



Per una nuova governance dei rischi

Risk & Compliance

Competenze, Metodologie
e Approcci

kpmg.com/it





Indice

Chi siamo

Risk & Compliance: affidabilità e innovazione

4

Scenario

Le nuove sfide della risk governance

6

La visione delle aziende

7

Competenze

8

Servizi

10

La nostra differenza

15



Risk & Compliance: affidabilità e innovazione

KPMG nel Mondo

KPMG, uno dei principali Network di servizi professionali alle imprese, leader nella revisione e organizzazione contabile, nella consulenza manageriale e nei servizi fiscali, legali e

amministrativi, è attivo in 152 Paesi del mondo con oltre 207 mila professionisti. KPMG punta a trasformare la conoscenza in valore per i clienti, per la propria comunità e per i mercati.

Le società aderenti a KPMG forniscono alle aziende clienti una vasta gamma di servizi multidisciplinari, secondo standard d'eccellenza omogenei su scala globale.

KPMG in Italia

Da oltre 50 anni KPMG accompagna i processi di crescita delle imprese. Oggi, con circa 4.250 professionisti, 26 sedi sull'intero territorio nazionale, oltre 5.000 clienti ed un portafoglio completo di servizi che risponde alle

necessità del mercato nazionale e internazionale, il Network KPMG è la più importante 'piattaforma' di servizi professionali attiva nel nostro Paese. Grazie ad un modello operativo di tipo federale, il Network

italiano può contare sulla capacità di mobilitare in tempo reale il pensiero e le competenze disponibili su scala globale, potendo però operare in piena autonomia strategica e gestionale sul mercato nazionale.

Risk & Compliance

La Practice dedicata ai servizi di Governance, Risk Management e Compliance, attiva dal 1998, rientra tra i 'core services' del Network KPMG. Grazie ad una crescita costante a livello globale realizzata attraverso il supporto strategico

e operativo alle aziende di tutti i settori produttivi e all'anticipazione delle tendenze in atto in tema di gestione e controllo dei rischi, la Practice può mobilitare competenze ed esperienze di circa 9.700 professionisti in 75

Paesi. In Italia sono attivi circa 350 professionisti dedicati a tempo pieno e in possesso delle competenze specialistiche e di industry necessarie per l'esecuzione delle progettualità più complesse.



KPMG nel Mondo



152 Paesi



207 mila professionisti

KPMG in Italia



26 uffici



4.250 professionisti

La Practice Risk & Compliance



75 Paesi



9.700 professionisti nel mondo



350 professionisti in Italia

Le nuove sfide della risk governance

“I rischi si generano dalla non conoscenza di quello che stiamo facendo”.

Warren Buffet

La gestione dei rischi d'impresa è considerata, ormai da tempo, centrale nei sistemi di corporate governance. In tale contesto, al Board è richiesto di svolgere un ruolo di *risk oversight* che consiste, come recentemente definito dai *principles of corporate governance* emessi dal G20/OECD, nella supervisione dei ruoli e delle responsabilità del processo di risk management, nella definizione della tipologia e del livello di rischio che la società è disposta ad assumere per raggiungere i propri obiettivi (propensione al rischio), nonché nelle modalità con cui i rischi devono essere gestiti.

Il Board e il management team sono chiamati a mettere in atto robusti processi di risk management che devono necessariamente partire dalla definizione delle strategie.

Le imprese si confrontano con scenari fortemente caratterizzati da complessità, velocità di cambiamento e da un livello di innovazione mai verificatosi in precedenza. I processi di digitalizzazione, ma anche l'avanzare di nuove modalità di business (es. sharing economy), richiedono immediate risposte in termini di trasformazione dei business model e delle filiere produttive.

Le organizzazioni che non hanno un adeguato livello di attenzione a questi segnali di cambiamento, si espongono a rischi rilevanti con conseguenze sul posizionamento e, in taluni casi, sulla stessa capacità di sopravvivenza. Per questo KPMG ha sviluppato, a livello globale, un approccio innovativo finalizzato all'analisi dei segnali di cambiamento, alla valutazione degli impatti sul business model e all'identificazione delle iniziative idonee ad abilitarne le opportunità. Pertanto nella visione di KPMG la risk governance, oltre a preservare l'approccio 'difensivo' sui rischi a tutela del valore delle imprese, è anche un fattore abilitante del cambiamento e delle opportunità di business che esso propone.

La visione delle aziende

Le agende dei Consigli di Amministrazione sono in continua evoluzione per riflettere il mutarsi delle aspettative degli stakeholders.

Le implicazioni della tecnologia/innovazione digitale, la cultura aziendale, le tematiche di HSE e *Corporate Social Responsibilities* sono alcune delle principali tematiche che emergono dallo

studio KPMG *On the 2019 Board Agenda*.

Lo studio è stato condotto intervistando Consiglieri di amministrazione ed imprenditori per cogliere le principali tematiche che sono oggetto di discussione nei consigli.

Ne emergono sette ambiti da tenere sotto osservazione.



La composizione del Consiglio e le competenze presenti devono essere adeguate per il perseguimento degli obiettivi strategici attuali e futuri.



I processi di gestione del rischio e di pianificazione strategica devono essere rivisti tenendo in considerazione la Trasformazione Digitale in corso.



Le Società si devono focalizzare sulla creazione di valore nel lungo periodo e comprendere le aspettative di tutti gli stakeholders chiave.



I piani di successione dei CEO e lo sviluppo dei *talent* devono divenire una priorità.



La cultura aziendale è un asset strategico che va valutata, monitorata e rafforzata.



Cybersecurity e *data privacy* continuano ad essere un argomento rilevante.



Le Società devono essere pronte a prevenire e gestire le crisi.

“Traditional ERM process may not be designed to address the disruptive risks posed by the digital transformation and to assess the continuing validity of key assumptions on which the company’s strategy and business model are based”.

KPMG’s *On the 2019 Board Agenda*



Competenze

Board Advisory and Governance Services

Le recenti evoluzioni della corporate governance, anche a seguito delle analisi effettuate sulle cause della crisi finanziaria di questi ultimi anni, hanno confermato che al Board spetta un ruolo da protagonista nei processi di gestione dei rischi. Il suo tradizionale ruolo di indirizzo strategico non si esaurisce nell'approvazione dei piani strategici e nella definizione degli assetti organizzativi più

ideali al loro conseguimento. Il Board è chiamato ad assicurare un adeguato livello di rischio, coerente con la remunerazione attesa del capitale investito e compatibile con la sostenibilità nel medio-lungo periodo. Inoltre deve garantire la presenza di elementi abilitanti per il conseguimento degli obiettivi, inclusi i presidi di controllo funzionali al mantenimento

dei livelli di rischio desiderati (risk appetite). In tale contesto KPMG ha sviluppato significative esperienze nell'assessment e nella progettazione di sistemi di risk governance e di controllo interno, supportando il Board nella definizione delle linee di indirizzo sul sistema di controllo interno e di gestione dei rischi e nella valutazione complessiva della sua adeguatezza.

Enterprise Risk Management and Risk Based Strategy

Oltre a innovare l'approccio sull'Enterprise Risk Management finalizzato a fornire gli strumenti più adeguati agli organi societari e al management per gestire e controllare l'impresa attraverso il coordinamento tra i soggetti coinvolti e l'integrazione nei processi, KPMG ha ritenuto di sviluppare un nuovo concept: la Risk Based Strategy (RBS). Questo framework mira a cogliere, in anticipo, i segnali di

cambiamento della cosiddetta 'quarta rivoluzione industriale' attualmente in atto che, attraverso un utilizzo pervasivo della tecnologia applicato ai business model tradizionali, produce il risultato di disintermediare intere filiere produttive (per questo si parla di *disruptive changes*). Digitalizzazione, sharing economy, stampanti 3D, big data, *peer-to-peer*, sono solo alcuni aspetti del mutamento in corso. Secondo una

recente survey, il cambiamento in atto farà perdere la posizione di *incumbent* al 40% degli operatori nei prossimi 5 anni; nonostante questo, il 45% dei rispondenti ritiene che non sia un tema da portare all'attenzione del Board. RBS consente di analizzare i segnali di cambiamento, valutarne gli impatti sul business in termini di rischio e opportunità, identificare le iniziative da intraprendere e gestire i rischi connessi alla trasformazione.

Internal Audit

KPMG ha sviluppato un nuovo Target Operating Model (TOR) per supportare i processi di trasformazione delle funzioni di Internal Audit e metterle in condizione di cogliere le nuove sfide della risk governance. Il TOR si fonda su tre elementi distintivi:

- Focalizzazione sulle conoscenze di industry come fattore abilitante del cambiamento di passo da un approccio 'Thinking Critically' a un approccio 'Critical Thinking', finalizzato a cogliere gli aspetti critici

del business in termini di rischi ma anche di opportunità;

- Utilizzo della tecnologia sia nei processi di Internal Audit (work-flow) sia nell'analisi dei dati (Data & Analytics) finalizzato a incrementare efficacia, efficienza e qualità della delivery (es. Time to Market);
- Strategie di sourcing focalizzate sulle risorse critiche con competenze di industry (es. *subject matter expert*) e utilizzo di *share service/ co-sourcing* per le altre competenze.

Compliance

La compliance rappresenta oggi una componente fondamentale della risk governance. Anche se l'approccio di risk management in tale ambito prevede strategie finalizzate alla riduzione pressoché totale del rischio, i sistemi di controllo richiamati dalle normative nazionali e internazionali vanno considerati nel più ampio sistema di controllo interno e di gestione dei rischi societari e,

pertanto, necessitano anch'essi di coordinamento con gli altri presidi di controllo interno. Se a questo elemento di complessità interna aggiungiamo anche quello di uno scenario normativo e regolamentare globalizzato e sistemi sanzionatori sempre più pervasivi, appare evidente che, anche in questo ambito, l'approccio tradizionale per 'silo' debba essere riconsiderato in ottica ERM.

Corporate Sustainability

La corporate sustainability è una componente sempre più importante della corporate governance: le imprese sono consapevoli che per essere competitive devono creare valore condiviso (Creating Shared Value - CSV) sia per l'organizzazione sia per le comunità in cui operano, attraverso il collegamento tra bisogni sociali (social need) e il modello di business/strategia aziendale.

KPMG supporta le organizzazioni nella creazione di valore condiviso, attraverso la definizione di politiche e pratiche operative che rafforzano la competitività dell'azienda migliorando al contempo le condizioni economiche e sociali della comunità in cui opera. In particolare, KPMG ha sviluppato modelli di quantificazione del ritorno economico delle politiche di corporate sustainability per l'azienda e la comunità, con l'obiettivo di identificare il vero valore (true value) delle scelte aziendali.

"Le nostre competenze specialistiche parlano il linguaggio dei settori produttivi: dai Financial Services, al Consumer & Industrial Market, alla Pubblica Amministrazione".

Servizi

KPMG ha sviluppato una gamma veramente unica di servizi e di competenze che permettono di rispondere alle esigenze di governo sostenibile da parte di piccole, medie e grandi imprese di ogni settore economico per assisterle nel loro obiettivo di coniugare, secondo un approccio integrato, crescita, gestione dei rischi, governance e compliance.



Board Advisory and Governance Services

Sistema di Controllo Interno e di Gestione dei Rischi (SCIGR)

- Assessment del SCIGR secondo i requisiti del Codice di Autodisciplina e delle leading practice internazionali in termini di ruoli e responsabilità, coordinamento dei soggetti coinvolti e integrazione nei processi aziendali, conformità alla normativa, monitoraggio e reporting;
- Supporto al Board nella definizione delle Linee di indirizzo sul SCIGR: progettazione e implementazione delle sue componenti e delle modalità di coordinamento dei soggetti coinvolti;
- Supporto alla funzione di Internal Audit e agli organi sociali nella predisposizione del modello di relazione periodica contenente la valutazione di adeguatezza del SCIGR in linea con il Framework CoSO, il modello delle tre linee di difesa e le altre leading practice di riferimento (es. combined assurance model).

Sistema Normativo Integrato

- Progettazione e realizzazione di sistemi normativi finalizzati a semplificare e razionalizzare il corpo procedurale attraverso un modello di governance di gruppo, basato sui processi e integrato con il SCIGR.

Corporate Governance Assessment

- Assistenza nella definizione del quadro generale dei principi e dei criteri di Corporate Governance applicabili (es. Codice di Autodisciplina) e gap analysis sul disegno e sull'effettivo funzionamento delle soluzioni adottate.

Due Diligence e Post Deal Integration del Sistema di Controllo Interno e di Gestione dei Rischi (SCIGR)

- Assistenza durante l'esecuzione di operazioni straordinarie nella valutazione di adeguatezza del SCIGR rispetto alle leading practice di riferimento;
- Assistenza per l'integrazione dei processi di Internal Audit, risk management e compliance in caso di operazioni straordinarie.



Enterprise Risk Management and Risk Based Strategy

Enterprise Risk Management (ERM)

- Attività di Risk Assessment finalizzate alla definizione del Corporate Risk Profile costituito dai principali rischi aziendali identificati e valutati rispetto agli obiettivi strategici e oggetto di reporting al vertice e agli organi societari;
- Implementazione del Framework ERM e supporto al Chief Risk Officer nella definizione di modelli di risk governance, risk assessment e quantification, risk appetite e tolerance, risk monitoring e reporting.

Dynamic Risk Assessment (DRA)

- In un contesto ormai caratterizzato da Volatility, Uncertainty, Complexity e Ambiguity i Modelli di ERM tradizionali non supportano le organizzazioni moderne ad identificare oltre che i rischi: i) le opportunità, ii) gli effetti dinamici innescati sul CRP da rischi esterni ed interni;
- Il DRA supporta le organizzazioni ad evidenziare gli effetti di eventi sistemici sulla società in ottica sia di rischio che di opportunità, nonché a valutare i propri rischi secondo differenti driver dinamici (oltre probabilità per impatto) anche l'interconnessione dei rischi, il loro effetto contagio e velocità di manifestazione.



Internal Audit

Internal Audit Sourcing

- Supporto alla funzione di Internal Audit nelle attività di pianificazione ed esecuzione degli interventi attraverso un nuovo approccio basato sull'utilizzo di tecnologia e competenze specialistiche di industry che consentono, attraverso l'analisi congiunta delle strategie e dei rischi, una maggiore focalizzazione sul sistema di controllo interno relativo alle iniziative e ai processi strategici.

Data Analytics Enabled Internal Audit

- Progettazione e implementazione di soluzioni IT per l'analisi massiva di dati e transazioni relativi a controlli chiave identificati in relazione ai principali rischi strategici e operativi e attivazione di strumenti di monitoraggio real-time.

Quality Assurance Review

- Valutazione indipendente della funzione di Internal Audit rispetto agli standard professionali dell'Institute of Internal Auditors e alle leading practice di riferimento attraverso un approccio metodologico finalizzato ad accrescere il valore generato dalle attività di Internal Audit.



Compliance

Integrity Risk Management/Compliance 231

- Supporto nella progettazione ed implementazione di Modelli Organizzativi ai sensi del D.lgs.231/01 attraverso l'analisi preliminare delle aree di rischio e dei relativi presidi di controllo, l'identificazione di aree di miglioramento, la realizzazione delle iniziative di rafforzamento del sistema di controllo interno;
- Supporto all'Organismo di Vigilanza ai sensi del D.lgs. 231/01 nella predisposizione del piano di vigilanza e nell'esecuzione delle verifiche di adeguatezza del sistema di controllo interno riferito al Modello 231.

Sistema di controllo interno sull'informativa finanziaria (SCIIF)

- Assistenza nell'adeguamento ai requisiti normativi, nazionali ed internazionali (L. 262/05, Sarbanes Oxley Act) riguardanti l'introduzione ed il mantenimento di adeguati sistemi di controllo interno sull'informativa finanziaria;
- Supporto nell'esecuzione di verifiche sull'adeguatezza del SCIIF in termini di disegno ed effettivo funzionamento dei controlli identificati;
- Assistenza al Dirigente Preposto attraverso l'analisi risk based del portafoglio dei controlli 262 identificati con l'obiettivo di razionalizzare e ridurre il numero e il costo dei *key control*.

Compliance Management

- Attività di assessment del rischio di non conformità e dei relativi presidi di controllo;
- Implementazione del Compliance Management Framework in termini di cultura aziendale, governance e organizzazione, risk assessment, programmi di compliance, comunicazione e formazione, monitoraggio e reporting.

Regulatory Compliance

- Assistenza nella definizione di modelli di controllo interno riferiti a leggi e regolamenti (antitrust, privacy, operazioni con parti correlate) anche attraverso l'utilizzo di tool di monitoraggio dell'evoluzione della normativa e di misurazione del profilo di rischio di compliance/regolatorio.

Tax Control Framework

- Progettazione e implementazione di modelli di controllo dei rischi relativi al processo fiscale anche con riferimento alla compliance cooperativa tra autorità fiscale e impresa (cd regime di adempimento collaborativo).



Corporate Sustainability

Strategia

Strategia e Corporate Shared Value (CSV)

- Definizione di un piano di creazione di valore condiviso (collegato agli obiettivi aziendali e ai *social need*) e sviluppo di politiche in ambito di Corporate Sustainability.

Benchmarking e Gap Analysis

- Analisi del posizionamento del 'profilo di sostenibilità' rispetto ai competitor e alle best practice e individuazione dei punti di forza e di miglioramento su specifiche tematiche rilevanti per il business.

Stakeholder Engagement e predisposizione della Matrice di materialità

- Identificazione dei temi rilevanti attraverso un'analisi interna ed esterna, mappatura degli stakeholder al fine di definirne la 'rilevanza strategica' e supporto nelle attività di Stakeholder Engagement.

Investimenti socialmente responsabili

- Supporto nel dialogo con gli investitori e *assessment* del livello di rispondenza dell'organizzazione alle richieste informative dalle agenzie/indici SRI (DJSI, FTSE4Good, CDP) e definizione di un relativo *action plan* per migliorare lo *scoring*.

Socio-economic Impact Assessment

- Valutazione degli impatti economici, sociali e ambientali delle attività di business (es. analisi del contributo al reddito e all'occupazione nazionale, analisi costi-benefici, SROI analysis).

Governance, ESG Risk & Reporting

Governance e disegno organizzativo

- Supporto nella definizione di strutture e principi di governance in grado di garantire il presidio e la gestione dei temi connessi alla sostenibilità. *Start-up* della funzione di Corporate Sustainability.

Integrity Management

- Supporto nella definizione del Codice Etico, del sistema di *whistleblowing*, delle attività di governance e formazione in grado di garantire il presidio del rispetto dei requisiti del Codice Etico.

Gestione della reputazione

- Reputational Risk Assessment attraverso un'analisi delle prospettive interne ed esterne e definizione di modelli di gestione e piani per il monitoraggio dei rischi reputazionali individuati.

Responsible Supply Chain Management

- Analisi della catena di fornitura secondo un approccio *Risk-based*, attraverso l'identificazione dei principali rischi socio-ambientali legati alla catena di fornitura, definizione dei criteri di *screening* e supporto nell'identificazione dei *tool* di monitoraggio.

Supporto nella predisposizione del Bilancio di Sostenibilità e del Bilancio Integrato

- Supporto nella predisposizione del Bilancio di Sostenibilità, del Bilancio Integrato e nella definizione di KPI di sostenibilità per il monitoraggio di strategie, politiche e attività di sostenibilità.



Climate Change e TCFD

- Definizione delle politiche di gestione dei cambiamenti climatici (valutazione dei rischi, definizione degli obiettivi e misurazione degli impatti), supporto nella predisposizione dell’informativa richiesta dalla TCFD.

HSE and ESG due diligence

- Valutazione degli aspetti ambientali e legati alla salute e sicurezza durante i processi di investimento, valutazione degli *asset* e dei potenziali *target*.

Human Rights Framework

- Sviluppo di un *framework* organizzativo per la gestione dei Diritti Umani in azienda (Policy, Due Diligence, Assessment, Reporting).

Sistemi di gestione

- Sviluppo di sistemi di gestione conformi ai requisiti ISO 14001 ed EMAS (ambiente), ISO 50001 (efficienza energetica), ISO 14064 (gas serra), ISO 14040 (LCA), ISO 9001 (qualità), OHSAS 18001 e ISO 45001 (salute e sicurezza).

HSE Audit

- Supporto nelle attività di auditing relativamente alle tematiche HSE sia per valutare la conformità normativa sia il rispetto degli standard adottati.

Supporto alla funzione Internal Audit

- Supporto alla funzione Internal Audit nell’analisi del processo di reporting non finanziario (NFI) e delle tematiche socio-ambientali. .

Informativa non finanziaria (D.Lgs. 254/2016)

- Supporto nell’adeguamento ai requisiti normativi previsti dal D.Lgs. 254/2016 e nella predisposizione della Dichiarazione Non Finanziaria.

Assurance

- Assurance della reportistica di sostenibilità;
- Revisione delle informazioni non finanziarie secondo i principi ISAE 3000 (Revised).

La nostra differenza

Indipendenza e Integrità

Massima etica professionale e ricerca continua dell'eccellenza

Multidisciplinarietà

Il confronto continuo, lo scambio di idee ed esperienze su temi professionali eterogenei potenzia la capacità di comprendere e gestire la complessità del business

Globali e Locali

Mettiamo a disposizione dei clienti l'intero portafoglio di competenze, sia a livello nazionale che internazionale

Working Together

**Il Team riveste un ruolo centrale nella nostra cultura.
Favorisce lo scambio di conoscenze e la qualità del servizio**

Competenze di Industry

Operiamo in tutti i principali settori, con una comprensione di insieme dei mercati e delle loro dinamiche evolutive

Infrastrutture tecnologiche

Piattaforme proprietarie evolute in grado di soddisfare esigenze complesse e offrire massima trasparenza a tutti gli stakeholder



Contatti

Antonio Mansi

Partner Advisory
Head of Risk & Compliance
T: +39 06 809711
E: amansi@kpmg.it

Corrado Avesani

Partner Advisory
T: +39 045 8157611
E: cavesani@kpmg.it

Piermario Barzagli

Partner Advisory
T: +39 02 676431
E: pbarzagli@kpmg.it

Giuseppe D'Antona

Partner Advisory
T: +39 02 676431
E: gdantona@kpmg.it

Paolo Mantovano

Partner Advisory
T: +39 02 676431
E: pmantovano@kpmg.it

Marco Stellin

Partner Advisory
T: +39 06 809711
E: mstellin@kpmg.it

Nicolò Zanghi

Partner Advisory
T: +39 02 676431
E: nzanghi@kpmg.it

kpmg.com/it



kpmg.com/app



© 2019 KPMG Advisory S.p.A. è una società per azioni di diritto italiano e fa parte del network KPMG di entità indipendenti affiliate a KPMG International Cooperative ("KPMG International"), entità di diritto svizzero. Tutti i diritti riservati.

Denominazione e logo KPMG sono marchi e segni distintivi di KPMG International.

Tutte le informazioni qui fornite sono di carattere generale e non intendono prendere in considerazione fatti riguardanti persone o entità particolari. Nonostante tutti i nostri sforzi, non siamo in grado di garantire che le informazioni qui fornite siano precise ed accurate al momento in cui vengono ricevute o che continueranno ad esserlo anche in futuro. Il volume non rappresenta un'offerta di vendita né una sollecitazione all'acquisto di alcun servizio.

Stampato in Italia.

Data di pubblicazione: Giugno 2019

Grafica: PG&W S.r.l. – www.pg-w.it