protiviti® Insights

Face the Future with Confidence

Settembre GOVERNANCE, RISK E COMPLIANCE 2020

a cura di / **Emma Marcandalli**
Managing Director

VERSO SISTEMI DI CONTROLLO INTERNO E DI GESTIONE DEI RISCHI DI NUOVA GENERAZIONE: LA VISIONE DI PROTIVITI SUPPORTATA DALLE SOLUZIONI SAP GRC

Immagina se la tua organizzazione potesse disporre di una visione olistica e integrata dei rischi e dei controlli aziendali; se potesse parlare un unico linguaggio condiviso e coerente in tema di rischi e controlli; se potesse eliminare sovrapposizioni e ridondanze, evitare disallineamenti e inefficienze, evidenziare interdipendenze, agevolare interlocuzione e coordinamento fra il business e le funzioni aziendali che operano sui Sistemi di Controllo Interno e di Gestione dei Rischi (SCIGR).

Immagina se tali funzioni potessero capitalizzare il patrimonio di dati e informazioni disponibili nei sistemi informativi aziendali per automatizzare le attività di controllo di secondo e terzo livello, intercettare con tempestività situazioni di rischio, anomalie o frodi su cui intervenire rapidamente, ampliare in modo efficiente il perimetro di verifica e monitoraggio del sistema di controllo interno; in definitiva, rendere più oggettive, affidabili e complete le evidenze sui rischi e sulle debolezze del sistema di controllo interno.

Immagina se il Management e i Vertici aziendali potessero disporre di un "Tableau de Board" di monitoraggio dei rischi e dei controlli di tutta l'azienda (ai vari livelli organizzativi, geografici e di business), che permettesse loro di intercettare/conoscere le criticità sulle quali intervenire per riportare le *performance* e il profilo di rischio associato a livelli di accettabilità, nonché di valutare consapevolmente l'adeguatezza complessiva del SCIGR.

Immagina, infine, se tutto ciò potesse essere fatto "*real-time*", con un quadro di sintesi sempre aggiornato, e nel rispetto dei principi rigorosi di tracciabilità, trasparenza e auditabilità.

Integrazione e **automazione** finalizzate alla semplificazione e all'efficienza sono dunque, nella visione di Protiviti, le parole d'ordine che devono guidare le aziende moderne e innovative nel percorso di trasformazione dei propri SCIGR, verso soluzioni di nuova generazione.

La buona notizia è che oggi l'immaginazione può diventare realtà. Dal nostro punto di osservazione, infatti, possiamo affermare che la tecnologia ha ormai fatto passi da gigante anche negli ambiti di Governance, Risk e Compliance (GRC) e ha finalmente raggiunto la maturità necessaria per realizzare:

a) l'automazione integrata e condivisa dei processi GRC,

b) l'analisi avanzata di dati complessi per finalità di controllo nonché

c) la possibilità di monitorare nel continuo l'efficacia ed effettiva operatività dei sistemi di controllo interno.

Tutto ciò anche avvalendosi di un'unica piattaforma software, come quella proposta da SAP con la sua **SUITE GRC**, che si compone di soluzioni - nativamente integrabili fra loro e con l'ERP SAP - in grado di soddisfare tutte le esigenze delle funzioni che operano sul SCIGR, rispettando al contempo le esigenze IT di semplificazione e ottimizzazione dell'architettura applicativa aziendale.
Il presente Insight approfondisce il nostro punto di vista sui SCIGR di nuova generazione e sugli errori che si possono evitare ricorrendo ad una piattaforma GRC completa e integrata, come quella proposta da SAP, che supporta la visione olistica proposta da Protiviti.

LO SCENARIO DI "VECCHIA" GENERAZIONE

Non è infrequente, in organizzazioni complesse, trovare più di una funzione aziendale che, a vario titolo, opera sui Sistemi di Controllo Interno e di Gestione dei Rischi, ancorché con focus, obiettivi e perimetri d'azione in tutto o in parte differenti.

A titolo esemplificativo e non esaustivo, citiamo, al secondo livello di controllo:

- le funzioni ERM e Compliance di Gruppo con ambiti d'azione diversificati da azienda ad azienda;
- le strutture Finance a presidio dei rischi finanziari, fiscali (anche in ottica Tax Control Framework) e di financial reporting (anche in ottica compliance ex L. 262/2005);
- le strutture HR/HSE a presidio dei rischi di salute e sicurezza sui luoghi di lavoro e della compliance alle normative HSE applicabili;
- le funzioni Legali/Affari Regolatori a presidio di tematiche ex D.Lgs. 231/2001, anticorruzione, antiriciclaggio, data privacy, antitrust, regolatorio, etc.;
- altre funzioni come le Operations, la Qualità, l'Information Technology, la Tutela Aziendale, a presidio dei rischi di continuità operativa, di qualità dei prodotti e dei processi produttivi, di sicurezza del patrimonio aziendale, dei dati e dei sistemi informativi.

E così via.

Al terzo livello di controllo, l'Internal Audit svolge un'attività di verifica indipendente, secondo logiche *risk-based*, volta a valutare l'adeguatezza, l'efficacia e l'effettiva operatività dei sistemi aziendali di gestione e controllo dei rischi aziendali.

Pur agendo sulle medesime dimensioni organizzative, geografiche, di processo e di linee di business, quasi mai le funzioni sopra menzionate condividono linguaggi, schemi e metodologie di *assessment*; raramente coordinano le attività di mappatura e verifica dei processi e dei controlli e le azioni di *remediation* che ne conseguono (ivi inclusi gli interventi sul corpo normativo aziendale); non sempre condividono gli esiti dei propri interventi e coordinano i flussi informativi verso il Management e gli Organi di Amministrazione e Controllo.

In questa situazione di sistemi "a silos", accade anche che alcune di queste funzioni adottino soluzioni informatiche "verticali" e "*stand-alone*", pensate e sviluppate solo per rispondere alle esigenze specifiche espresse dalla struttura che le implementa, spesso senza le *capabilities* idonee a sfruttare in modo intelligente l'immenso patrimonio di dati che i sistemi informativi aziendali mettono a disposizione delle organizzazioni. Tutto ciò senza alcuna possibilità di successiva scalabilità ad altri ambiti GRC o di futuro sviluppo di funzionalità innovative e basate su logiche di intelligenza artificiale, idonee a supportare la visione di sistemi di "nuova generazione".

Ne emerge un quadro complesso, fatto di sovrapposizioni, ridondanze, disallineamenti, incongruenze, lentezze, con impatti inevitabilmente negativi sull'efficacia ed efficienza dei vari livelli di controllo e sulla capacità di dare una visione olistica e integrata al Management e ai Vertici aziendali. Oltre a creare confusione generale nell'organizzazione, se non addirittura scarso gradimento da parte del business verso le tematiche GRC; e impegnare l'azienda con investimenti IT magari contenuti nel breve termine, ma che rischiano di essere poco utili e di generare ulteriore entropia se guardati in prospettiva.

LO SCENARIO DI "NUOVA" GENERAZIONE

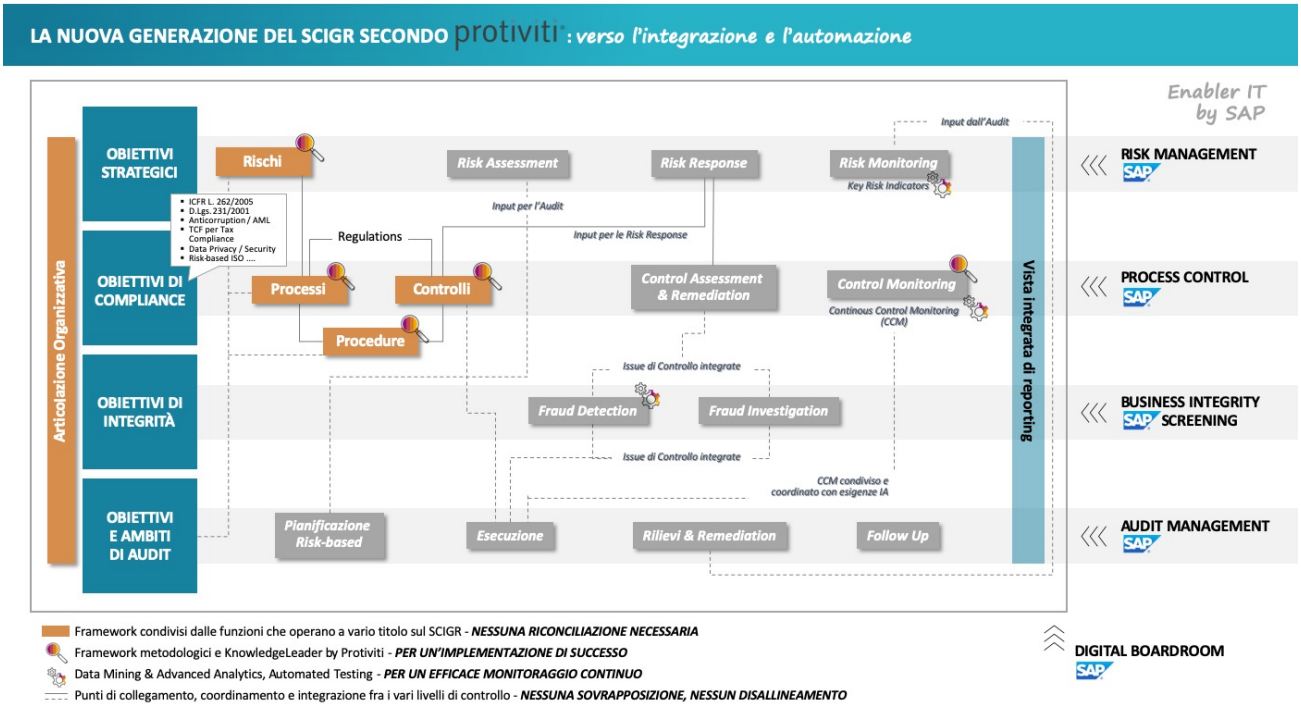
Cosa occorre fare per superare i "silos" sopra descritti?

Innanzitutto, occorre avere una **visione chiara dello scenario ottimale a tendere** - come quella proposta da Protiviti e rappresentata in figura - che metta in evidenza tanto i punti critici di possibile connessione fra i vari livelli di controllo, quanto le attività di controllo che possono essere automatizzate e ottimizzate attraverso funzionalità di *data mining* e *analytics* avanzate, potenzialmente in grado di sfruttare capacità di machine learning e intelligenza artificiale.

Quindi, è necessario **superare le barriere e le logiche dell'"orticello"**, sedersi ad un unico tavolo e iniziare a condividere e cooperare. E questa è una sfida non sempre facile da affrontare nelle organizzazioni particolarmente complesse e articolate nelle linee di difesa.

Infine (*last but not least*), occorre fare la **scelta giusta sulla tecnologia che dovrà supportare la visione integrata**: perché, senza "*enabler*" tecnologico, la meta

dell'integrazione (e certamente dell'automazione) diventa difficilmente raggiungibile. Anche qui, meglio superare le "parrocchie" e scegliere una piattaforma unica, in grado di rispondere alle esigenze delle varie funzioni che operano sul SCIGR. È pertanto necessario abbandonare le viste unicamente "verticali" e privilegiare piattaforme scalabili e nativamente integrabili, in grado di supportare un percorso di più ampio respiro.



LA SUITE GRC DI SAP A SUPPORTO DEI SCIGR DI NUOVA GENERAZIONE

Da anni i nostri esperti della *practice* Technology Consulting lavorano con i nostri consulenti di Risk, Compliance e Internal Audit sulle soluzioni SAP per soddisfare i bisogni espressi dai clienti in questi ambiti. L'esperienza di recente maturata conferma che la Suite GRC di SAP è coerente con la visione Protiviti sui SCIGR di nuova generazione e consente di realizzarla nei seguenti modi.

1. **A ciascuno la risposta pensata per soddisfare le specifiche esigenze.** La Suite GRC di SAP supporta le varie linee di difesa con soluzioni "*ad hoc*", pensate e sviluppate per rispondere alle esigenze specifiche di ciascuna funzione di controllo. In particolare:

   - **SAP Risk Management** permette, attraverso l'ingaggio delle funzioni di business, di gestire in modo strutturato le attività di identificazione e valutazione dei rischi di business (supportando altresì analisi di scenario e simulazioni Montecarlo), di definizione delle *risk response* e delle relative *ownership*, di monitoraggio di idonei indicatori alimentabili manualmente o attraverso acquisizione di dati dai sistemi sorgente, di *reporting* sempre aggiornato al Management e ai Vertici aziendali.

- **SAP Process Control** agevola la gestione coordinata e integrata dei processi di *compliance* a procedure, norme e leggi/regolamenti, guidando l'identificazione, la gestione e il monitoraggio periodico dei controlli rilevanti per le normative applicabili all'organizzazione, e permettendo contestualmente di mettere a fattor comune controlli rilevanti rispetto a più normative, allo scopo di evitare ridondanze o disallineamenti. La soluzione permette altresì la gestione dell'intero ciclo di vita delle *policy* e procedure aziendali, così da avere un unico punto di accesso alla documentazione normativa interna.

- **SAP Business Integrity Screening** è pensato per un duplice scopo: da un lato, supportare le funzioni competenti nello *screening* automatizzato delle terze parti, attraverso il confronto dei dati presenti nei sistemi informativi aziendali (SAP e non SAP) con liste acquisite da *provider* specializzati (e.g. liste OFAC, Thomson Reuters, Dow Jones, etc.) ovvero costruite "*ad hoc*" dall'azienda; dall'altro, consente di impostare, calibrare e eseguire in automatico strategie e metodi di *detection* allo scopo di intercettare (*real-time* o con una frequenza predeterminata) transazioni sospette, cui dar seguito attraverso verifiche, blocchi e/o avvio di attività di investigazione. Qualora impostati dall'Internal Audit, i risultati della *detection* possono essere integrati nella soluzione Audit Management.

- **SAP Audit Management** supporta le funzioni di Internal Audit nella gestione dell'intero ciclo di audit, dalla pianificazione al *follow up* e al *reporting*, dalla gestione delle risorse al monitoraggio delle *performance* della funzione. Agevola l'interlocuzione con il Management per lo scambio di informazioni su criticità e proposte di intervento correttivo e facilita il monitoraggio delle azioni correttive concordate. Permette all'Internal Audit di acquisire i *framework* organizzativi, di processo e di rischio impostati dalle seconde linee di difesa per le finalità di definizione dell'universo di audit, così come le informazioni sui rischi e sui controlli rilevati per le finalità di pianificazione ed esecuzione degli interventi di audit. Agevola lo scambio di informazioni su rilievi e carenze con le altre funzioni di controllo, al fine di ottimizzare gli interventi correttivi proposti al Management. Infine, può essere interfacciato con **SAP Business Integrity Screening** per consentire all'Internal Audit di svolgere attività di *fraud detection*.

2. **A tutte le funzioni coinvolte la possibilità di condividere *framework* e informazioni di interesse comune nonché di coordinare la pianificazione delle attività di verifica di pertinenza.** Pur potendo essere implementate separatamente, le soluzioni SAP sopra menzionate hanno il vantaggio di risiedere sulla medesima piattaforma tecnologica e possono pertanto condividere *framework*, dati e informazioni di interesse comune, allo scopo ultimo di evitare sovrapposizioni o disallineamenti. Così, ad esempio, le varie funzioni di controllo possono condurre le attività di pertinenza agendo su "oggetti" (quali l'organizzazione, i processi, i rischi e i controlli, le normative, le *policy* e procedure aziendali, ovvero qualsiasi altro *asset* rilevante ai fini del SCIGR) articolati e denominati allo stesso modo e, quindi, condivisi con lo stesso linguaggio da chiunque svolga attività di analisi dei rischi e dei controlli. Allo stesso modo, le funzioni di controllo possono anche condividere in modo trasparente i propri piani di lavoro allo scopo di ottimizzare lo svolgimento di attività di verifica sugli stessi "oggetti" (ancorché con finalità differenti).

Framework condivisi
Nessuna riconciliazione necessaria

Reporting e viste coerenti
Grazie ad elementi comuni e condivisi

Responsabilità chiare
Basate sulle "ownership"

Coordinamento facilitato
Sulle tre line di difesa

Convergenza
Fra processi, metodologie e informazioni

3. **A chi è chiamato ad eseguire verifiche o analisi massive la possibilità di fare leva sui dati per automatizzare attività di test e di *detection*.** Le soluzioni SAP mettono a disposizione funzionalità di *data mining*, *advanced analytics* e *machine learning*, che consentono di automatizzare il monitoraggio continuo dei controlli interni (in particolare attraverso **SAP Process Control**) nonché lo *screening* delle terze parti e la *detection* di frodi o altre anomalie critiche per l'azienda (in particolare attraverso **SAP Business Integrity Screening**). L'ambizione di poter da un lato **ampliare** il perimetro di analisi dell'adeguatezza del sistema di controllo interno, dall'altro di **intercettare tempestivamente** situazioni di anomalia sulle quali effettuare approfondimento e/o intervenire tempestivamente, diventa finalmente realizzabile.

4. **Alla C-Suite la possibilità di disporre di un quadro sinottico completo e aggiornato in tempo reale sui temi di rischio e controllo interno.** La combinazione della Suite GRC con **SAP Digital Boardroom** completa il quadro avveniristico, che in passato abbiamo solo immaginato: una *dashboard* integrata di indicatori di *performance* per la C-Suite, aggiornata "*real time*" e facilmente navigabile; un unico punto di accesso alle informazioni "chiave", per fornire una visione olistica, completa anche di indicatori di rischio e di controllo, così preziosi al Management e ai Vertici aziendali per prendere decisioni "*risk-informed*".

Un'unica vista dei rischi e dei controlli legati agli obiettivi dell'impresa

CONCLUSIONI

Innovare i processi e i sistemi in ambito SCIGR non è più un'opzione per le organizzazioni moderne e complesse. In base alla nostra esperienza, un approccio strutturato al percorso richiede:

- Un'attenta diagnosi della situazione di partenza, considerando tutti gli aspetti rilevanti, quali l'assetto organizzativo esistente, i soggetti a vario titolo coinvolti e gli ambiti coperti, i processi in essere, le metodologie applicate, i flussi di *reporting* a tutti i livelli.

- Una presa di coscienza dei punti di debolezza e delle aree di miglioramento, che permetta di definire un modello coordinato e integrato, condiviso da tutte le funzioni che operano sul SCIGR.

- Un *commitment* forte che dia visibilità e rilievo strategico all'iniziativa, che rafforzi la cultura dell'organizzazione sui temi di rischi e di controllo interno e che assicuri l'ingaggio di tutti gli attori rilevanti per il successo della stessa.

- La scelta di una soluzione tecnologica robusta, scalabile, facilmente integrabile sia orizzontalmente (ovvero fra i vari prodotti a supporto delle funzioni di controllo), sia verticalmente (ovvero con i sistemi IT sorgente su cui risiedono i dati e le informazioni rilevanti ai fini del SCIGR), oltre che in continua evoluzione per stare al passo con le innovazioni - ancora in corso - in materia di intelligenza artificiale.

I nostri esperti delle *practice* Risk, Compliance, Internal Audit e Technology Consulting saranno lieti di assistere la vostra organizzazione nella costruzione del percorso e della soluzione più idonea rispetto al vostro contesto culturale, ai vincoli da considerare e ai benefici attesi nel breve, medio e lungo termine.

Non esitate a contattarci, il momento di agire è ORA.

CONTATTI

— **Emma Marcandalli** / Managing Director / **emma.marcandalli@protiviti.it**

— **Enrico Ferretti** / Managing Director / **enrico.ferretti@protiviti.it**

SAP® PartnerEdge®