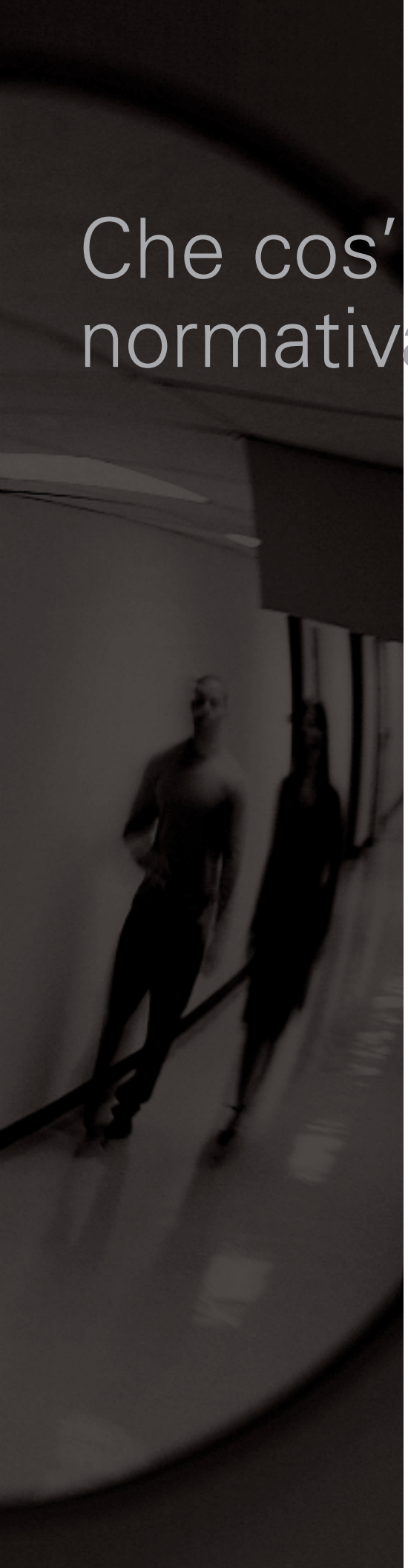
Conformità normativa = ROI

Come allinearsi ai requisiti normativi per massimizzare il ritorno degli investimenti IT



Che cos'è la conformità normativa?

LA CONFORMITÀ NORMATIVA È LA FUNZIONE GESTIONALE che assicura la piena osservanza di tutte le norme e i regolamenti, sia che disciplinino più settori economici (quali il Sarbanes-Oxley Act) sia che riguardino uno specifico settore (Basilea II) o abbiano carattere federale (OMB Circular A-123).

Le organizzazioni hanno la responsabilità di adottare, monitorare e convalidare policy, procedure e attività di controllo della conformità normativa e di intervenire rapidamente con misure correttive e verifiche continue per garantire l'efficacia di tale osservanza e il rispetto degli obblighi documentali in materia.

La conformità normativa deve rappresentare una priorità strategica per ogni azienda, tenuto conto delle gravi conseguenze che può produrre quando disattesa. Le soluzioni CA per la gestione della conformità possono aiutare le organizzazioni ad automatizzare tali processi ed essere così in grado di fornire immediatamente le informazioni richieste alle persone appropriate, di monitorare i vari tipi di politiche e di adottare automaticamente misure correttive e tenere traccia della risoluzione dei problemi al fine di assicurare la costante osservanza dei dettami delle autorità governative e degli organismi normativi.

Lo scopo di questa brochure è delineare i concetti chiave della conformità normativa e mostrarvi come massimizzare il ROI dell'investimento IT.

Requisiti comuni in materia di conformità normativa

Trasparenza globale
- Acquisire una visione più chiara dei rischi e delle prestazioni aziendali
- Preservare il valore e la fiducia degli azionisti

Acquisire la conformità con investimenti razionali
- Migliorare l'efficienza operativa
- Ridurre i costi
- Adottare quadri operativi adattivi e flessibili
- Automatizzare i controlli

Conformità vincolante a normative vincolanti
- Sviluppare e documentare policy, procedure e controlli sostenibili e ripetibili
- Garantire la definizione dei ruoli e degli accessi appropriati
- Apportare valore all'azienda capitalizzando gli impegni assunti in materia di conformità per migliorare le decisioni aziendali

Gran parte dei controlli di conformità è incentrata sull'IT. Ecco perché è importante esaminare l'Internal Control Framework (quadro di controllo interno) dell'azienda:

- Controlli dei processi
- Controllo dell'accesso ai sistemi
- Procedure di doppio controllo
- Procedure di modifica dei sistemi (gestione dei cambiamenti)
- Controlli di integrità
- Monitoraggio/Reporting
- Programmi per rispondere alle esigenze aziendali
- Procedure di emergenza e di ripristino

Perché la conformità normativa è vitale per il DNA della vostra organizzazione?

Oggi, il rispetto delle normative governative travalica i confini della conformità legale e giunge a rappresentare una funzione critica del business. Si può anzi dire che, per essere realmente conforme, l'organizzazione deve avere la conformità tra i suoi fattori organici costitutivi: in altre parole, fissata nel suo DNA.

Un'azienda richiede un quadro operativo, una cornice funzionale e una struttura gestionale complessiva che possano fungere da base propulsiva per realizzare maggiori efficienze, indipendentemente dal mutare dei requisiti normativi in vigore. Analogamente, la conformità normativa richiede la capacità di tradurre gli aspetti critici del business e dell'osservanza delle normative in soluzioni concrete per l'intera organizzazione - con il supporto dell'IT.

Processi, controllo degli accessi, gestione delle identità, storage management e gestione della configurazione sono componenti fondanti del DNA stesso della conformità normativa, un DNA che può aiutare ad affrontare un ampio spettro di aspetti relativi alla conformità e al governo societario. Sono la risposta a un'esigenza che non è di un solo giorno, ma che abbraccia l'intero arco di vita delle informazioni aziendali.

Affrontare tutte le sfide proposte dalla conformità normativa con un programma e una piattaforma unici e completi è senz'altro il metodo più efficace. Le società che si rivelano proattive, coerenti ed esaustive nel loro impegno per la conformità possono non solo superare tali sfide, ma anche favorire la maggiore efficienza delle loro attività. Viceversa, le società che affrontano la conformità normativa con riluttanza si trovano a pagare il prezzo più alto e a ricavare benefici minimi dagli impegni assunti.

Noi di CA siamo perfettamente a conoscenza della sovrapposizione di molti aspetti critici della conformità normativa. Per questo consigliamo alle aziende di adottare un insieme di requisiti di controllo comuni - un quadro e una cornice operativa per la conformità - che si fondino su una serie di procedure ottimali che includono l'adozione degli standard COBIT, ITIL, COSO e ISO 17799.

Gestione e riduzione dei rischi con gli

Internal Control Framework

Gli Internal Control Framework sono le attività interne a un processo aziendale, in un'area e a un livello qualsiasi dell'azienda, deputate alla gestione o alla riduzione dei rischi. I controlli possono essere preventivi o reattivi ed essere condotti manualmente o in modo automatico. I controlli IT si applicano alle risorse IT e alla relativa struttura di governo.

In ossequio agli standard COSO, perché un controllo sia efficace è necessario che siano rispettati cinque elementi chiave. Le soluzioni software CA per la gestione dell'IT offrono un supporto fondamentale per la soddisfazione dei requisiti evidenziati in blu.

Ambiente di controllo

- Controllo sulle attività IT decentralizzate
- Titolarità delle applicazioni e dei dati
- Separazione delle mansioni
- Atteggiamento dei vertici aziendali rispetto all'IT
- Struttura dell'organizzazione IT
- Reclutamento, formazione e valutazione del personale IT
- Policy, procedure e standard IT

Valutazione dei rischi

- Gestione del portafoglio IT
- Gestione delle richieste IT
- Gestione dei programmi IT
- Gestione dei cambiamenti IT
- Gestione del livello di servizio IT
- Gestione del rischio IT
- Esistenza di una metodologia SDLC
- Pianificazione delle strategie IT
- Gestione delle ottimizzazioni e delle verifiche IT
- Gestione dei fornitori IT
- Gestione dell'outsourcing IT

Informazioni e comunicazioni

- Gestione delle conoscenze IT
- Gestione e reporting dei programmi IT
- Comunicazioni tra reparti contabili e settore IT
- Coinvolgimento e soddisfazione degli utenti IT

Attività di controllo

- Documentazione dei processi IT
- Documentazione dei sistemi e dei controlli
- Separazione delle mansioni IT
- Controlli delle applicazioni automatizzate
- Utilizzo delle informazioni generate dal sistema
- Procedure di controllo dei cambiamenti
- Protezione dei dati e delle risorse IT correlate
- Procedure di backup delle applicazioni e dei dati
- Disaster Recovery/Business Continuity
- Verifiche dei contratti per il software

Monitoraggio

- Analisi e governo delle risorse IT
- Rilevamento delle intrusioni
- Verifiche interne all'IT
- Monitoraggio delle prestazioni IT

Termini chiave

COSO High-Level:

Il rapporto del Committee of Sponsoring Organizations della Treadway Commission (COSO) "Internal Control-Integrated Framework".

COBIT:

Control Objectives for Information and related Technology. Introdotto nel 1996, il COBIT consiste nella definizione di un insieme di procedure comunemente applicate e accettate in materia di controllo e di governo delle tecnologie informatiche (IT), il cui scopo è colmare il divario tra rischi aziendali, esigenze di controllo e problematiche tecniche da una parte e procedure documentali ottimali dall'altra.

ISO 17799:

Un insieme completo e riconosciuto a livello internazionale di procedure ottimali per la sicurezza delle informazioni.

ITIL:

L'IT Integration Library è una risorsa sviluppata nel 1983 da un'agenzia governativa britannica per la valutazione delle attività IT delle imprese aggiudicatarie di pubblici appalti. In essa sono definiti i processi e le attività a supporto dei servizi IT.

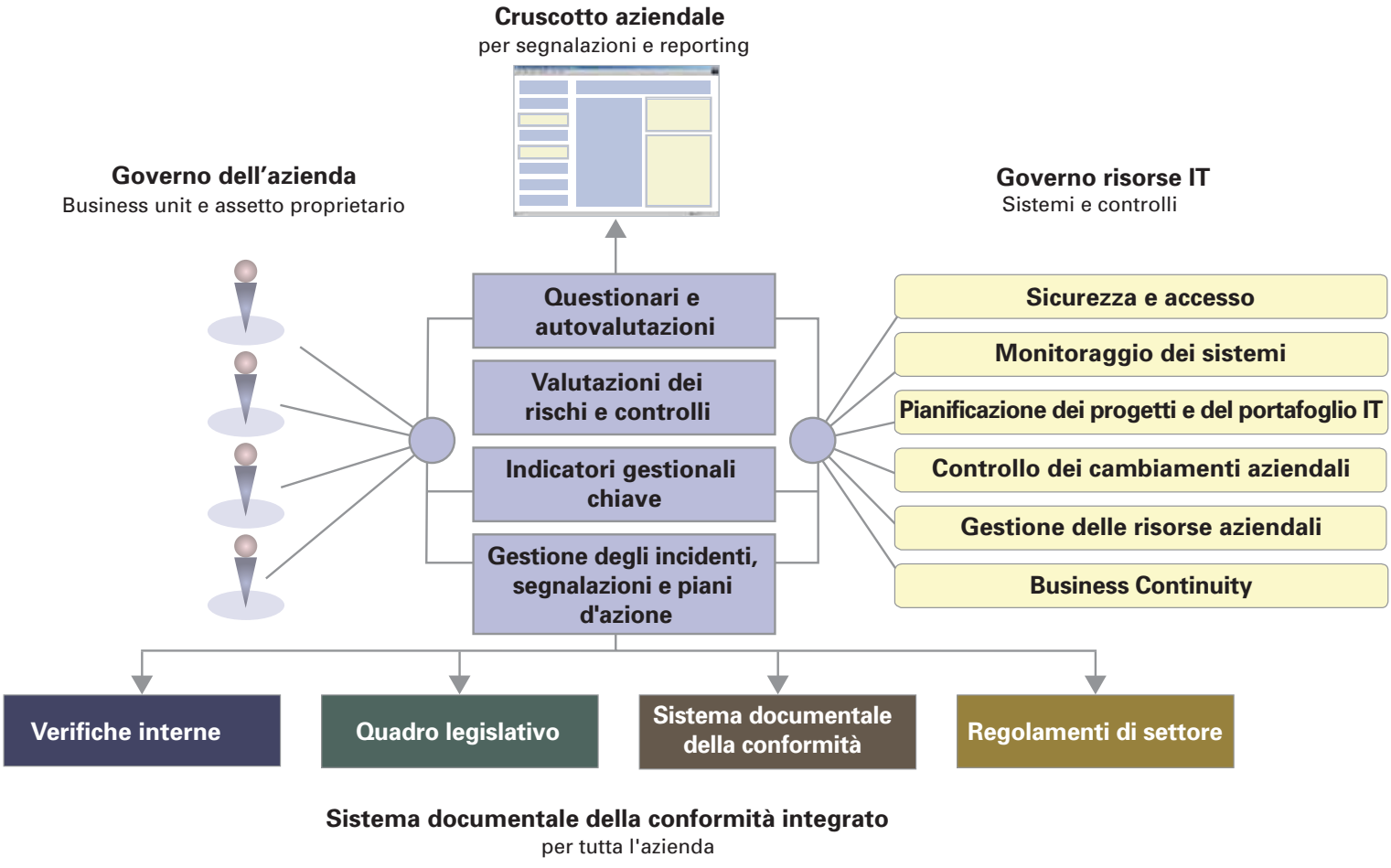
L'importanza dell'IT

L'assunzione delle decisioni e la gestione delle attività richiedono la disponibilità di informazioni complete e accurate da parte delle aziende. I sistemi IT sono quelli che forniscono tali informazioni.

In assenza di informazioni complete e accurate, le aziende non hanno la garanzia che i rischi vengano gestiti. È qui che entra in campo la tecnologia: per supportare i processi di gestione dei rischi.

Pensate alla vostra organizzazione come a una casa. L'IT ne rappresenta le fondamenta o l'infrastruttura su cui poggiano l'intelaiatura e le altre strutture di supporto. La presenza di punti deboli nelle fondamenta della casa-azienda può essere causa di crepe (lacune) o di conseguenze persino più gravi: il collasso della struttura aziendale nelle forme della frode o del fallimento.

Gestione integrata dei rischi e della conformità



La realizzazione di un programma di conformità sostenibile

Per realizzare un programma di conformità sostenibile, le società devono creare un'infrastruttura di conformità su tre livelli che consenta l'adozione di azioni affidabili e ripetibili. Tre livelli di successo che CA può aiutarvi a conseguire:

Unificare le risorse umane

- Creare ex novo o ridisegnare ruoli e incarichi per la definizione e l'assegnazione delle responsabilità in materia di conformità e divulgazione delle informazioni
- Stabilire iniziative formative, inclusi nuovi programmi e standard
- Favorire un sistema di comunicazione variato e aperto in seno all'intera organizzazione

Migliorare i processi

- Definire processi per la valutazione, la verifica, l'ottimizzazione, il monitoraggio e la certificazione dei controlli interni su base trimestrale e annua
- Integrare le attività di identificazione dei rischi, di valutazione dei controlli e di monitoraggio nell'ambito della gestione quotidiana dei controlli interni
- Migliorare la comprensione dei processi aziendali
- Stabilire processi guida per la gestione della conformità

Ottimizzare la tecnologia

- Valutare e implementare fattori tecnologici a supporto della gestione dei controlli interni
- Progettare e implementare tecnologie migliorative dei processi di controllo e di monitoraggio
- Implementare un cruscotto aziendale che fornisca un quadro delle informazioni di controllo e di monitoraggio finanziario e dei processi interni, dei parametri di qualità e dello stato di conformità normativa
- Sviluppare capacità di monitoraggio, reporting e analisi in tempo reale
- Sfruttamento delle tecnologie esistenti e/o implementazione di nuove tecnologie

I vantaggi della conformità normativa in termini di gestione

Un approccio proattivo, coerente ed esaustivo alla conformità può aiutarvi ad acquisire maggiori efficienze e a ridurre i costi, attraverso un triplice miglioramento delle prestazioni aziendali:

Riducendo i rischi

- Riduzione degli eventi critici nell'ambito delle pubbliche relazioni
- Riduzione delle violazioni minori alla sicurezza, con conseguente risparmio di risorse
- Visione più chiara della situazione aziendale per una reattività più appropriata
- Maggiore agilità

Favorendo l'efficienza

- Migliore comprensione e ottimizzazione dei processi di controllo interno esistenti
- Riduzione del carico sulle risorse di help desk (fino al 50% delle richieste di assistenza riguarda la reimpostazione delle password)
- Maggiore produttività del personale, che accede più rapidamente alle applicazioni interne grazie al provisioning automatico degli account
- Riduzione dei costi operativi (la gestione centralizzata di tutte le identità e degli accessi degli utenti riduce i costi amministrativi)

Aumentando l'efficacia

- Migliore comprensione e ottimizzazione dei processi di controllo interno esistenti
- Migliore accesso a informazioni aggiornate con conseguente ottimizzazione delle attività di definizione del budget, di pianificazione e di analisi
- Maggiore competitività
- Processo decisionale più efficiente
- Maggiore agilità nel cogliere le nuove opportunità
- Automazione dei controlli per una maggiore trasparenza

Perché scegliere CA per ogni esigenza in materia di conformità?

La conformità normativa è ormai una realtà acquisita e la tendenza è verso l'aumento della sua complessità con l'aumentare delle norme e dei regolamenti emanati. Ogni sforzo mirato sembra destinato a trasformarsi in un inesauribile "buco nero" di risorse, tempo e finanze. Eppure una soluzione c'è.

Una piattaforma di conformità ben congegnata e implementata può tradursi in significativi benefici in termini di miglioramento delle prestazioni aziendali. Adottate la conformità come una strategia e utilizzatela per far crescere la vostra azienda!

Le soluzioni CA per la conformità tutelano la privacy e la sicurezza delle informazioni e aiutano a gestire e controllare le modifiche ai sistemi e ai dati per supportare le iniziative in ambito di conformità normativa. Inoltre favoriscono l'automazione, offrono protezione contro l'accesso non autorizzato e aiutano a identificare le attività non conformi.

Vasta e completa, la gamma delle soluzioni software CA per l'automazione dei controlli gestionali richiesti dalla conformità assicura al contempo la soddisfazione dei requisiti a breve termine e, sfruttando l'investimento con l'adozione di procedure ottimali, quella delle mutevoli e complesse esigenze del futuro.

- CA è costantemente impegnata a sviluppare uno spettro di prodotti software per l'impresa che favoriscono il flusso e il controllo delle informazioni aziendali critiche

- CA è in grado di offrire soluzioni indipendenti dalla piattaforma, adatte a qualsiasi hardware e sistema operativo

- Il software CA per la gestione dell'IT apporta valore all'azienda, migliorando la qualità complessiva del business e la redditività, e generando inoltre un ROI misurabile

- Il software CA per la gestione dell'IT consente ai clienti di soddisfare i requisiti specifici delle varie normative

- Le soluzioni CA per la gestione dell'IT forniscono un valido supporto per automatizzare i processi, ridurre la complessità e abbreviare il time-to-value

Nella visione di CA, **la conformità è fatta di persone, processi e tecnologie, NON di prodotti.**

Soluzioni CA = maggior ritorno degli investimenti IT

Gestione della sicurezza

eTrust® Compliance Platform è un set integrato di soluzioni che consente alle aziende di semplificare e automatizzare significativamente i controlli IT interni: un componente chiave per il successo di qualsiasi programma di conformità normativa. Questa piattaforma offre funzionalità di gestione delle identità e degli accessi, provisioning, monitoraggio e verifiche di sicurezza in un'unica soluzione completa e integrata. Grazie a essa, i clienti possono potenziare i controlli IT interni per assicurare maggiore protezione e privacy ai dati in ogni scenario aziendale.

Ottimizzazione dei servizi aziendali

Le soluzioni CA per l'ottimizzazione dei servizi aziendali (BSO, Business Service Optimization) supportano le iniziative aziendali per la gestione della conformità e dei rischi, automatizzando le attività di controllo delineate dal COBIT (sia a livello di applicazione che a livello più generale di IT) con il più ampio supporto dei processi ITIL (gestione degli incidenti, dei problemi, dei cambiamenti, delle configurazioni e delle release, gestione dei livelli di servizio e gestione finanziaria). Le soluzioni BSO di CA forniscono informazioni in tempo reale sul complesso delle risorse IT aziendali in relazione a desktop, licenze e servizi; assicurano un meccanismo di controllo standardizzato per la gestione, la registrazione e la documentazione delle modifiche apportate ai sistemi IT e, infine, offrono una visione dettagliata dei progetti, delle risorse e del personale IT.

Gestione dei sistemi aziendali

Le soluzioni CA per la gestione dei sistemi aziendali (ESM, Enterprise Systems Management) supportano la conformità normativa dell'infrastruttura IT attraverso l'integrazione della gestione delle attività proprie di questo settore dell'impresa. Esse consentono di sfruttare gli investimenti esistenti in tecnologie gestionali, assicurando che reti e sistemi siano gestiti in modo appropriato, che processi ed eventi siano automatizzati per l'ottimizzazione, che applicazioni e database siano amministrati in un'ottica di efficienza e che desktop e server vengano predisposti e configurati accuratamente.

Gestione dello storage

Le soluzioni di storage management di CA consentono alle organizzazioni di massimizzare il valore degli investimenti in tecnologie di storage e di adeguarne razionalmente gli ulteriori requisiti per soddisfare le normative governative e le policy societarie. CA offre soluzioni di storage management e disponibilità dei dati integrate con cui gestire tutte le risorse informative, dai laptop al mainframe, con un approccio conveniente e scalabile alla protezione e al ripristino efficiente dei dati in caso di incidenti. Grazie alle soluzioni intelligenti di CA per lo storage management, le organizzazioni possono semplificare, gestire con sicurezza e proteggere le risorse informative e di storage, garantendone al contempo l'allineamento ottimale agli obiettivi aziendali.

Per ulteriori informazioni, visitare il sito ca.com/it/compliance.