

1. Introduzione

Questo contributo si propone di illustrare alcune difficoltà riscontrabili nell'applicazione delle misure richieste dalla legge. Si vedrà come, per un'efficace ed efficiente implementazione delle misure, sia necessario adottare un approccio interdisciplinare che comprenda la partecipazione di esperti di compliance e di organizzazione e si indicheranno alcuni standard internazionali di supporto.

2. Compliance e Organizzazione

Una delle aree dell'informatica giuridica riguarda gli adempimenti tecnici e organizzativi che le aziende devono soddisfare per essere conformi a quanto dispone la legge.

Il tema più importante di quest'area è senz'altro quello noto sotto la denominazione di *Privacy*, che comprende le norme collegate al Decreto Legislativo 196 del 2003, inclusi i Provvedimenti del Garante per la Protezione dei Dati Personali. Queste norme, seppure in modo disomogeneo, devono essere applicati in tutte le imprese italiane, mentre altre devono comunque essere prese in considerazione, anche se si tratta di argomenti settoriali (come la Legge Pisanu del 2005 per i fornitori di connettività) o per le quali l'assenza di specifiche misure non è reato, ma può avere impatto sulla valutazione di eventuali altri delitti (come il Decreto Legislativo 231 del 2001 sulla Responsabilità Amministrativa delle Imprese).

Il controllo di quali norme siano applicabili ad un'impresa e la scelta su come attuare misure tecniche e organizzative per soddisfarne i requisiti è svolta da una funzione aziendale normalmente chiamata *Compliance*.

Le imprese, però, devono essere organizzate per condurre il proprio business. Di conseguenza, i processi aziendali sono strutturati in modo da garantire efficacia ed efficienza

nella realizzazione dei prodotti o nell'erogazione dei servizi offerti ai clienti. Il soddisfacimento di quanto richiesto dalla Legge non è il loro principale obiettivo, anche se tale argomento va tenuto in considerazione quando si strutturano i processi. Tipici di un'impresa sono: il processo di relazione con i clienti, il processo di realizzazione dei prodotti o dell'erogazione dei servizi, il processo di gestione degli approvvigionamenti, il processo di gestione del personale, il processo amministrativo.

La loro strutturazione, la misurazione della loro efficacia ed efficienza e la gestione del loro miglioramento sono attività coordinate dalla funzione normalmente chiamata *Organizzazione*. Posto che i processi di un'impresa influiscono direttamente o indirettamente sulla qualità dei prodotti realizzati o dei servizi erogati, ossia sulla soddisfazione delle aspettative dei clienti, si utilizza anche *Organizzazione e Qualità*. Tale espressione si sta diffondendo anche grazie allo standard internazionale ISO 9001 sui Sistemi di Gestione per la Qualità.

Troppo spesso, purtroppo, i rapporti tra le funzioni Compliance e Organizzazione non sono strutturati come dovrebbero e questo contributo vuole mostrare come sia necessario impostare correttamente tali rapporti. Infatti, le misure necessarie per soddisfare la normativa vigente devono essere inserite nei processi aziendali e, viceversa, i processi aziendali devono essere modellati anche per garantire il soddisfacimento di tutti i requisiti legali.

Per capire i rapporti tra Compliance e Organizzazione, saranno illustrati alcuni principi di organizzazione aziendale posti alla base di importanti standard internazionali e si vedrà come siano convenienti anche per applicare i requisiti di tipo legale.

3. Le norme ISO 9001 e ISO/IEC 27001

L'International Organization for Standardization (indicata anche con il falso acronimo ISO) è un'organizzazione che si occupa della pubblicazione di standard e normative riconosciuti da Comitati rappresentativi di più Paesi e di più interessi (clienti, fornitori, pubblica amministrazione, eccetera). Uno degli standard più noti emessi dalla ISO è la ISO 9001, dedicata alla descrizione degli elementi fondamentali di un Sistema di Gestione per la Qualità, ossia di come un'impresa debba essere organizzata per fornire i propri prodotti o servizi in accordo a quanto stabilito con i propri clienti.

Si osservi che il termine "cliente" ha una connotazione molto ampia e comprende anche un utente di un servizio pubblico, un privato, un'impresa o una diversa area della stessa impresa in cui opera il "fornitore". Anche il termine "accordo" deve essere inteso in modo ampio, non limitandosi ai soli contratti scritti e controfirmati dalle parti, ma anche agli accordi non esplicitati (per esempio, in un contratto di acquisto di un'automobile non si fa normalmente menzione della presenza di uno sterzo sul veicolo) o alle semplici aspettative del cliente (per esempio, l'utente di un pronto soccorso pubblico non firma alcun contratto con la struttura ospedaliera, ma si aspetta comunque di essere assistito nel modo migliore).

Infine, è opportuno notare come gli standard ISO non utilizzino il termine "impresa", bensì "organizzazione", per garantire l'applicabilità degli standard a tutte le realtà. In questa sede si preferirà il termine "impresa", in quanto più immediato ad un lettore non abituato alla terminologia ISO e per evitare confusione con la funzione Organizzazione.

Secondo la ISO, i principi base di un Sistema di Gestione per la Qualità sono i seguenti:

a) Orientamento al cliente: l'impresa deve comprendere e soddisfare le necessità dei propri clienti
b) Leadership: i leader di un'impresa sono i primi responsabili nel dirigerla e nell'ottenere i risultati desiderati
c) Coinvolgimento del personale
d) Approccio per processi: le attività e le risorse devono essere gestite all'interno dei processi
e) Approccio sistemico alla gestione: per garantire l'efficacia e l'efficienza dei processi, questi devono essere individuati e gestiti anche considerandone le interrelazioni
f) Miglioramento continuo: il miglioramento dell'efficacia ed efficienza dei propri processi deve essere un obiettivo primario di un'impresa
g) Decisioni basate su dati di fatto
h) Rapporti di reciproco beneficio con i fornitori

I principi da b) ad f) sono applicabili anche quando si parla di compliance. Sovente, purtroppo, gli interventi richiesti dalla funzione di Compliance non tengono conto né di questi principi né delle esigenze organizzative, creando di fatto due binari paralleli che non portano alcun beneficio.

Sono presentati di seguito alcuni esempi, utili per capire i principi sopra esposti e come le due funzioni debbano essere tra loro collegate. Gli esempi sono reali, anche se presentati in forma semplificata e, per ovvi motivi, non sono riportate informazioni per risalire all'impresa a cui si riferiscono.

4. Approccio per processi

In un'impresa, secondo il principio d), le attività e le risorse devono essere gestite all'interno dei processi aziendali e quindi individuato e stabilito il flusso delle informazioni e dei materiali in modo da capire completamente quali sono gli elementi di ingresso (input) di un insieme di attività e quali sono gli elementi in uscita (output) attesi. Questo approccio ha come caratteristica la *misurabilità* dell'efficacia e dell'efficienza dei processi.

Un esempio di come sia necessario definire con attenzione gli input di ciascun processo è fornito da un'azienda internazionale in cui è stato recentemente introdotto un nuovo sistema informatico di gestione dei clienti (CRM o Customer Relationship Management).

Seguendo i processi aziendali, i requisiti del CRM sono stati formalizzati dal personale tecnico in un documento, sono stati contattati i potenziali fornitori per avere un'offerta di soluzioni basate sui requisiti elencati, è stato scelto il fornitore sulla base della completezza ed economicità dell'offerta e il software è stato reso disponibile all'azienda dopo due anni di lavoro e qualche milione di Euro. In una delle sessioni di formazione un dipendente italiano ha fatto notare che il software non consentiva agli utenti l'autonoma sostituzione della password, così come richiesto dall'Allegato B del Dlgs 196 del 2003, applicabile in quanto il software è utilizzato per il trattamento dei dati personali dei clienti.

E' successo che il processo di acquisizione di una soluzione software non è mai stato integrato con il processo di gestione della compliance a livello dei singoli Paesi in cui opera l'impresa. In altre parole, tra gli input del processo di definizione dei requisiti e di gestione degli approvvigionamenti non era stato richiesto il parere della funzione Compliance.

Ad un'analisi più approfondita, si è rilevato che in precedenza era stato emesso un Ordine di Servizio con indicate le misure da prendere nell'acquisto di nuovi software, ma le procedure aziendali non erano mai state aggiornate in questo senso e, fatalmente, la funzione acquisti non l'ha applicato.

Questo difetto macroscopico non è purtroppo isolato. Troppe volte gli adempimenti legali sono recepiti da un'impresa solo attraverso la pubblicazione di specifica modulistica, slegata però dalla documentazione di uso quotidiano, con il risultato che poi viene dimenticata e non più utilizzata nel giro di un paio di mesi.

Occorre quindi riesaminare e rimodellare i processi, con i relativi strumenti, ogniqualvolta devono essere recepiti nuovi adempimenti di carattere legale, in modo che questi diventino parte del lavoro di tutti i giorni. E' evidente che per ottenere questo risultato, le funzioni di Compliance e Organizzazione debbano collaborare.

5. Approccio sistemico

L'approccio sistemico, come si è già detto, si accompagna all'approccio per processi e richiede di non vedere ogni processo come slegato dagli altri, ma come un insieme di entità tra loro correlate. Nell'esempio precedente si è visto come sia stato possibile ignorare la relazione tra processo di compliance e quello di acquisti.

Altro esempio di mancanza di approccio sistemico riguarda un'azienda di ricerche di mercato, la cui responsabile Compliance doveva stabilire il tempo massimo di conservazione dei dati sulle interviste, soprattutto quelli delle persone intervistate.

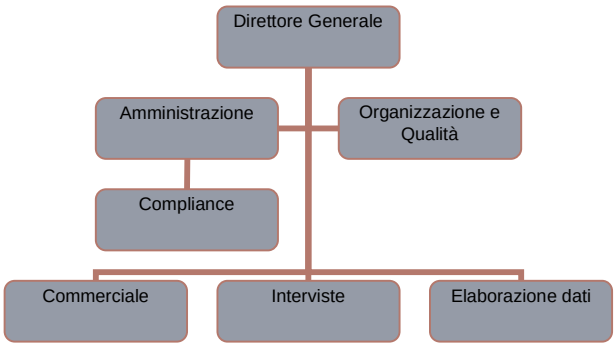
In questo caso, la regola dipende da come viene sviluppato ciascun progetto di ricerca: il cliente può richiedere di condurre interviste per tre anni evitando di ricontattare due volte le stesse persone, oppure di disporre nei due mesi successivi alle interviste della documentazione per effettuare dei controlli sul numero di persone intervistate e per elaborare statistiche, per esempio, sulle percentuali di uomini e donne, oppure di disporre dei dati di coloro che hanno accettato di partecipare all'estrazione di un premio dopo sei mesi.

Il processo commerciale deve precisare le necessità del cliente e comunicarle ai responsabili del progetto. Questi dovranno fornire le opportune specifiche al processo di gestione dei sistemi informativi, affinché programmino opportunamente il momento di cancellazione dei dati. Dovrà anche essere coinvolto il processo di gestione del personale affinché gli intervistatori raccolgano il consenso dell'intervistato con le opportune specifiche.

Come si vede anche da questo esempio, una richiesta apparentemente banale esige il coinvolgimento di più entità. Ed è proprio la capacità di mettere in relazione diversi processi, tipica dell'Organizzazione, che risponde al principio di approccio sistemico.

6. Attribuzione delle responsabilità

L'azienda di cui sopra è strutturata secondo il seguente organigramma:



Le funzioni Compliance e Organizzazione sono a due diversi livelli di distanza dal vertice aziendale e le distanze su carta si ritrovano poi nella realtà. In questo caso, le due responsabili di funzione avevano rapporti di antipatia reciproca e la questione sui tempi di conservazione non è ancora stata risolta.

Di solito, la funzione di Compliance ha una posizione di maggior importanza rispetto all'Organizzazione e ciò può portare all'emissione di disposizioni slegate dalla normale organizzazione aziendale e dai normali flussi di lavoro, con i risultati visti sopra.

Al di là, comunque, delle scelte di strutturazione degli organigrammi, è opportuno che vengano definite linee di comunicazione tra questa due funzioni aziendali e sia esplicitamente richiesto di utilizzarle, con l'attribuzione di precise responsabilità. Nel caso specifico, andava stabilito che l'emanazione di Ordini di Servizio da parte della Compliance e di procedure organizzative da parte di Organizzazione fossero responsabilità congiunte delle due funzioni, con tempi ben definiti di approvazione dei documenti e precisato un processo di coinvolgimento dei vertici aziendali in caso di veti incrociati.

7. Leadership

Si dice che la padella va dove la porta chi ne tiene il manico. In altri termini, un'azienda si comporta come vuole la Direzione.

Se la Direzione è interessata all'attuazione delle misure di sicurezza richieste dalla normativa vigente, queste saranno realizzate e mantenute al meglio. In caso contrario, il personale individuerà le azioni minime per potersi dichiarare non responsabile agli occhi della Legge e della Direzione nel caso si presentasse qualche inconveniente.

Questa non è una posizione tipica degli italiani: la letteratura in materia e l'esperienza personale confermano la diffusione di questo atteggiamento in tutto il mondo, Paesi anglosassoni inclusi. Tutto ciò è molto comprensibile: se la Direzione preferisce correre il rischio di non implementare al meglio le misure di sicurezza, non si capisce perché i dipendenti o i fornitori debbano discutere le decisioni di chi ha maggior potere di loro.

In un'azienda di trasporti, una procedura prevedeva l'assegnazione di diritti di accesso alle informazioni basati sul ruolo di ciascun utente del sistema informatico e la loro attivazione solo a seguito di un'approvazione scritta dei Responsabili del Trattamento dei Dati. Dopo pochi giorni dall'emissione della procedura, l'Amministratore Delegato, dovendo far elaborare ai propri consulenti dei report sulla clientela, ha richiesto gli accessi per tali consulenti al software di CRM (con dati personali!) direttamente agli operatori del sistema informatico. La richiesta fu fatta al telefono: trattandosi dell'Amministratore Delegato, non sembrava il caso di fargli compilare i moduli previsti.

Fatalmente, dopo poco, la gestione dei diritti di accesso non ha più seguito la normale procedura ed è stato necessario un complesso lavoro per rimettere sotto controllo tale processo.

Il principio di leadership, quindi, non deve essere solo inteso come emanazione di politiche, ma anche come sorveglianza, da parte della Direzione, dei propri comportamenti, in quanto specchio della cultura aziendale e, di conseguenza, dei comportamenti del personale.

Un ulteriore esempio riguarda un altro aspetto della leadership: l'azienda è un ISP di grandi dimensioni, fornitore anche del servizio di posta elettronica per i propri clienti. Nel caso in cui un utente dimentichi la password di accesso al servizio, per azzerarla l'ISP ha previsto la possibilità di chiamare un contact center mediante un Numero Verde. Il responsabile del contact center, in mancanza di linee guida da parte della Direzione, si è inventato una procedura di autenticazione dei clienti, chiedendo loro nome, cognome, data di nascita, codice fiscale (o partita IVA).

Tale meccanismo di autenticazione è molto debole e quando il Responsabile della Sicurezza delle Informazioni (anche lui membro della Direzione) se ne è accorto, ha obiettato.

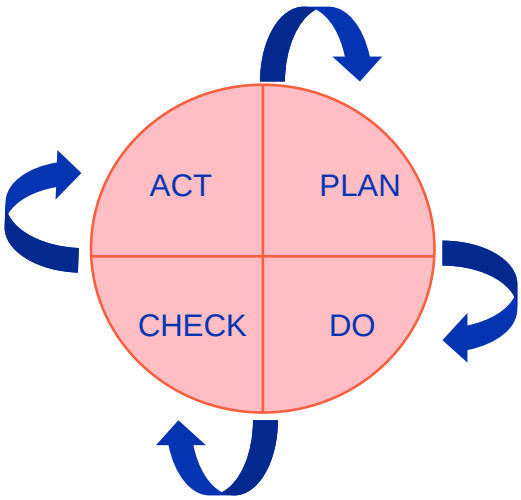
La responsabilità di tale situazione è proprio della Direzione, che non ha fornito al responsabile del contact center, digiuno di qualsiasi nozione di sicurezza, alcuna linea guida, formazione o consulenza, ossia le risorse, anche economiche, per poter affrontare adeguatamente il compito affidatogli.

8. Miglioramento continuo

L'esempio dell'ISP ci permette di illustrare anche un ulteriore principio. Per garantire la corretta implementazione delle misure è necessario avviare un processo di pianificazione e monitoraggio delle attività. Uno dei modelli più noti è il cosiddetto ciclo di Deming o ciclo Plan-Do-Check-Act

Nell'ISP dell'esempio precedente era compito della Direzione stabilire gli obiettivi di sicurezza (Plan) che il contact center avrebbe dovuto seguire (Do) e monitorare e verificare l'avanzamento delle azioni attraverso opportuni audit da parte di persone competenti (Check) per verificare l'efficacia del meccanismo e migliorarlo nel caso in cui non ritenesse efficace l'azione (Act). Il Responsabile della Sicurezza delle Informazioni, piuttosto che "scoprire" la debolezza del meccanismo di autenticazione dei clienti, avrebbe dovuto monitorare nel tempo le scelte effettuate dal responsabile del contact center e richiedere gli opportuni miglioramenti.

Il ciclo è rappresentato dalla figura.



Il "miglioramento" non deve essere solo inteso come continua sfida per raggiungere certe performance o per ottenere una qualità eccelsa, ma anche, e soprattutto, come "adeguamento" continuo alle richieste di mercato e all'ambiente in cui opera l'impresa, del quale fa parte la normativa applicabile.

Il principio di miglioramento continuo, è bene ricordarlo, prevede che vengano seguiti tutti i passi: è esperienza fin troppo comune vedere come molte attività siano solo pianificate e mai realizzate. Ed è quindi opportuno sottolineare come le risorse e le energie di un'impresa debbano essere equamente ripartite tra i vari passaggi.

9. Le norme ISO

Per sviluppare al meglio i principi sopra elencati, è utile studiare alcune norme ISO sui "Sistemi di gestione". Tali norme descrivono alcuni ambiti specifici di un'impresa (la qualità, la sicurezza delle informazioni, la gestione dei servizi IT) e i requisiti minimi o consigliabili per i processi che ne garantiscono l'efficacia.

Le norme indicate possono anche essere utilizzate dalle aziende per sottoporsi ad audit da parte degli Organismi di Certificazione per ricevere, se ritenute conformi, un certificato di conformità alla norma scelta. La certificazione, negli ultimi dieci anni, è sempre più richiesta per poter partecipare ai bandi di gara emanati dalla Pubblica Amministrazione o da alcune grandi aziende. Questo ha fatto sì che in troppi casi l'utilizzo degli standard ISO sia visto come "male necessario" e, di conseguenza, siano applicati male e con inutili inefficienze. In altre parole, le norme ISO sono oggi viste come portatrici di "carta, inutile burocrazia e perdita di tempo".

Una loro lettura, interpretazione e applicazione attente, invece, possono portare molti benefici alle imprese. Come abbiamo visto, gli esempi negativi presentati si sarebbero potuti evitare se fossero stati correttamente seguiti i principi delle norme ISO.

La norma più famosa è la ISO 9001, la cui ultima versione, molto simile a quella del 2000, è del 2008. La versione della ISO 9001 del 2000 era anche nota come Visio 2000. La ISO 9001 è utile per modellare i principali processi di business (commerciale, gestione delle commesse, acquisti, ...).

La ISO/IEC 20000-1, emessa nel 2005, serve per modellare i principali processi di gestione dei servizi informatici. Per approfondimenti merita tenere presente anche la ISO/IEC 20000-2:2005.

La ISO/IEC 27001 del 2005 riporta i requisiti minimi per la pianificazione e gestione delle misure di sicurezza delle informazioni. Tra questi, l'elaborazione di un Risk Assessment e l'implementazione di misure coerenti con i rischi individuati. Altri standard collegati alla ISO/IEC 27001 sono: la ISO/IEC 27002:2005 sulle misure di sicurezza e la ISO/IEC 27005:2008 sulla conduzione del Risk Assessment e conseguente gestione del rischio.

La ISO/IEC 9126-1:2007, infine, riporta una modalità di valutazione della qualità del software. La norma non tratta solo dei requisiti funzionali, ma anche di altri aspetti che dovrebbero essere presi in considerazione quando un'azienda sviluppa o acquista del software.

10. Conclusioni

Questo scritto vuole essere un invito a vedere l'applicazione dei requisiti legali in un'impresa non più come emanazione di nuove regole o istruzioni al personale, ma in congiunzione con una revisione dei processi dell'impresa, in modo che i requisiti siano recepiti con maggiore efficacia ed efficienza.

Per gestire un'impresa seguendo un approccio per processi e per disporre di una ottima base di conoscenza in merito alle più consolidate modalità di organizzazione di alcune aree di un'impresa, sono stati prese come riferimento alcune norme ISO e i loro principi fondamentali.

Gli esempi fatti evidenziano come l'approccio per processi e l'applicazione dei principi delle norme ISO possano dare buone garanzie di corretta applicazione dei requisiti legali.

11. Appendice: Carta di Pescara

Nell'ambito di ECL 2009, è stato richiesto ai relatori di fornire alcuni spunti per quanto riguarda la normativa sulla privacy.

Nell'ambito dell'intervento effettuato, mi sono permesso di fare alcune riflessioni che elenco qui di seguito.

- Attuare il ciclo di miglioramento anche a livello istituzionale: a seguito dei controlli e delle domande effettuate all'Ufficio del Garante (Check), mettere a disposizione (Act) interpretazioni
    - > chiare ed esaurienti (la risposta alla FAQ 14 sul Provvedimento del 27 novembre 2008 sugli Amministratori di Sistema è un esempio di come non dovrebbero essere fornite tali interpretazioni)
    - > facilmente accessibili (alcune interpretazioni, ancorché non ufficiali, sono riportate solo dalla stampa e non dal sito web del Garante, peraltro non facilmente navigabile e con funzionalità di ricerca molto carenti)
    - > opportunamente pubblicizzate (sulla newsletter del Garante, a cui è anche difficile iscriversi, visto che la relativa pagina web è messa in scarsa evidenza, sono riportate solo alcune notizie: a solo titolo di esempio, non sono mai state riportate le notizie dell'emissione del Provvedimento del 27 novembre 2008, del suo aggiornamento con le FAQ, della sua proroga).

- Il Dlgs 196/2003 presenta alcune incongruenze. Per esempio, viene richiesto di pianificare la formazione sul DPS, ma non c'è alcuna richiesta di effettuarla, riducendo il ciclo Plan-Do-Check-Act alla sola prima fase.

- Riesaminare le misure riportate nell'allegato B alla luce della norma ISO/IEC 27002:2005 (già ISO/IEC 17799:2005 e BS 7799-1).

- Sottolineare l'importanza di misure sostanziali (p.e. il non uso di utenze generiche del punto 3 o l'attestazione da parte dei fornitori del punto 25), oggi raramente applicate (Do), al posto di misure formali come il DPS (oggetto di troppe discussioni), spesso associate alla fase di Pianificazione del ciclo Planb-Do-Check-Act, a cui non sempre segue la parte di realizzazione.

- Promuovere la pubblicazione di modelli (es. DPS) per ridurre le spese necessarie alla "sicurezza formale".