

GOVERNARE LA COMPLIANCE E IL NON-COMPLIANCE RISK

SOMMARIO

<i>GRC Overview</i>	1
<i>Il nostro approccio integrato</i>	2
<i>Il Tool Dynasec</i>	3
<i>Adfor Service Portfolio</i>	4

Notizie di rilievo:

Recenti studi indicano che le società che sono comprese in Fortune 1000 sono soggette a circa 35-40 tra normative e regolamenti e che la gestione di tutti questi regolamenti è diventato un grave fattore di rischio.

A causa della complessità normativa, i costi relativi di GRC per le imprese sono in crescita esponenziale. Ad esempio, secondo un recente studio SIA, il costo di conformità sulla sicurezza negli Stati Uniti è quasi raddoppiato in tre anni arrivando fino a \$ 25 Miliardi di euro nel 2006.

"Le aziende che, per ogni sfida che hanno sul fronte normativo, selezionano singole soluzioni spenderanno 10 volte di più per la componente IT dei progetti delle imprese che seguono un approccio più integrato e proattivo.". Gartner Group

IL PARADIGMA GRC

Oggi l'evolversi non solo del business, ma anche dei regolamenti e delle normative nazionali ed internazionali, da recepire attraverso l'adeguamento continuo dei processi interni e delle regole da applicare, introduce nelle organizzazioni una continua e crescente complessità.

GRC, acronimo di "Governance-Risk-Compliance", è un nuovo paradigma di management che vuole sottolineare le strette interrelazioni fra le tre componenti. Con GRC si intende l'insieme delle attività, in sinergia fra loro, che hanno l'obiettivo di assicurare il continuo allineamento tra Governance aziendale, controllo e mitigazione dei Rischi e Compliance ai regolamenti ed alle normative di riferimento.

L'approccio integrato fra le attività di GRC consente di trasformare ciò che possono essere considerati dei vincoli in opportunità per creare valore, mediante la promozione di una cultura aziendale che incentivi la trasparenza, il rispetto delle norme, il controllo e la prevenzione dei rischi e l'efficienza delle performance, qualità che gli stakeholder ed i clienti apprezzano in misura

sempre maggiore.

Il rispetto nel tempo di ogni specifico regolamento e delle sue evoluzioni e modifiche, sia esso derivante da una nuova normativa di legge sia interno, può essere complicato, lungo e costoso: emerge una nuova classe di rischio, il non-compliance risk. E' il rischio che i processi organizzativi e produttivi non siano completamente aderenti alle normative, complice la crescente complessità e pervasività delle regole. Per ogni Azienda diventa evidente l'esigenza di una piattaforma GRC integrata con la quale gestire la complessità degli adempimenti e, soprattutto, minimizzare il rischio di non conformità, che può tradursi in perdite economiche anche rilevanti e rischi talvolta di natura penale. Nonostante in generale si dichiarino un alto livello di attenzione al tema, solo poche Organizzazioni sono riuscite finora a dotarsi di una piattaforma di gestione realmente integrata.



LA SITUAZIONE ATTUALE

La maggior parte delle Aziende ha in essere una gestione della compliance, sebbene il paradigma GRC non sia ancora diffuso ed applicato. Ciò porta ad un approccio "in silos", ovvero adottando differenti metodologie e diverse soluzioni software per ciascun ambito di intervento, che rimangono "soluzioni a sè stanti" con difficoltà nella valutazione delle mutue implicazioni e minima possibilità di riutilizzo dei controlli e delle informazioni.

L'approccio "per silos" porta all'insorgere di criticità, in particolare:

- incoerenza tra i vari settori di intervento;
- difficoltà nel costruire una visione unificata dei rischi e della compliance che finisce per ridurre l'efficacia del processo decisionale;
- proliferare di strumenti destrutturati ed inadeguati (come i fogli excel), nei quali tuttavia vi si trasferisce molto know-how;
- duplicazioni di attività e sovrapposizioni degli sforzi che aumentano i costi e gli impegni di gestione, a fronte di una minore sicurezza.

IL NOSTRO APPROCCIO INTEGRATO

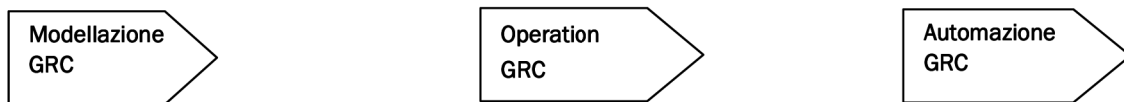
Un approccio integrato alla GRC ha come obiettivo la costruzione di un ambiente che permetta contestualmente di:

- gestire ciascun processo GRC in modo completamente autonomo;
- fornire strumenti per la definizione di relazioni complesse, la condivisione di informazioni e il collegamento tra le diverse norme, regolamenti e controlli.

Dynasec ha definito una metodologia per una definizione e gestione efficiente dei processi GRC, chiamata GRC Modelling. Essa si basa su:

- Definizione di un'unica terminologia GRC: l'adozione di un glossario comune è essenziale per migliorare l'efficacia della comunicazione all'interno dell'organizzazione riguardo ad una tematica nuova;
- Creazione di una struttura organizzativa unificata: migliora l'efficacia delle valutazioni in quanto consente una valutazione del rischio e dell'efficacia dei controlli sull'intero ciclo di vita del processo;
- Granularità a livello di rischio e delle esigenze di controllo. Infatti, vi è un rapporto "multi-a-molti" tra rischi e controlli. Un controllo che ricorre in due regolamenti distinti, potrebbe essere di fondamentale importanza per un regolamento e meno importante per l'altro e la capacità di definire il livello di granularità opportuno in tutti i punti dove agisce un controllo è fondamentale per il successo di un approccio integrato.
- Definire le relazioni gerarchiche tra i controlli, affinché l'azione di governo e mitigazione intervenga all'opportuno livello di dettaglio in dipendenza della granularità definita. Ciò è fondamentale al fine di ridurre la duplicazione dei controlli sulle diverse procedure di compliance proofing e, contestualmente, favorire la linearità ed uniformità delle azioni di verifica e risoluzione delle non conformità. Per esempio, un elevato livello di controllo derivante da un regolamento ad impatto su un certo processo può essere coincidente con la combinazione di 5 controlli incidenti su un altro processo, che necessita di azioni ad un livello di granularità maggiore. La capacità di definire "smart link" che colleghino gerarchie multilivello tra i rischi, controlli e processi GRC è di vitale importanza per la riduzione dell'overhead di gestione e di test in tutta l'azienda e consentire un piano organico di governo.

Lo sviluppo di una strategia completa e integrata di GRC si articola su tre fasi logiche:



In questa fase viene disegnato ed impostato il modello di controllo e l'integrazione dei diversi flussi di lavoro in ambito GRC.

Le principali attività di questa fase sono:

- La definizione di un linguaggio comune;
- La predisposizione di una struttura organizzativa appropriata;
- La definizione delle gerarchie tra rischi, controlli e moduli (modelli di controllo);
- La definizione delle relazioni "multi-a-molti" tra gli attributi dei rischi, dei controlli e le altre entità coinvolte;
- La modellizzazione dei flussi di informazioni fra le varie unità.

Fase in cui vengono specificate le modalità con le quali ogni singola azienda del gruppo o unità utilizzerà la piattaforma software per svolgere le attività GRC ad essa assegnate.

Le principali attività di questa fase includono:

- Processo di documentazione;
- Valutazione ponderata dei rischi e dei controlli;
- Dashboard e modalità di reporting;
- "What-if" analysis degli eventuali interventi di mitigazione e soluzione delle non conformità e debolezze riscontrate;
- Pianificazione degli interventi di soluzione delle non conformità, mitigazione dei rischi;
- Valutazione dei "valori a rischio" (perdite potenziali);
- Altro.

Dopo che le operazioni GRC in corso sono state modellate ed avviate, i processi GRC possono evolvere verso un'automazione più "spinta". In questa fase, i processi GRC (tutti o in parte) possono essere interfacciati in modalità "diretta" con l'organizzazione e i sistemi on-line risparmiando così ulteriormente tempi e impegni rispetto ad una automazione governata da processi manuali.

L'evoluzione può richiedere un certo tempo per andare a regime e necessitare di dati storici per la costruzione di specifiche metriche di valutazione automatica, quali:

- Tracciabilità degli eventi di perdita e serie storiche;
- Valorizzazione e monitoraggio dei Key Risk Indicator;
- Valorizzazione e monitoraggio dei Key Performance Indicator;
- Identificazione delle anomalie di comportamento per BCP e/o degli Scenari di gestione delle frodi.



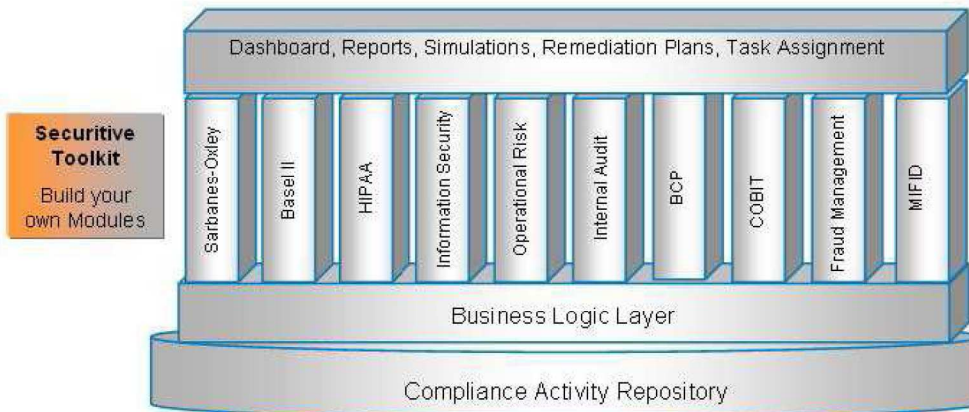
Dynasec Enterprise è una piattaforma software web based, che consente alle imprese di controllare e gestire con continuità le conformità, la governance e il rischio dei processi della macchina operativa, con una serie di strumenti di GRC Modeling. Ci sono 5 gruppi di applicazioni GRC supportate:

- **Operational Risk Management (ORM)**, include i moduli come il generale ORM, Basilea II, Solvency.
- **Internal Control Management (ICM)**, include i moduli per il Controllo Interno, la SOX, il Tabaksbat, ecc
- **IT Risk and Governance (ITG)**, include i moduli: Cobit, ITIL, ISO17799, ISO27001, Business Continuity Planning (BCP)
- **Internal Audit Management (IA)**
- **General Compliance (GC)**, per particolari esigenze come la governance d'impresa e le relative procedure, progetti speciali, leggi locali, e altro ancora.

IL TOOL

Dynasec fornisce gli strumenti e le funzionalità necessarie per la progettazione integrata del Flusso di lavoro e dei dati tra i diversi progetti GRC, fornendo per ogni modulo software la serie completa di funzionalità, un unico flusso di lavoro e, se pertinenti, le relative best practice.

Il modello di dati di Dynasec è composto da 4 strati logici costruito come un unico modello dei dati. È questa architettura intelligente, che consente la condivisione delle informazioni tra i vari progetti GRC, l'eliminazione della ridondanza tra rischi e controlli e l'abilitazione ad ogni progetto che permette di gestire separatamente, per un determinato periodo di tempo, la metodologia, i flussi di lavoro e i report necessari.



- Il layer di base è un repository che memorizza tutti i soggetti che fanno parte dei progetti GRC, come: unità organizzative, processi, sotto-processi, sistemi, rischi, controlli, eventi di perdita, scenari e altri.
- Il secondo layer fornisce strumenti che consentono di utilizzare la modellazione GRC - la creazione di relazioni complesse tra l'entità dei dati e i flussi di lavoro in modo da facilitare il concetto di multi regolamentazione integrata.
- Il terzo layer è il livello delle applicazioni per i diversi moduli GRC. Ogni Applicazione è composta dalla metodologia pertinente, le funzionalità e la Flusso di lavoro necessari per i suoi requisiti specifici.
- Il quarto layer è uno strato di gestione, che consente la comunicazione, il coordinamento, e la misurazione dei processi GRC.
- Gli utenti autorizzati possono creare e visualizzare report, cruscotti, piani di bonifica e di simulazioni, segnalazioni e notifiche, e altro ancora.

The screenshot shows the **DYNASEC Secureitive™ Enterprise Edition** interface. The top navigation bar includes **Logout**, **Wizard**, **Definition**, **Documentation**, **Testing**, and **Reporting**. The user is logged in as **admin** from the **IT Dep.** in **Europe**. The main content area displays a **Compliance Chart** for the **IT Dep.** under the **Testing > Qualitative by Process** view. The chart shows compliance percentages for various processes, with bars indicating the current status and target levels.

Process	Compliance	Control Level	Weight	Compliance Chart
Access Control	43.59 %	High	8.33%	43.59% 15.46% 46.95%
Asset Classification & Control	53.46 %	High	8.33%	53.46% 20.78% 25.76%
Business Continuity Management	67.74 %	High	8.33%	67.74% 9.68% 32.58%
Communications	69.46 %	High	8.33%	69.46% 8.38% 22.17%
Compliance	29.44 %	High	8.33%	29.44% 15.56% 55%
ISMS requirements	76.67 %	High	8.33%	76.67% 13.33% 10%
Organizational Security	81.02 %	High	8.33%	81.02% 7.41% 11.57%
Personnel Security	34.34 %	High	8.33%	34.34% 31.31% 34.34%
Physical & Environmental Security	34.2 %	High	8.33%	34.2% 7.36% 58.44%
Risk Assessment	25.56 %	High	8.33%	25.56% 11.11% 63.33%
Security Policy	90.91 %	High	8.33%	90.91% 9.09%
Systems Development & Maintenance	71.19 %	High	8.33%	71.19% 11.43% 17.38%
Overall Compliance	56.47			56.47% 17.65% 30.88%

adfor

Adfor Spa
Via Columella, 40
20100 Milano
Tel. +39 02 25201411

info@adfor.it
www.adfor.it

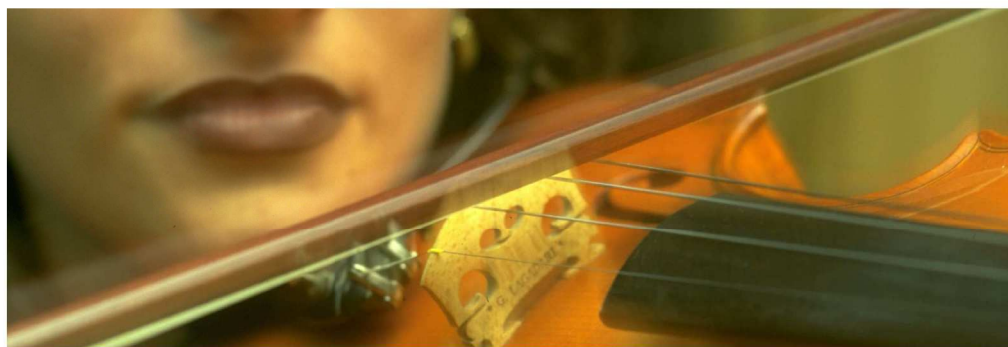
Adfor

Adfor, nata nel 1986, è una società indipendente di servizi di Consulenza organizzativa, direzionale e ICT, Formazione manageriale e tecnologica, sviluppo e distribuzione di applicazioni software, gestione e sviluppo delle risorse umane. Adfor aiuta le aziende e le pubbliche amministrazioni nella realizzazione del cambiamento e nel governo delle complessità progettuali, organizzative e tecnologiche, al fine di ottenere l'eccellenza necessaria a supportare e sviluppare il business. Adfor collabora con l'Università Cattolica di Milano per l'offerta di corsi di Alta Formazione in ICT Management e di Alta Formazione in Project Management. L'attività di Consulenza sviluppata fin dagli anni '90, in sinergia con le altre divisioni ha consentito e consente ai Clienti di affrontare con successo le sfide del mercato ottenendo risultati significativi e misurabili.

Dynasec

Fondata nel 2002, Dynasec fornisce, a livello mondiale, una soluzione di GRC integrato (Governance, Risk e Compliance), infatti la sua piattaforma software per la gestione di più Norme e Regolamenti, quali: il controllo interno, Sarbanes-Oxley (SOX), Basilea II Operational Risk, solvibilità, Cobit, Itil, I SO17799, ISO27001, Internal Audit, Business Continuity Planning (BCP), la lotta antifrode gestione, e altro ancora.

L'elenco delle aziende che hanno implementato l'approccio multi regolamento di Dynasec annoverano tra le altre: Rabobank, Mitsui Sumitomo Insurance, Dexia, Arag Assicurazioni, Electricity Company di Israel, Cellcom Mobile di Israel, Banca Hapoalim e molti altri.



ADFOR SERVICE PORTFOLIO

- Assessment degli standard di gestione esistenti e gap analysis GRC
- Censimento dei processi, delle normative e dei controlli esistenti e normalizzazione per set-up iniziale dello strumento
- Set-up iniziale di Securitive Enterprise mediante caricamento delle informazioni normalizzate
- Ottimizzazione ed evoluzione delle informazioni all'interno di Securitive Enterprise
- Predisposizione dei dashboard di valutazione del rischio
- Predisposizione dei dashboard per il reporting direzionale
- Supporto al risk self assessment, alla valutazione degli esiti e degli interventi di miglioramento
- Supporto alle attività di auditing e di valutazione delle non conformità
- Supporto all'evoluzione della piattaforma informativa (nuove norme, regolamenti, controlli, dashboard, ecc.)