



Conformità = ROI

Come trasformare i requisiti normativi
in un impulso per il business

Executive Summary

Nel nuovo panorama normativo, delineato da direttive quale quella dell'Unione Europea sulla protezione dei dati o dal Sarbanes-Oxley Act, i responsabili tecnologici e commerciali sono alle prese con il compito di garantire che le attività IT e i processi gestionali siano conformi ai complessi requisiti di governance.

Secondo un articolo pubblicato sulla rivista *CIO Insight*, il 65 % dei CIO prevede infatti che le iniziative volte a garantire una buona *corporate governance* saranno per i prossimi due anni un'importante fonte di distrazione dalle attività di business.

Negli anni recenti molte aziende hanno tentato con maggiore o minor fortuna di conformarsi ai vari requisiti, uno per volta. Ma questo approccio ha spesso portato a iniziative costose e non ben mirate, che richiedevano continui aggiustamenti. I CIO più avveduti hanno però scoperto che si ottengono risultati migliori se i manager adottano una visione olistica della conformità aziendale.

Anziché considerare ogni normativa come una sfida isolata e a sé stante, i CIO più all'avanguardia ora elaborano le iniziative di conformità secondo un

approccio ad ampio spettro, essenzialmente servendosi di processi gestionali standardizzati per garantire una copertura generale volta a soddisfare più normative.

Questo è quanto succede presso Computer Associates International Inc., (CA). La società di Islandia, New York, ha adottato una visione olistica della conformità sia al proprio interno, per le proprie attività aziendali, che all'esterno, per i clienti alla ricerca di soluzioni di attuazione della compliance che fossero anche migliorative della performance aziendale, della gestione delle identità digitali, della sicurezza e dell'archiviazione e del recupero dei dati.

Una strategia olistica di successo è caratterizzata da sei requisiti essenziali:

1. Un deciso coinvolgimento del management esecutivo
2. Opportuni sistemi di controllo aziendale
3. Verifiche regolari
4. Formazione ad ampio spettro e comunicazioni regolari
5. Meccanismi di feedback che coinvolgano i dipendenti
6. Piani d'azione correttivi e disciplinari efficaci destinati a risolvere le inosservanze in materia di conformità

Al servizio del business

Le aziende più accorte hanno assunto manager di lunga esperienza che conoscono a fondo le normative in materia di conformità. Vi presentiamo alcuni degli esperti di compliance di CA.



Nome: Robert W. Davis

Titolo: Executive Vice President, Chief Financial Officer

Background: Già Vice President of Corporate Finance e Chief Accounting Officer presso Dell Inc., è diventato Chief Accounting Officer di CA nel 2002. Ha iniziato la sua carriera in Price Waterhouse dapprima come Staff Accountant e ben presto nel dipartimento SEC Services della casa di consulenza. Collabora strettamente con il CEO John Swainson e con team di manager per garantire che le attività IT e commerciali di CA siano adeguatamente allineate ai requisiti di conformità.



Nome: Kevin Kern

Titolo: Senior Vice President e CIO

Background: Kern porta con sé la sua esperienza in campo internazionale, elemento essenziale a proposito di conformità. In passato ha rivestito la carica di CIO presso la divisione EMEA (Europa, Medio Oriente e Africa) di Compaq Computer. È responsabile a livello globale della strategia, dello sviluppo e del deployment delle risorse IT - compresi data center, sistemi e applicazioni, sicurezza dei sistemi e networking.



Nome: Patrick J. Gnazzo

Titolo: Senior Vice President, Business Practices e Chief Compliance Officer

Background: Collabora strettamente con Kenneth V. Handal, Executive Vice President e General Counsel, e con il Compliance Committee del Consiglio di amministrazione di CA. È responsabile dello sviluppo e dell'implementazione di un programma globale di conformità ed etica. Si occupa inoltre di sovrintendere all'osservanza delle norme di legge e alla creazione di un programma di gestione delle informazioni e dei documenti aziendali. In passato ha fatto parte del Consiglio di amministrazione della Ethics Officers Association e tiene spesso conferenze riguardanti l'etica e la conformità normativa.

Sebbene le strategie di attuazione della compliance siano diverse da azienda ad azienda, le iniziative capaci di dare i risultati attesi hanno vari elementi chiave in comune. Innanzitutto, la conformità non può prescindere da un opportuno investimento finanziario. PricewaterhouseCoopers riporta che il 51% delle multinazionali americane ed europee aumenteranno la spesa media destinata all'attuazione della conformità di un buon 23% nel corso dei prossimi 12 - 24 mesi. In secondo luogo, la conformità è una necessità per tutti i tipi di aziende, siano esse pubbliche, private, grandi, medie o piccole. Le start up ad azionariato privato, ad esempio, devono aderire ai criteri delle norme GAAP (Generally Accepted Accounting Principles) per agevolare possibili IPO (Initial Public Offering) o per attirare più facilmente potenziali acquirenti. Inoltre, le società a capitale privato e le società non statunitensi devono spesso dar prova della loro conformità normativa per poter intrattenere relazioni commerciali con grandi società quotate in borsa che vogliono garantire a tutti i propri soci operazioni commerciali trasparenti. In terzo luogo, la compliance presuppone un'efficace collaborazione in particolare fra CEO, CFO, CIO, consulenti legali e Chief Compliance Officer di un'azienda, ma in generale fra tutti i dirigenti.

Questo livello di comunicazione è essenziale, perché la definizione di conformità aziendale continua a cambiare. I dirigenti inoltre ricevono spesso pareri e indicazioni contraddittorie dai vari revisori. Le normative internazionali in materia di conservazione dei dati e di procedure aziendali sono spesso in contrasto fra loro. L'imminenza della scadenza dell'adeguamento alle normative, poi, induce le organizzazioni a cercare delle scorciatoie, come ad esempio documentare un processo gestionale superato, anziché soluzioni efficaci nel lungo periodo, come l'automazione di tali processi.

Adottando una visione olistica della conformità, le organizzazioni possono vincere queste sfide e adeguarsi in modo più efficace alle nuove normative che si profilano all'orizzonte.

Il primo passo - Il punto di vista di un CIO

Il tempo è un bene prezioso per John Halamka. Nella sua veste di Chief Information Officer della Harvard Medical School, Halamka fa gli straordinari per soddisfare una serie di requisiti normativi, dal garantire la riservatezza dei dati degli studenti all'impedire l'accesso non autorizzato alle cartelle cliniche.

Sei regole verso la conformità

- 1. Dare l'esempio.** La conformità normativa inizia dai vertici. Il management deve prendere sul serio e ritenersi responsabile dell'attuazione della compliance.
- 2. Implementare controlli appropriati.** Adottare processi e procedure adeguati per proteggere le attività dell'azienda da danni accidentali o intenzionali.
- 3. Svolgere i controlli con regolarità.** Rivedere le procedure di controllo con cadenza regolare e rafforzare quanto prima gli anelli più deboli della catena.
- 4. Formare e comunicare con regolarità.** Informare i dipendenti su ciò che ci si attende da loro per mezzo di comunicazioni regolari in forma scritta ed elettronica, a cui far eventualmente seguire discussioni verbali.
- 5. Dare ascolto alle critiche.** Predisporre un processo che permetta ai dipendenti di esprimere le proprie preoccupazioni senza timore di conseguenze. Ad esempio creare una hot line per comunicazioni anonime.
- 6. Agire opportunamente e con rapidità.** Quando sorgono dei problemi di conformità, eseguire un controllo e, se opportuno, adottare misure disciplinari o correttive.

"Il tempo che dedico alle problematiche di conformità è sempre di più," osserva con rammarico Halamka. "È necessario rendersi conto che non esiste il prodotto magico in grado di soddisfare tutte le esigenze di compliance. Essa richiede invece una serie di processi e soluzioni, e una sorveglianza continua."

Sono molti i CIO che condividono il punto di vista di Halamka. Secondo un articolo della rivista *CIO Insight*, un buon 87% dei reparti IT aziendali è formalmente coinvolto nel processo di continuo adeguamento alla conformità normativa e il 46% dei CIO prevede per il 2005 un aumento della spesa IT destinata alla compliance.

In tutto il mondo, i senior executive IT sono alle prese con la necessità di soddisfare decine di requisiti di conformità a normative locali, statali, federali e internazionali. In generale, tali normative sono finalizzate a garantire la riservatezza delle informazioni sui clienti, la sicurezza dei dati e l'integrità delle informazioni, migliorando nel contempo i controlli finanziari e i processi gestionali generali.

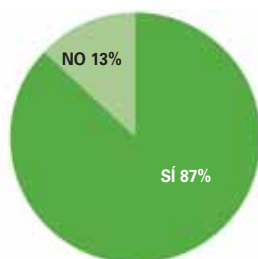
Il cammino verso la conformità non è facile. Molte organizzazioni reinventano la ruota ogni volta che passano da un'iniziativa di conformità (ad esempio la Direttiva UE in materia di protezione dei dati) alla successiva (ad esempio il Sarbanes-Oxley). Anziché affrontare ciascuna di esse in modo isolato, le organizzazioni più attente scelgono l'approccio olistico

alla conformità, adottando una serie di processi, soluzioni software e servizi IT generalmente applicabili a tutti i principali requisiti normativi attuali (vedi l'elenco delle normative). Molte di queste organizzazioni all'avanguardia si rifanno a sei regole fondamentali per raggiungere e mantenere la conformità normativa (v. riquadro pagina precedente).

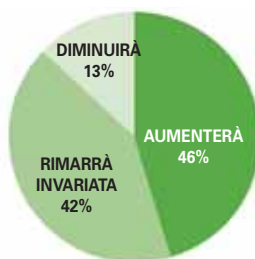
Prima regola - Iniziare dall'alto

La prima regola riguarda esclusivamente i dirigenti. Senza un coinvolgimento serio e costante del top management dell'azienda, le iniziative di conformità sono destinate a incontrare difficoltà o al fallimento

Il reparto IT della vostra azienda partecipa formalmente al processo di attuazione della conformità normativa in corso?



Come cambierà la spesa per la conformità normativa della vostra azienda nel 2005?



L'impegno per adeguarsi alle normative sarà un'importante fonte di distrazione dalle attività di business per i prossimi due anni?



Fonte: CIO INSIGHT

totale. "Grazie all'interesse dei manager, le aziende stanno iniziando a pensare alla compliance più come a un insieme di 'best practices' piuttosto che come a una semplice 'legge' da osservare," afferma Sanjay Anand, autore del testo "The Sarbanes-Oxley Guide for Finance and Information Technology Professionals", una guida alla normativa Sarbanes-Oxley per operatori finanziari e IT. "In altre parole, ora accettiamo la compliance come una componente necessaria delle attività di business e dell'impegno a mantenersi onesti. Il timore, l'ostilità e l'inosservanza della normativa e delle iniziative legate alla conformità stanno cominciando a lasciare il passo alla cooperazione, al riconoscimento di opportunità e al rispetto."

Questo è quanto sta succedendo in CA. "Dobbiamo poter contare su un atteggiamento di condivisione a partire dal consiglio di amministrazione in giù," afferma Robert Davis, Chief Financial Officer di CA a Islandia, N.Y. E Patrick Gnazzo, Senior Vice President, Business Practices e Chief Compliance Officer presso CA, aggiunge: "Il management deve prendere sul serio e ritenersi responsabile dell'attuazione della compliance."

Il consiglio di amministrazione di CA comprende anche un Compliance Committee che si riunisce formalmente almeno otto volte all'anno. Dopo l'avvento del Sarbanes-Oxley Act, questo comitato è divenuto ancora più attivo e comunica regolarmente con il Presidente e CEO di CA John Swainson, con il CFO Davis, il CCO Gnazzo, il Senior Vice President e CIO Kevin Kern e con altri protagonisti del processo di conformità.

Il Consiglio svolge inoltre un ruolo di primo piano nel reclutare per CA dirigenti esperti di compliance e nel garantire che il portafoglio di prodotti di CA comprenda soluzioni orientate alla conformità normativa. Di questi dirigenti fa parte Gnazzo, arrivato in CA nel gennaio del 2005 con il compito di sviluppare e implementare un programma completo di conformità ed etica. Egli è inoltre responsabile dell'osservanza delle norme di legge e ha introdotto in CA un programma di gestione delle informazioni e dei documenti aziendali.

Dirigente con una lunga esperienza nell'ambito della compliance, Gnazzo occupava precedentemente una posizione simile presso la United Technologies Corp., società da 36,7 miliardi di dollari produttrice di sistemi di costruzione e prodotti per il settore aerospaziale. Faceva inoltre parte del consiglio di amministrazione della Ethics Officers Association (www.eoa.org), un'organizzazione leader comprendente i più importanti esperti di compliance al mondo.

Mentre molte società hanno cominciato a prendere sul serio la conformità solo negli ultimi due o tre anni, Gnazzo si occupa di queste problematiche da oltre vent'anni. Nel 1986, United Technologies è stata una delle 32 società fornitrici del Dipartimento della Difesa che ha sottoscritto l'iniziativa dell'industria della difesa Defense Industry Initiative su Business Ethics and Conduct (nota come DII, www.dii.org). I membri hanno recepito e implementato una serie di principi di etica aziendale nell'intento di eliminare una presunta cattiva condotta commerciale di alcuni fornitori del settore della difesa.

L'esperienza di Gnazzo con il DII e United Technologies, dove occorre programmi di conformità per oltre 200.000 dipendenti in 180 paesi, è di buon augurio per CA. "Pat è una delle menti migliori del settore in tema di compliance," afferma il CIO di CA Kern.

Pensare in modo globale

Invece di affrontare il problema della conformità regione per regione, le aziende devono adottare una visione globale. Questo è possibile soltanto se il team dei senior executive ha un'esperienza di livello internazionale e familiarità con le prassi e le normative locali dei vari paesi del mondo.

"Il nostro CEO [Swainson] ed io siamo appena stati in Giappone dove è stata approvata di recente una severa normativa sulla riservatezza delle informazioni sui consumatori," racconta il CFO di CA Davis. "È necessario essere al corrente di queste normative in quanto riguardano vari settori dell'industria e paesi diversi."

"La natura umana non cambia di molto da paese a paese," aggiunge il CCO di CA, Gnazzo. "Le differenze fra una regione e l'altra sono culturali. Per

implementare un programma di conformità che possa essere definito internazionale, è necessario tener conto delle varie culture. In alcuni paesi un regalo da 250 dollari per un partner commerciale può essere appropriato e ragionevole, in altri potrebbe essere contro le regole."

Gnazzo si affida anche a suoi collaboratori sparsi in tutto il mondo per mettere a punto dei programmi localizzati di conservazione dei documenti. "Non possiamo gestire i documenti aziendali da un'unica postazione centrale ubicata negli Stati Uniti. Dobbiamo chiedere ai nostri collaboratori in tutto il mondo di stabilire quali sono per loro i documenti più importanti e quali leggi ne regolano la conservazione."

L'esperienza di CA in campo internazionale copre tutte le attività IT e commerciali dell'azienda stessa. Il CIO Kern, ad esempio, in precedenza svolgeva la medesima funzione presso la divisione EMEA (Europa, Medio Oriente, Africa) di Compaq Computer. Ai tempi Compaq era una società da 15 miliardi di dollari con attività molto complesse, ricorda Kern. "Avevo a che fare con implementazioni locali, normative sulla riservatezza dei dati e altre leggi internazionali spesso più rigide di alcune norme sulla conformità degli Stati Uniti," afferma.

E Davis, CFO, aggiunge: "In quei casi devi individuare le normative più severe e soddisfarle, poi puoi anche rilassarti un attimo e soddisfare tutte le altre normative relative al tuo settore"

Seconda regola - Implementare controlli appropriati

Una volta costituito un team di provata esperienza responsabile della conformità, si passa a documentare e valutare tutte le procedure gestionali. In questa fase, molte aziende scoprono di avere procedure antiquate o manuali non conformi alle normative correnti. Alcune organizzazioni ad esempio non prevedono una separazione dei compiti fra personale di vendita, dirigenti finanziari e altri reparti dell'azienda.

CA si avvale del proprio software come pure della piattaforma software di classe enterprise di SAP AG per garantire che vengano effettuati i controlli opportuni. In particolare, l'iniziativa Global Computing Controls (GCC) della società utilizza soluzioni BrightStor per la gestione, la protezione e il recupero dei dati, eTrust per il controllo degli accessi e le attività di auditing e amministrazione, ed eTrust CA-TopSecret Security per la protezione dei sistemi operativi e dei database aziendali.

Inizialmente, l'implementazione dei controlli

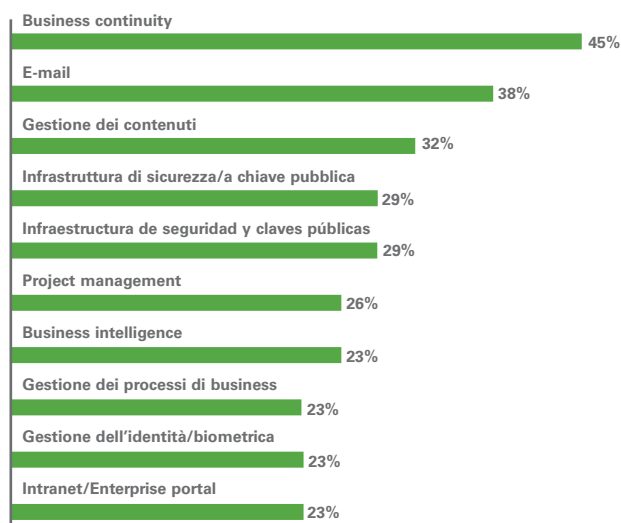
Indicare due fra le categorie seguenti che hanno ricevuto la quota maggiore di finanziamenti supplementari per la conformità nel budget 2005



Fonte: CIO INSIGHT

appropriati può sembrare un'impresa titanica. Ma i senior executive possono sfruttare svariati standard fondamentali come punti di partenza e semplificare così il processo. Ad esempio possono adottare il COBIT (Control Objectives for Information and related Technology), un diffuso standard metodologico messo a punto dalla Information Systems Audit and Control Association e dall'IT Governance Institute, pubblicato nel 1996 e aggiornato regolarmente. Secondo la definizione dell'istituto, il COBIT rappresenta un insieme di obiettivi di controllo generalmente accettati per tutti i sistemi informativi aziendali, ovvero personal computer, minicomputer, mainframe e ambienti distribuiti. Esso si basa sul concetto che le risorse IT devono essere gestite da un insieme di processi raggruppati per affinità naturale al fine di fornire le informazioni pertinenti e affidabili di cui, nell'opinione dell'istituto, necessita un'organizzazione per raggiungere i propri obiettivi. Mentre il COBIT,

Quali dei prodotti software o dei sistemi seguenti ha acquistato o intende acquistare la vostra società per attuare la conformità normativa?



Fonte: CIO INSIGHT

adottato da società dislocate in oltre 100 paesi, è focalizzato su un'efficace IT governance, ITIL (IT Infrastructure Library) è un'infrastruttura di gestione di processi e servizi, più pratica nel suo approccio alla gestione IT del COBIT; inoltre, secondo Forrester Research di Cambridge, Massachusetts, essa opera a un livello più capillare rispetto a quello delle infrastrutture di governance tradizionali.

La metodologia ITIL si articola in una serie di documenti contenenti linee guida su come fornire

servizi IT di qualità e sulle infrastrutture logistiche e di ambiente necessarie per supportare l'IT secondo quanto stabilito dall'Office of Government Commerce di Norwich in Gran Bretagna.

Un altro importante standard di controllo è l'ISO (International Organization for Standardization) 17799. Sebbene le metodologie COBIT e ITIL si riferiscano alla necessità della sicurezza IT e ne illustrino le caratteristiche, secondo Forrester esse tuttavia non forniscono direttive dettagliate a proposito della struttura pratica della sicurezza e dei controlli IT. Né ITIL né COBIT, quindi, sono sufficientemente specifici circa la sicurezza delle informazioni al punto di soddisfare le esigenze di un'organizzazione a questo particolare livello. È in quest'ambito che abbiamo invece assistito a un'adozione generalizzata della ISO17799 (BS7799), norma su cui è basato lo schema intorno a cui viene costruita un'architettura di sicurezza informatica. Come già altri schemi di base, la ISO17799 fornisce una struttura all'interno della quale sviluppare e organizzare i controlli specifici per la propria realtà operativa, per quanto, riferisce Forrester, essa non provveda automaticamente a "riempire gli spazi vuoti" durante il processo di documentazione.

Oltre a implementare standard orientati ai controlli, le società continuano a investire pesantemente in software e servizi IT in linea con i requisiti di conformità. Secondo la rivista *CIO Insight*, il 45% delle organizzazioni intende infatti acquistare quest'anno software di business continuity, seguito da software di tracciabilità delle e-mail (38%), gestione dei contenuti (32%) e financial reporting (29%).

CA ha anche acquistato società fornitrici di soluzioni software che supportano significativamente le iniziative di conformità aziendale. Netegrity Inc., acquistata nel novembre 2004, offre a CA e ai suoi clienti robuste soluzioni software di gestione delle identità e degli accessi. Ora incluso nella suite di Identity and Access Management di eTrust, il software di Netegrity garantisce che gli utenti possano accedere soltanto ai sistemi aziendali che sono autorizzati a utilizzare. Un'altra società acquisita di recente, Niku, sviluppa software di gestione del ciclo di vita dell'IT che permette ai manager di vedere in tempo reale il portafoglio di investimenti IT dell'organizzazione, consentendo di gestire l'infrastruttura informativa come business vero e proprio. CA sta integrando le soluzioni di IT-MG (Management and Governance) di Niku nella divisione Business Service Optimization, BSO, di CA. Le soluzioni CA di cui è responsabile la divisione BSO consentono alle organizzazioni di allineare gli investimenti IT agli obiettivi aziendali, controllare i costi IT, fornire l'IT come servizio e soddisfare requisiti di conformità sempre più severi.

Fusioni e conformità

Se non attuate correttamente, le acquisizioni possono in realtà vanificare gli sforzi compiuti per soddisfare i requisiti di conformità. È un fatto che svariate fusioni e acquisizioni ad alto profilo sono fallite perché una o entrambe le società coinvolte non avevano adottato misure adeguate in termini di conformità.

Quando meditano un possibile connubio di aziende, i manager potrebbero trovare vantaggioso adottare l'approccio di CA in tema di fusioni e acquisizioni. Il CIO di CA, Kern, è "fortemente coinvolto" negli incontri preliminari di discussione della fusione. Collaborando strettamente con Michael J. Christenson, Executive Vice

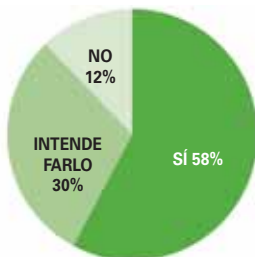
President di Strategy and Business Development di CA, Kern valuta attentamente l'altra società, abbinando persone, processi e tecnologie gli uni agli altri. "Acquisisco tutte le informazioni del caso per capire se una fusione ha senso da un punto di vista strategico e sono anche in grado di individuare eventuali problemi di conformità in ambito IT che dovranno essere investigati o risolti."

Kern collabora strettamente anche con i team di sviluppo di CA per garantire che prodotti nuovi ed esistenti soddisfino le esigenze di conformità dei clienti. "Il nostro ruolo va ben oltre il fornire semplici pareri al team di sviluppo," spiega Kern. "Abbiamo infatti un ruolo formale che prevede l'approvazione finale di tutti i prodotti e delle soluzioni software che rilasciamo. Diamo il nostro feedback sulla qualità del software, la redditività degli investimenti prevista e il TCO (Total Cost of Ownership)."

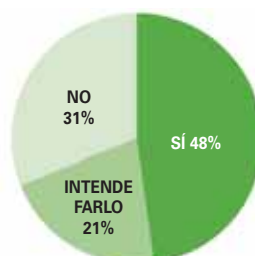
La vostra società prevede che il CIO certifichi i risultati finanziari?



La vostra società ha sviluppato un processo per il monitoraggio costante dell'efficacia delle misure di attuazione della conformità?



La vostra società ha nominato un Chief Compliance Officer o una figura equivalente che sovrintenda alle attività di attuazione della conformità normativa?



Fonte: CIO INSIGHT

Terza regola - Svolgere i controlli con regolarità

CIO Insight riporta che circa il 60% delle società ha implementato processi per il monitoraggio continuo dell'efficacia delle iniziative di conformità adottate, e un ulteriore 30% ha in programma di sviluppare tali processi nel corso del prossimo anno.

Molti CIO paragonano le scadenze relative all'adeguamento alle normative di oggi al panico per l'anno 2000 del 1999. Allora le aziende erano in corsa con il tempo per controllare miliardi di righe di codice e, se necessario, aggiornare le applicazioni per supportare le date a quattro cifre, ovvero "2000", in alternativa a quelle a due cifre, ovvero "00".

A differenza del problema dell'anno 2000, però, le iniziative di conformità di oggi richiedono un'applicazione costante e ripetuti controlli. "La maggior parte delle società è in attesa di capire che vento tira fra i revisori e come reagisce il mercato a esiti di controlli interni non proprio cristallini," afferma Larry White, presidente del consiglio di amministrazione dell'Institute of Management Accountants (www.imanet.org), che conta più di 70.000 membri. "Le aziende stanno cominciando a capire che [la conformità] non è uno di quei grandi eventi che si verificano una volta sola, seguiti da un improvviso calo di attenzione. Se si vuole mantenere la conformità, non si può mollare la presa. Le aziende dovranno cominciare a cercare soluzioni per rendere più efficiente il lavoro di tutti i giorni."

John Halamka della Harvard Medical School ha qualcosa da dire in proposito. "Sei mesi fa pensavamo

di aver predisposto tutti i controlli necessari per le nostre policy di security,” ricorda Halamka. “Ma i nuovi attacchi e i malware più recenti ci hanno costretto a modificare le nostre policy e a sviluppare nuovi strumenti di valutazione per capire se qualcuno qui utilizza software peer-to-peer o altre applicazioni contrarie alle nostre policy.”

L'approccio proattivo della Harvard Medical School nei confronti della conformità non è tuttavia condiviso da molte organizzazioni che, invece, affrontano i problemi man mano che si presentano. “Si tende a rispondere al fuoco senza elaborare processi sostenibili efficienti,” osserva con rammarico White. “In particolare per quanto riguarda la Sarbanes-Oxley, le organizzazioni tendono ad applicare una logica di controllo alle

Le frecce al vostro arco

Alcune delle soluzioni IT di attuazione della conformità normativa offerte da CA

Gestione della sicurezza. eTrust Compliance Platform di CA è un insieme di soluzioni integrate che consentono alle aziende di semplificare significativamente e automatizzare i controlli IT interni, componente essenziale di un valido programma di conformità normativa.

Business Service Optimization. Le soluzioni sviluppate dalla divisione Business Service Optimization di CA sostengono le iniziative di conformità grazie alla capacità di supportare sia i controlli a livello di applicazione che i controlli di carattere generale in ambito IT. Le soluzioni BSO possono abilitare l'automazione dei processi e dei controlli IT con il più ampio supporto delle metodologie ITIL (gestione degli inconvenienti, dei problemi, delle modifiche, della configurazione e delle versioni del software).

Gestione dell'infrastruttura IT. Gli strumenti di gestione dell'infrastruttura IT possono essere utilizzati dalle organizzazioni per elaborare best practice di impatto economico contenuto, volte a migliorare al massimo la disponibilità della rete e dei sistemi, a garantire la business continuity e offrire metodi consolidati di financial reporting in cui convergono informazioni da fonti e sistemi molteplici disseminati nell'organizzazione.

Gestione dello storage. Le soluzioni di gestione dello storage di CA offrono alle organizzazioni l'opportunità di valorizzare al massimo gli investimenti in risorse di memorizzazione dei dati e soddisfare le esigenze di storage supplementare derivanti dalla necessità di conformarsi alle disposizioni governative e alle policy aziendali. CA fornisce soluzioni integrate di gestione dello storage e disponibilità dei dati atte a gestire il patrimonio informativo dal laptop al mainframe.

verifiche, ma non attingono alle tecniche di monitoraggio continuo dei processi, tipiche della produzione industriale, per controllare la qualità.”

Anche le modifiche del codice di applicazioni legacy possono minare gli sforzi compiuti per soddisfare i requisiti di conformità. “Nel mondo IT, molti fra i programmatori migliori e i membri dello staff ricorrono a degli espedienti per intervenire sui sistemi legacy,” osserva Chellappa Kumar, CIO del New York College of Osteopathic Medicine (NYCOM), la seconda scuola di medicina più grande degli Stati Uniti, ubicata a Old Westbury, New York. “Queste persone non lascerebbero mai intenzionalmente libero accesso ai dati, ma questi espedienti possono creare inavvertitamente le condizioni perché ciò succeda.”

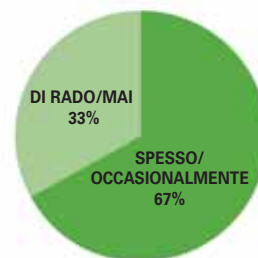
Quarta regola - Informare

Naturalmente, qualsiasi misura di controllo aziendale orientata all'implementazione della conformità non vale nulla senza una comunicazione e una formazione degli utenti adeguate. “Comunicare la filosofia di base e una formazione adeguata in itinere sono per le società le due aree più irte di ostacoli quando si tratta di conformità,” afferma Anand, esperto di compliance e autore di successo.

“Pur a fronte del dovuto coinvolgimento del top management e di investimenti sufficienti in sistemi e tecnologia, la preparazione dei dipendenti in relazione all'importanza della conformità e nel come utilizzare correttamente gli strumenti a disposizione, è l'area in cui le aziende sono più carenti.”

“Il training e il riorientamento culturale sono due dei più importanti fattori di successo per un'implementazione riuscita della conformità normativa,” aggiunge Chellappa Kumar del NYCOM, che dedica circa il 20% del suo tempo alle

Con che frequenza il CIO incontra il Chief Counsel per parlare della conformità normativa?



Fonte: CIO INSIGHT

problematiche di compliance. “È essenziale far sì che il personale prenda sul serio il problema della conformità. Spesso vedo che le organizzazioni cercano soltanto una soluzione tecnica, dimenticando che devono convincere i dipendenti di quanto sia importante la conformità.”

Al NYCOM Kumar tiene ogni mese degli incontri di carattere pratico con gli utenti, durante i quali vengono prese in esame le problematiche correnti in fatto di processi e le possibili soluzioni tecniche dei problemi individuati. Altre organizzazioni hanno inserito materiale sulla compliance nei documenti di HR, nelle intranet e nella newsletter elettronica mensile indirizzata ai dipendenti

Quinta regola - Dare ascolto alle critiche

Se una società si dimostra carente in termini di compliance, i dipendenti devono avere a disposizione dei canali di comunicazione che consentano loro di esprimere le proprie perplessità senza timore di conseguenze. Questi possono essere costituiti da una hot line per comunicazioni anonime o da account di posta elettronica anonimi che diano ai dipendenti la possibilità di rendere note le proprie osservazioni. “Oltre a fare in modo che questi canali di comunicazione vengano creati, occorre anche accertarsi che tutti i dipendenti siano a conoscenza della loro esistenza,” ha sottolineato Ed Golod, presidente di Revenue Accelerators, una società di New York specializzata in servizi di consulenza strategica per i manager.

L'Health Science Center dell'Università del Texas, ad esempio, mette a disposizione un numero verde tramite il quale i dipendenti possono denunciare in forma anonima casi sospetti di violazione delle leggi federali o statali o del regolamento dell'università. Inoltre i dipendenti possono utilizzare la hot line dedicata alla conformità per porre quesiti in caso di

dubbio su come comportarsi in una particolare situazione.

Tutte le accuse di presunte violazioni vengono riportate all'Office of Legal Affairs and Institutional Compliance dell'Health Science Center dell'Università del Texas per approfondimento. L'origine della chiamata non viene rintracciata, né le chiamate vengono registrate e il centro non dispone di funzioni di identificazione del chiamante. Agli anonimi che chiamano viene tuttavia fornito un numero di segnalazione che possono utilizzare per richiamare la hot line dedicata alla conformità per aggiornamenti sulla questione sollevata. I dipendenti che chiamano la hot line sono protetti contro ritorsioni o altre conseguenze dalla legge statale e federale e dal regolamento dell'università.

Anche CA ha creato una hot line dedicata alla conformità etica. Durante le riunioni del comitato di controllo della società, Gnazzo esamina lo stato di tutte le chiamate con i membri del comitato per garantire che tutte vengano attentamente analizzate.

Sesta regola - Agire opportunamente e con rapidità

Quando sorgono dei problemi di conformità, le aziende devono eseguire un controllo e, se opportuno, adottare misure disciplinari o correttive.

Secondo il parere di Faegre & Benson, uno studio legale di Minneapolis, Minnesota, le aziende dovrebbero decidere come condurre delle indagini in materia di conformità prima di trovarsi ad affrontare un'accusa o una denuncia specifica. Molto importante, nell'opinione dello studio, è decidere se condurre l'inchiesta internamente (e in tal caso chi dovrebbe farlo) o se rivolgersi a un investigatore esterno. La seconda soluzione potrebbe giocare a favore dell'indipendenza e della credibilità dell'inchiesta,

Spesa mondiale in risorse di gestione delle informazioni per la conformità - Per segmento (milioni di \$)

	2004	2005	2006	2007	2008	2009	2004-2009 CAGR (%)
Software	2.741	3.839	5.292	6.764	8.219	9.650	28,6
Hardware	1.063	1.483	2.068	2.723	3.498	4.346	32,5
Servizi	3.719	4.191	4.702	5.269	5.850	6.484	11,8
Totale	7.523	9.513	12.062	14.756	17.567	20.480	22,2

SOURCE: IDC, "WORLDWIDE INFORMATION MANAGEMENT FOR COMPLIANCE 2005.2009 FORECAST", IDC #33024, MARZO 2005

facilitare l'interazione con i revisori della società in relazione al raggio d'azione e ai risultati dell'inchiesta e rendere più semplice la gestione delle questioni riguardanti il cosiddetto "attorney-client privilege" ("privilegio avvocato-assistito" mirante a consentire uno scambio d'informazioni completo e libero fra avvocato e assistito, tutelando la riservatezza delle comunicazioni e dei documenti correlati all'inchiesta o all'erogazione di una consulenza legale).

Un altro aspetto importante è fare in modo che l'investigatore abbia accesso libero e immediato a tutti i documenti pertinenti; ciò implica che le aziende devono avere sistemi di archiviazione e conservazione dei dati efficaci e adeguati alle normative in essere e a quelle di una potenziale introduzione futura di ulteriori regole.

"Il numero e la rigosità delle normative in materia di conformità aumenterà piuttosto che diminuire," sostiene Anand. "Questo è dovuto all'evoluzione socio-economica del business e della società.

Assisteremo inoltre a una diminuzione esponenziale dell'ostilità nei confronti di questa legislazione negli anni a venire, man mano che impariamo ad adattarci alle nuove realtà delle funzioni manageriali e della responsabilità aziendale. La conformità normativa continuerà a cercare di salvaguardare l'onestà delle persone, a tutto vantaggio del maggior numero di soggetti interessati e degli azionisti."

Il CCO di CA, Gnazzo, conclude: "Qualcuno deve assumersi la responsabilità globale di garantire che vi sia un coordinamento fra i requisiti di conformità attuali e futuri."

In CA e in altre società avanzate questa responsabilità globale investe innanzitutto il Consiglio di amministrazione, estendendosi a CEO, CFO, CIO e Chief Compliance Officer. Facendo leva su questo capitale intellettuale e sugli strumenti IT appropriati, le aziende possono raggiungere e mantenere un'efficace conformità normativa.

Per ulteriori informazioni: www.ca.com/it/compliance



Computer Associates®