MANAGEMENT CONSULTING
Marcello Colaianni

Consulente - Formatore - Auditor

Mobile + 39 393.3265594 | **Sito** www.marcellocolaianni.it
Mail marcello@marcellocolaianni.it
Blog marcellocolaianniblog.wordpress.com

GOVERNANCE - RISK - COMPLIANCE

DI COSA SI TRATTA

GRC è l'acronimo di Governance, Risk e Compliance: tre dimensioni che, affrontate in modo integrato, costituiscono il framework di riferimento per una gestione aziendale solida, trasparente e orientata al lungo periodo. Non si tratta di tre discipline separate, ma di un sistema unitario in cui ciascuna componente rafforza e sostiene le altre.

1) La **GOVERNANCE** definisce chi prende le decisioni e come vengono prese: è la struttura di regole, processi e organi aziendali — dalla Proprietà al vertice esecutivo — che orienta l'impresa verso i propri obiettivi strategici, garantendo trasparenza, integrità e responsabilità a tutti i livelli.
2) Il **RISK MANAGEMENT**, nell'ambito GRC, fa riferimento specificamente al rischio di compliance (o **rischio normativo**) che si articola nei seguenti 3 componenti:
   - ➥ **Rischio sanzionatorio**: multe, sanzioni amministrative e/o penali
   - ➥ **Rischio finanziario indiretto**: perdita di contratti, esclusione da gare, mancato accesso al credito
   - ➥ **Rischio reputazionale**: danno d'immagine verso clienti, mercato, autorità di vigilanza a seguito della mancata osservanza di leggi, regolamenti, codici di condotta o standard applicabili all'organizzazione.
3) La **COMPLIANCE** è la conformità alle leggi, ai regolamenti e alle linee guida applicabili all'organizzazione. Può essere certificata secondo la norma UNI ISO 37301, che fornisce evidenza oggettiva dell'adeguatezza dei presidi adottati rispetto all'intero perimetro normativo, cogente e volontario, dell'organizzazione.

PERCHÉ ADEGUARSI

Tre sono le ragioni fondamentali per adottare un approccio GRC strutturato e integrato:

RISCHIO - il panorama normativo in cui operano le organizzazioni è in costante evoluzione e crescente complessità. L'assenza di una governance efficace, di una gestione strutturata dei rischi e di presidi di conformità adeguati espone l'organizzazione, e i suoi responsabili, a sanzioni amministrative e penali, perdite finanziarie, danni reputazionali e responsabilità personale.

VALORI - un'organizzazione che adotta il GRC come approccio culturale prima ancora che normativo comunica al mercato, agli stakeholder e ai propri collaboratori un impegno concreto verso trasparenza, integrità ed etica d'impresa.

BISOGNO - ogni organizzazione, indipendentemente dalle dimensioni e dal settore, ha bisogno di assetti proporzionati, coerenti e documentati per raggiungere i propri obiettivi strategici e costruire un vantaggio competitivo sostenibile. Il GRC non è un costo di conformità: è un investimento sulla solidità e sulla continuità dell'impresa.

SERVIZI EROGATI

Questa scheda riassume l'intero portfolio di servizi per priorità e funzione:

- **4 Percorsi integrati:**
  1. **Privacy & AI Governance** (GDPR, D. Lgs. 196/03, AI Act, L. 132/2025; d. Lgs. 160/2026, ISO/IEC 27001, 27701, 42001, certificazione ISDP 10003);
  2. **Compliance 231 & Gestione del Rischio** [D. Lgs. 231/01: MOGC, OdV; ISO 37301, ISO 22301 (continuità operativa)];
  3. **Anticorruzione & Integrità** (normativa vigente, nuova Direttiva UE anticorruzione, ISO 37001);
  4. **Qualificazione e Affidabilità negli Appalti Pubblici** (Self-cleaning e White List Antimafia).

  Ciascuno unisce normativa cogente e Sistema di gestione ISO corrispondente, con propri Servizi erogati e Approfondimenti (estensioni, ampiezza ISO, Rating di legalità).
- **Aree specialistiche:**
  - **Qualità & Co.** – sistemi di gestione ISO 9001, 14001, 45001, 50001 e altri, anche integrati fra loro e in raccordo con il Modello 231
  - **Responsabilità sociale** – la S e la G dell'ESG: UNI/PdR 125 (parità di genere), SA 8000, PAS 24000, rendicontazione sociale e di governance
  - **Antiriciclaggio (AML/CFT)** – per i soggetti obbligati (intermediari, professionisti, operatori non finanziari) e, nelle imprese, innesto nel sistema di gestione Compliance (ISO 37301) quando il profilo di rischio lo richiede
  - **Governance e Organizzazione** – assetti del CdA, riforma Legge Capitali (D. Lgs. 47/2026), gestione dei rischi e controllo interno, organigramma, gruppi di lavoro
- **Servizi trasversali:**
  - **Audit** nella conduzione di verifiche di prima, seconda e terza parte, in tutti gli ambiti di sistema
  - **Formazione**: percorsi per ruolo e livello gerarchico, su ogni ambito normativo e di sistema
  - **Presidio di Governance e Organizzazione:** ruoli, deleghe, leadership commitment, al servizio della compliance
- **Assunzione di ruoli operativi**
  - **Consulente Privacy, Privacy Manager/Officer, DPO/RPD** (Data Protection Officer/Responsabile per la Protezione dei Dati)
  - **Componente / Presidente OdV o OdG** (per gli enti sportivi - MOCAS)
  - **AML Compliance Manager – Esperto Responsabile Antiriciclaggio / AML Internal Auditor**
  - **Consulente per il Sistema di Gestione**
  - **Auditor / Lead Auditor** - per verifiche ispettive interne ed esterne con riferimento al Sistema di gestione.

- **Risultati aggiuntivi (non servizi a sé)**

  Rating di legalità AGCM →non è un servizio da erogare separatamente, ma un beneficio che deriva automaticamente dal lavoro già previsto nei Percorsi Compliance 231 (Modello 231, lett. c del Regolamento), Anticorruzione (modelli di prevenzione della corruzione, lett. g) e nella scheda Qualificazione e Affidabilità negli Appalti (iscrizione White List, lett. e).

  Tra i benefici concreti: riduzione del 20% della garanzia provvisoria in gara, accesso agevolato al credito bancario.

SINERGIE PROFESSIONALI

La materia GRC ha un'estensione tale da abbracciare, per sua natura, ambiti professionali diversi e complementari. È del tutto naturale e fisiologico che, nell'erogazione di servizi GRC, convergano più figure professionali, ciascuna con le proprie competenze specifiche, titoli abilitativi e metodologie: non in concorrenza, ma in sinergia.

Il perimetro GRC - normativo, regolatorio e organizzativo - non si sovrappone a quello del Dottore **Commercialista** e del consulente fiscale, ma ne è naturalmente complementare. Il commercialista presidia i numeri, i bilanci, la fiscalità e le operazioni straordinarie; il consulente GRC presidia i processi, i sistemi di controllo, la conformità normativa e lo sviluppo organizzativo.

- **Governance societaria:** il commercialista supporta CdA e assemblee sul piano fiscale e contabile; il consulente GRC struttura i modelli organizzativi e i presidi di compliance
- **KPI e controllo di gestione:** la consulenza tradizionale misura quanto l'impresa guadagna; il consulente GRC misura quanto l'impresa è conforme e ben governata
- **Due diligence:** il commercialista conduce la due diligence contabile e fiscale; il consulente GRC integra la prospettiva normativa e regolatoria

In sintesi: dove il commercialista vede i numeri, il consulente GRC vede i processi e le regole che li governano. Insieme, offrono al cliente una visione completa e integrata della propria organizzazione.

Analogo rapporto di complementarità lega il consulente GRC all'**Avvocato**. L'avvocato presidia l'interpretazione della norma, i pareri legali, la contrattualistica e la difesa dell'impresa, in giudizio e davanti alle Autorità; il consulente GRC traduce la norma in organizzazione: processi, procedure, controlli, formazione e verifiche periodiche.

- **Modello 231:** l'avvocato valuta i profili di responsabilità dell'ente e difende l'impresa nel procedimento; il consulente GRC costruisce e aggiorna il Modello, ne verifica l'attuazione e supporta l'Organismo di Vigilanza
- **Privacy e AI:** l'avvocato cura pareri, contratti e contenzioso davanti al Garante e al giudice; il consulente GRC imposta ruoli, registri, valutazioni d'impatto, procedure e audit
- **Ispezioni e sanzioni:** l'avvocato assiste l'impresa nel contraddittorio e nell'impugnazione; il consulente GRC lavora prima, perché l'ispezione trovi un sistema documentato e funzionante

In sintesi: l'avvocato dice che cosa la norma richiede e difende l'impresa quando qualcosa è andato storto; il consulente GRC fa in modo che l'organizzazione la rispetti ogni giorno, e possa dimostrarlo.

Complementare è anche il rapporto con il **Consulente del Lavoro**. Il consulente del lavoro presidia il rapporto di lavoro: assunzioni, contratti, applicazione del CCNL, paghe e contributi, adempimenti verso INPS e INAIL,

assistenza nelle ispezioni e nelle vertenze di lavoro; il consulente GRC inserisce questi ambiti nel sistema di regole, controlli e responsabilità dell'organizzazione.

- **Rapporti di lavoro e Modello 231:** il consulente del lavoro garantisce la corretta gestione e la regolarità dei rapporti di lavoro; il consulente GRC mappa i rischi di reato collegati al lavoro (intermediazione illecita e sfruttamento del lavoro, impiego di lavoratori irregolari, salute e sicurezza) e definisce i controlli del Modello
- **Privacy dei lavoratori e controlli a distanza:** il consulente del lavoro tratta i dati del personale per conto dell'impresa e cura accordi sindacali e autorizzazioni per videosorveglianza e strumenti di controllo; il consulente GRC imposta ruoli, informative, valutazioni d'impatto e regole sull'uso dell'AI nella gestione del personale
- **Parità di genere:** il consulente del lavoro elabora i dati retributivi e gestisce l'esonero contributivo; il consulente GRC costruisce e mantiene il sistema di gestione UNI/PdR 125 e accompagna l'impresa alla certificazione

In sintesi: il consulente del lavoro amministra i rapporti di lavoro; il consulente GRC fa in modo che le regole che li governano diventino un sistema di controlli verificabile, a tutela dell'impresa e delle persone che vi lavorano.