La gestione integrata dei rischi: aspetti metodologici, organizzativi e modelli di presidio

Antonio Mansi
Aldo Cinquegrana

Roma, 2 luglio 2018

Agenda

- Principali riferimenti
- Gli attori del Sistema di controllo interno e gestione dei rischi
- Focus: Linee di indirizzo SCIGR
- Focus: Risk Appetite e Risk Tolerance
- Focus: Il livello di controllo - modelli di presidio e processo integrato
- Focus: Compliance Trasformation e presidio dei rischi

Principali riferimenti

Il Codice di autodisciplina

Il **Codice di Autodisciplina** enfatizza **la centralità del rischio e dell'integrazione del sistema di controllo interno e gestione dei rischi.**

Principi ispiratori

Centralità del rischio	Sistema dei controlli unico e "integrato"

Ruoli attribuiti al CdA

- **definisce la natura e il livello di rischio compatibile con gli obiettivi strategici dell'emittente,** includendo nelle proprie valutazioni tutti i rischi che possono assumere rilievo nell'ottica della sostenibilità nel medio-lungo periodo dell'attività dell'emittente;
- **valuta l'adeguatezza dell'assetto organizzativo, amministrativo e contabile** dell'emittente nonché quello delle controllate aventi rilevanza strategica, **con particolare riferimento al sistema di controllo interno e di gestione dei rischi**;

[cfr. 1.C.1]

Previo parere del comitato controllo e rischi:

- **definisce le linee di indirizzo del sistema di controllo interno e di gestione dei rischi**, in modo che i principali rischi afferenti all'emittente e alle sue controllate risultino correttamente identificati, nonché adeguatamente misurati, gestiti e monitorati, determinando inoltre il grado di compatibilità di tali rischi con una gestione dell'impresa coerente con gli obiettivi strategici individuati;
- valuta, con cadenza almeno annuale, **l'adeguatezza del sistema di controllo interno e di gestione dei rischi rispetto alle caratteristiche dell'impresa e al profilo di rischio assunto, nonché la sua efficacia**.

[cfr. 7.C.1]

Principali riferimenti

Le nuove sfide della Risk Governance

La gestione dei rischi di impresa è considerata, ormai da tempo, centrale nei sistemi di **corporate governance.**

In tale contesto, le principali normative e le **leading practices** di riferimento (es. recentemente i **principles of corporate governance** emessi dal **G20/OECD**) richiedono al Board di svolgere un ruolo di **risk oversight**, che consiste 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 accettare per raggiungere i propri obiettivi (**risk appetite**), nonché sulla 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

La **risk governance**, oltre a preservare l'approccio "difensivo" sui rischi a tutela del valore delle imprese, deve anche essere un **fattore abilitante del cambiamento e delle opportunità di business** che esso propone

Gli **attori della risk governance** devono **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**

Principali riferimenti

Board Risk Oversight

Le regole e linee guida di corporate governance a livello internazionale, oltre ad enfatizzare la centralità del rischio, sottolineano **l'importanza del ruolo di risk oversight del Board**

Principles of Corporate Governance, G20/OECD

Nuovi riferimenti sono inclusi in merito al ruolo del Consiglio di Amministrazione nell'attività di risk management e controllo interno. I nuovi principi prevedono la raccomandazione di istituire comitati specializzati in temi di gestione dei rischi ed il compito per il Board di ***"oversight of the company's risk management";***

(UK) Corporate Governance Code

Il codice di Corporate Governance inglese (conosciuto come "Combined Code") prevede espressamente che "the board is responsible for determining the nature and extent of the significant risks it is willing to take in achieving Its strategic objectives. The board should maintain sound risk management and internal control systems";

(UK) Guidance on Risk Management, Internal Control and Related Financial and Business reporting (FRC)

Tale guida, che costituisce il riferimento operativo nell'applicazione dei principi introdotti dal Codice di Corporate Governance inglese, prevede tra i compiti del Board:

- "***ensuring the design and implementation of appropriate risk management and internal control system*** that identify the risks face facing the company and enable the Board a robust assessment of the principal risk;
- determining the ***nature and extent of the principal risks*** faced and those risks which the organization is willing to take in achieving its strategic objectives (determining "risk appetite");
- ***agreeing how the principal risks should be managed*** or mitigated to reduce the likelihood of their incident or their impact;
- ***monitoring and reviewing the risk management and internal control systems***, and the management's process of monitoring and reviewing, and satisfy itself that they are functioning effectively and that corrective action is being taken where necessary".

Principali riferimenti

Il Codice di autodisciplina

CoSO* 2013

Il framework sottolinea il ruolo del *board* e dei suoi comitati (controllo e rischi, remunerazione, nomine)

Board Oversight

- Al ***board*** spetta un "*oversight responsibility*", il CEO e il senior management hanno una diretta responsabilità nello sviluppo e implementazione del sistema di controllo interno
- Il *board* è **indipendente** dal management e dimostra particolari **abilità e competenze** nello svolgere le sue responsabilità di supervisore

Le tre linee di controllo

- Il **management e il personale** rappresentano la prima linea di controllo nelle attività *day-to-day*
- Le **funzioni di supporto al business** forniscono la guida sui requisiti di controllo interno e valutano il rispetto degli standard definiti
- L'**internal auditor** è la terza linea di controllo nella valutazione e reporting sul controllo interno e raccomanda al management azioni correttive o miglioramenti

* CoSO (Committee of Sponsoring Organizations of the Treadway Commission), *Internal Control - Integrated Framework, Framework and Appendices*, (2013)

Principali riferimenti

Disposizioni di vigilanza prudenziale per le banche - 15° aggiornamento

L'entrata in vigore delle nuove disposizioni di vigilanza comporta un notevole cambiamento/aggiornamento per gli intermediari finanziari. **La magnitudo dell'impatto dipende dalla specificità di ogni intermediario.**

Di seguito **si riepilogano i principali temi chiave** che sono stati introdotti dalle disposizioni di vigilanza:

- **Governance**: Vengono univocamente attribuiti ruoli e responsabilità agli organi aziendali di supervisione, gestione e controllo. Definiti e dettagliati i compiti e le responsabilità dei vari organi e funzioni di controllo**.**

- **Funzioni aziendali di controllo**: La disciplina introduce novità rilevanti in relazione alle funzioni di *Risk Management*, *Compliance* ed *Internal Audit*. Inoltre prevede la formalizzazione delle interrelazioni tra le funzioni aziendali di controllo e nuove responsabilità per il rischio di natura fiscale (controlli di secondo livello).

- ***Risk Appetite Framework*: (RAF):** Introduzione dell'obbligo di definire e formalizzare un quadro di riferimento per la determinazione della propensione al rischio (*Risk Appetite Framework*). Tale quadro definisce la propensione al rischio, le soglie di tolleranza, i limiti di rischio, le politiche di governo dei rischi, i processi di riferimento necessari per definirli ed attuarli.

- ***Esternalizzazioni di funzioni aziendali*:**
  1) Definizione di una *Policy* di esternalizzazione;
  2) Nomine di Referenti per l'esternalizzazione di funzioni importanti o di controllo;
  3) Definizione e formalizzazione di accordi contrattuali con il fornitore con un set di clausole base;
  4) Comunicazioni a Banca d'Italia sui controlli effettuati sulle funzioni operative importanti/di controllo (annua) e sulla volontà di esternalizzare funzioni operative importati/ di controllo (ad evento).

- **Incident management:** comunicazione degli incidenti e dei fattori anomali rilevanti alle strutture preposte alla dichiarazione dello stato d'emergenza.
- Introduzione del **ruolo del CODISE**, struttura per il coordinamento della gestione delle crisi operative della piazza finanziaria italiana presieduta dalla Banca d'Italia.

- **Organizzazione della funzione di ICT, sicurezza informatica, controllo del rischio informatico,** compliance ICT e i compiti della funzione di revisione interna.
- **Valutazione del rischio potenziale** cui sono soggette le risorse informatiche esaminate.
- Individuazione delle misure di sicurezza idonee a conseguire il **contenimento del rischio individuato** (trattamento del rischio).
- Policy di sicurezza informatica approvata dall'organo con funzione di supervisione strategica e comunicata a tutto il personale e terze parti.
- **Sicurezza delle informazioni e delle risorse ICT** (presidi fisici, accessi logici, autenticazione, monitoraggio, tracciamento, sviluppo sicuro del SW, gestione del personale, ecc.).
- **Gestione dei cambiamenti.**
- **Gestione degli incidenti di sicurezza.**
- **Disponibilità delle informazioni e dei servizi ICT.**
- La **gestione dei dati** deve soddisfare specifici requisiti (es.: data governance, data warehouse, documentazione delle procedure di gestione dei dati, ecc. ...).
- Applicazione della **politica di esternalizzazione** (anche in funzione dei requisiti alla sezione IV del cap. 7) con disposizione di specifiche indicazioni.
- Valutazioni dei rischi connessi al **cloud computing.**

Gli impatti delle nuove disposizioni di vigilanza prudenziali sono trasversali su tutta la Banca

Agenda

- Principali riferimenti
- Gli attori del Sistema di controllo interno e gestione dei rischi
- Focus: Linee di indirizzo SCIGR
- Focus: Risk Appetite e Risk Tolerance
- Focus: Il livello di controllo - modelli di presidio e processo integrato
- Focus: Compliance Trasformation e presidio dei rischi

Gli attori del SCIGR

Gli attori del Sistema di controllo interno e gestione dei rischi

Secondo il codice di autodisciplina e le best practice di riferimento, diversi attori contribuiscono al funzionamento del SCIGR. Il **CdA svolge un ruolo centrale** nella supervisione del complessivo SCIGR

Specifici compiti in tema di controllo dei rischi; sono articolate in relazione a dimensioni, complessità e profilo di rischio dell'impresa

cd **Funzioni di secondo livello di controllo**

Attori del SCIGR

Supporta il CdA con istruttorie e valutazione sul SCIGR

Dà esecuzione alle linee di indirizzo del CdA e cura l'identificazione dei principali rischi aziendali

Vigila su efficacia SCIGR

Verifica funzionamento e adeguatezza SCIGR

Business Judgment Rule

A legal principle that makes officers, directors, managers, and other agents of a corporation immune from liability to the corporation for loss incurred in corporate transactions that are within their authority and power to make when sufficient evidence demonstrates that the transactions were made according to risk and control system

Gli attori del SCIGR

Il Consiglio di Amministrazione (1/3)

1

La concreta esplicazione del ruolo del Consiglio di Amministrazione si sostanzia nella definizione delle **Linee di indirizzo sul SCIGR**, in modo che i principali rischi afferenti alla società e alle sue controllate, risultino correttamente identificati, nonché adeguatamente misurati, gestiti e monitorati.

Il CdA, previo parere del CCR, definisce, tramite una linea guida, **l'architettura e il funzionamento complessivo** il sistema di controllo interno e di gestione dei rischi (SCIGR) nell'ambito del sistema normativo aziendale

NEW

Codice di Autodisciplina 2015

Art. 7.C.1 – d) Il consiglio di amministrazione descrive*, nella relazione sul governo societario, le principali caratteristiche del sistema di controllo interno e di gestione dei rischi e* ***le modalità di coordinamento tra i soggetti in esso coinvolti,*** *esprimendo la propria valutazione sull'adeguatezza dello stesso*

Il Codice introduce la necessità che l'emittente preveda adeguate **modalità di coordinamento** tra il CdA, l'amministratore incaricato del SCIGR, il CCR, il responsabile della funzione *audit*, gli altri ruoli e funzioni aziendali coinvolti, nonché il CS, al fine di **massimizzare l'efficienza del SCIGR, ridurre la duplicazione di attività e realizzare un efficace sistema di controlli interni**.

Le modalità di coordinamento tra i soggetti coinvolti dovranno essere considerate, inoltre, dal CdA nell'ambito della valutazione dell'adeguatezza e dell'efficacia del sistema.

Gli attori del SCIGR

Il Consiglio di Amministrazione (2/3)

2

Nella definizione del "**Risk Appetite**", al fine di determinare il grado di compatibilità dei principali rischi aziendali con una gestione dell'impresa coerente con gli obiettivi strategici.

A tal fine, il Risk Appetite dovrebbe:

- essere **facile da comunicare** e quindi **facile da comprendere** per gli stakeholder;
- essere direttamente **collegato alla strategia aziendale**;
- fissare **limiti quantitativi** e **dichiarazioni qualitative** per i rischi che sono difficili da misurare. I limiti quantitativi possono essere espressi in termini di guadagni, capitale, liquidità, o altre metriche appropriate (ad esempio la crescita, la volatilità). Dichiarazioni qualitative dovrebbero integrare le misure quantitative.

Fonte: Financial Stability Board: "Principles for An Effective Risk Appetite Framework"

NEW

Codice di Autodisciplina 2015

Art. 1.C.1 – b) *Il consiglio di amministrazione definisce la natura e il livello di rischio compatibile con gli obiettivi strategici dell'emittente, includendo nelle proprie valutazioni tutti i rischi che possono assumere rilievo nell'ottica* ***della sostenibilità nel medio-lungo periodo dell'attività dell'emittente***

Il Codice introduce un riferimento esplicito al **parametro della sostenibilità** che, a partire dalla valutazione dei rischi dell'attività, finisce con il permeare l'intero arco di attività della società, richiedendo di fatto al CdA di fissare i **valori generali** cui si dovrà ispirare l'attività d'impresa. L'ampia formulazione del Codice sembra non soltanto riferirsi alla valutazione dei rischi strettamente collegati alle variabili economico-finanziarie dell'impresa, ma anche aprire la strada **alla valutazione di ulteriori rischi, di natura non strettamente finanziaria**.

Inoltre, il Codice prevede che, nelle società appartenenti all'indice **FTSE-Mib**, il CdA possa valutare l'opportunità di costituire un **apposito comitato dedicato alla supervisione delle questioni di sostenibilità**.

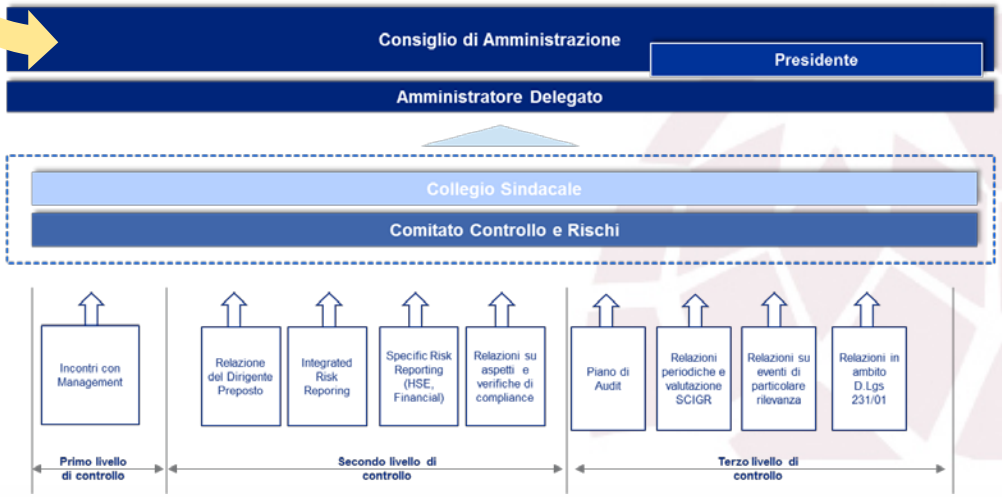
Gli attori del SCIGR

Il Consiglio di Amministrazione (3/3)

3

Nella valutazione periodica dell'**adeguatezza del SCIGR** rispetto alle caratteristiche dell'impresa e al profilo di rischio assunto, nonché della sua efficacia.

A tal fine il CdA riceve specifici i **flussi informativi** (cd. Flussi verticali) dalle funzioni aziendali preposte al controllo sia di II livello (es. Risk Management, Compliance, etc) sia di III livello (Internal Audit)



L'insieme delle interrelazioni che intercorrono tra organi aziendali, funzioni di controllo e management, rappresenta uno dei fondamentali meccanismi operativi di funzionamento del SCIGR

Gli attori del SCIGR

Il Comitato controllo e rischi

Il CdA individua al suo interno un Comitato Controllo e Rischi (CCR), con il compito di **supportare**, con un'adeguata attività istruttoria, le **valutazioni e le decisioni del CdA relative al SCIGR**

Principali Responsabilità in ambito SCIGR

Il CCR, nell'assistere il CdA: (…)

b) **esprime pareri** su specifici aspetti inerenti alla **identificazione dei principali rischi** aziendali;

c) **esamina** le relazioni periodiche, aventi per oggetto la **valutazione del sistema di controllo interno e di gestione dei rischi**, e quelle di particolare rilevanza predisposte dalla funzione internal audit; (…)

f) **riferisce** al consiglio, almeno semestralmente, (…), **sull'attività svolta** nonché **sull'adeguatezza del sistema di controllo interno e di gestione dei rischi**

art. 7.C.2

Composizione

Il CCR è composto da **amministratori indipendenti** o da **amministratori non esecutivi**, in **maggioranza indipendenti**. ***art. 7.P.4***

NEW

Codice di Autodisciplina 2015

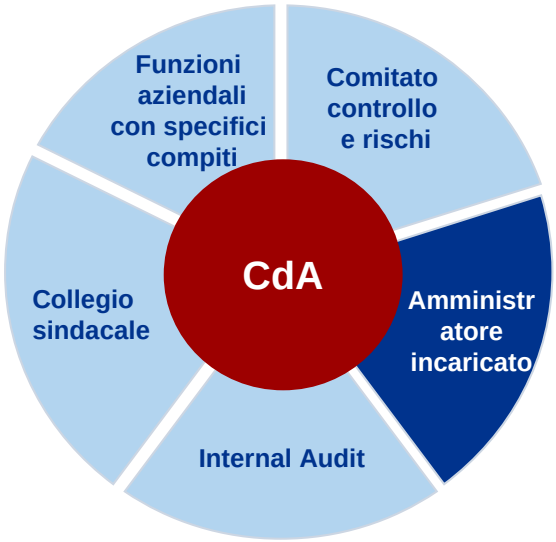
Art. 7.C.2 – g) *Il CCR supporta, con un'adeguata attività istruttoria, le valutazioni e le decisioni del consiglio di amministrazione* ***relative alla gestione di rischi derivanti da fatti pregiudizievoli*** *di cui il CdA sia venuto a conoscenza*

Il Codice esplicita, che l'attività di supporto del CCR al CdA deve avere luogo **anche e, in particolare, al verificarsi di fatti pregiudizievoli** di cui il Consiglio venga a conoscenza.

Gli attori del SCIGR

Amministratore incaricato

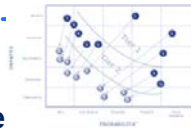
4



Il CdA individua al suo interno **uno o più amministratori incaricati dell'istituzione e del mantenimento di un efficace ed efficiente SCIGR**

Principali Responsabilità

a) cura l'**identificazione dei principali rischi aziendali**, tenendo conto delle caratteristiche delle attività svolte dalla società e dalle sue controllate, e li **sottopone periodicamente all'esame del CdA**;



b) **dà esecuzione alle linee di indirizzo** definite dal CdA, curando la **progettazione, realizzazione** e **gestione** del **SCIGR** e **verificandone** costantemente l'**adeguatezza** e **l'efficacia**;

c) si occupa dell'**adattamento** di tale sistema alla dinamica delle **condizioni operative e del panorama legislativo e regolamentare;**

d) può **chiedere alla funzione di internal audit** lo svolgimento di **verifiche su specifiche aree operative;**

e) **riferisce tempestivamente** al **CCR (o al CdA)** in merito a **problematiche** e **criticità** emerse nello svolgimento della propria attività o di cui abbia avuto comunque notizia, affinché il comitato (o il consiglio) possa prendere le opportune iniziative.

art. 7.C.4

Gli attori del SCIGR

Secondo e terzo livello di controllo

Le funzioni aziendali alle quali sono affidati i cosiddetti **controlli "di secondo livello"** sono volte a **monitorare i rischi tipici aziendali** (rischio operativo, finanziario, di mercato, di non conformità, etc.)

Le funzioni cui è attribuito un controllo di secondo livello sono chiamate a **mettere in atto un processo strutturato di analisi dei rischi** e sono **soggette alla revisione generale da parte dell'internal audit**.

Commento art. 7

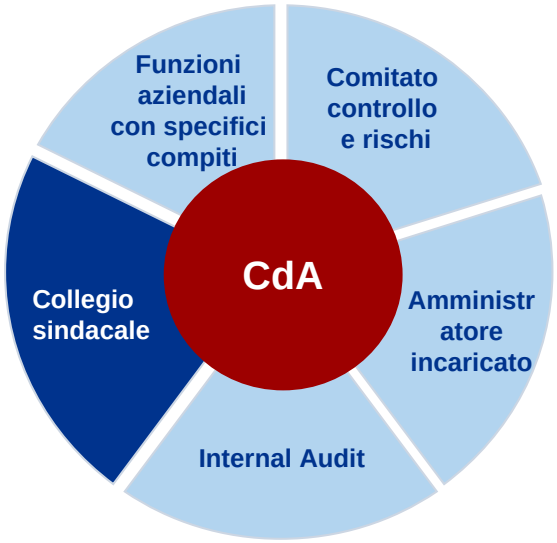
NEW **Codice di Autodisciplina 2015**

Commento Art 7 *- Un ruolo di* ***particolare rilevanza*** *nell'ambito del SCIGR è normalmente ricoperto* ***dalle funzioni legali e di compliance****, con particolare riferimento al presidio del rischio legale e di non conformità, ivi incluso anche il rischio della commissione di illeciti penali a danno o nell'interesse dell'azienda*

Commento Art 7 *- Almeno nelle società emittenti appartenenti all'indice FTSE-Mib, un adeguato SCIGR deve essere dotato di un* ***sistema interno di segnalazione*** *da parte dei dipendenti di eventuali irregolarità o violazioni della normativa applicabile e delle procedure interne (c.d. sistemi di* ***whistleblowing****) in linea con le best practices esistenti in ambito nazionale e internazionale, che garantiscano un canale informativo specifico e riservato nonché l'anonimato del segnalante.*

Gli attori del SCIGR

Il Collegio SIndacale



Il quadro degli attori del sistema dei controlli è completato dal **Collegio Sindacale**, che rappresenta il **vertice del sistema di vigilanza di un emittente.**

Il **Collegio Sindacale** ha la responsabilità di vigilare sulla completezza, adeguatezza, funzionalità e affidabilità del SCIGR.

È destinatario dei flussi informativi necessari per l'esercizio dei propri compiti.

Al Collegio Sindacale spetta un **compito di vigilanza anche preventiva e non meramente *ex post***, che si traduce in una **verifica sui processi** il cui esito va portato all'attenzione degli amministratori, affinché essi adottino le **misure correttive** eventualmente necessarie.

Agenda

- Principali riferimenti
- Gli attori del Sistema di controllo interno e gestione dei rischi
- Focus: Linee di indirizzo SCIGR
- Focus: Risk Appetite e Risk Tolerance
- Focus: Il livello di controllo - modelli di presidio e processo integrato
- Focus: Compliance Trasformation e presidio dei rischi

Focus: Linee di indirizzo SCIGR

Obiettivi

Il Consiglio di Amministrazione al fine di fornire le linee di indirizzo del SCIGR **definisce uno strumento normativo per la disciplina integrata del SCIGR** coerente con i requisiti normativi (ove applicabili es. nel settore finanziario), di autodisciplina e di leading practices (es. CoSO Report)

Obiettivi

- consolidare e strutturare in modo organico ed efficiente **il ruolo delle differenti componenti del SCIGR**
- **identificare i flussi informativi** in materia di SCIGR e le modalità di coordinamento e collaborazione tra gli attori
- nei gruppi aziendali, definire un **modello di relazione** (**direzione e coordinamento**) tra la società e le società controllate in materia di SCIGR

Focus: Linee di indirizzo SCIGR

Principali contenuti (1/3)

Le **Linee di Indirizzo del CdA** descrivono il SCIGR e in particolare prevedono i seguenti contenuti:

1 OBIETTIVO, AMBITO DI APPLICAZIONE E MODALITA' DI RECEPIMENTO
- OBIETTIVO DEL DOCUMENTO
- AMBITO DI APPLICAZIONE E MODALITA' DI RECEPIMENTO

2 PRINCIPI E FRAMEWORK DI RIFERIMENTO
- PRINCIPI DI RIFERIMENTO DEL SCIGR
- FRAMEWORK DI RIFERIMENTO

3 ARCHITETTURA

4 ATTORI, COMPITI E RESPONSABILITA'
- CONSIGLIO DI AMMINISTRAZIONE
- PRESIDENTE DEL CONSIGLIO DI AMMINISTRAZIONE
- COMITATO CONTROLLO E RISCHI
- AMMINISTRATORE DELEGATO
- ...

5 MODALITA' DI ATTUAZIONE NELLE SOCIETA' CONTROLLATE

6 FLUSSI INFORMATIVI E MODALITA' DI COORDINAMENTO

Focus: Linee di indirizzo SCIGR

Principali contenuti (2/3)

Linee Guida SCIGR

PRINCIPALI CONTENUTI 1/2

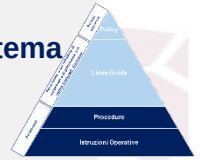
Principi e framework di riferimento:

- sistema integrato
- conformità alla legge e coerenza con il quadro di riferimento generale
- approccio basato sui rischi
- ….

Architettura del SCIGR

Il SCIGR è l'insieme di strumenti, strutture organizzative, norme e regole aziendali volte a consentire una conduzione dell'impresa sana, corretta e coerente con gli obiettivi aziendali.

A tal riguardo, l'architettura del SCIGR è definita sulla base di un **Sistema Normativo Integrato.**



Approfondimento slide successive

Lo SCIGR, inoltre, prevede un'articolazione delle responsabilità di controllo su tre livelli :

- **Primo livello:** Identifica, valuta, gestisce e monitora i rischi di competenza in relazione ai quali individua e attua specifiche azioni di trattamento dirette ad assicurare il corretto svolgimento delle operazioni.
- **Secondo livello di controllo:** monitora i rischi aziendali, propone le linee guida sui relativi sistemi di controllo e verifica l'adeguatezza degli stessi al fine di assicurare efficienza ed efficacia delle operazioni, adeguato controllo dei rischi, prudente conduzione del business, affidabilità delle informazioni, conformità a leggi, regolamenti e procedure interne**.**
- **Terzo livello di controllo:** Fornisce assurance indipendente sull'adeguatezza ed effettiva operatività del primo e secondo livello di controllo ed, in generale, sul SCIGR.

Focus: Linee di indirizzo SCIGR

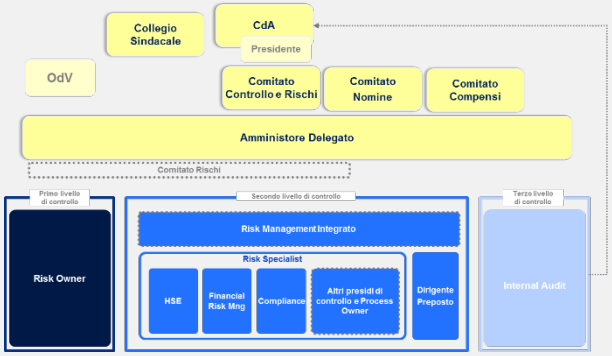
Principali contenuti (3/3)

Linee Guida SCIGR

PRINCIPALI CONTENUTI 2/2

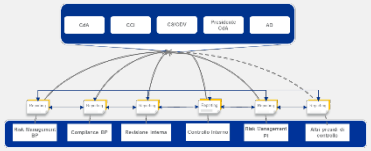
Attori, compiti e responsabilità:
Identificazione di tutti gli attori del SCIGR e delle responsabilità degli stessi in tale ambito:

- Esemplificativo -



Modalità di attuazione nelle società controllate:
Identificazione delle modalità di recepimento delle linee di indirizzo nelle società controllate

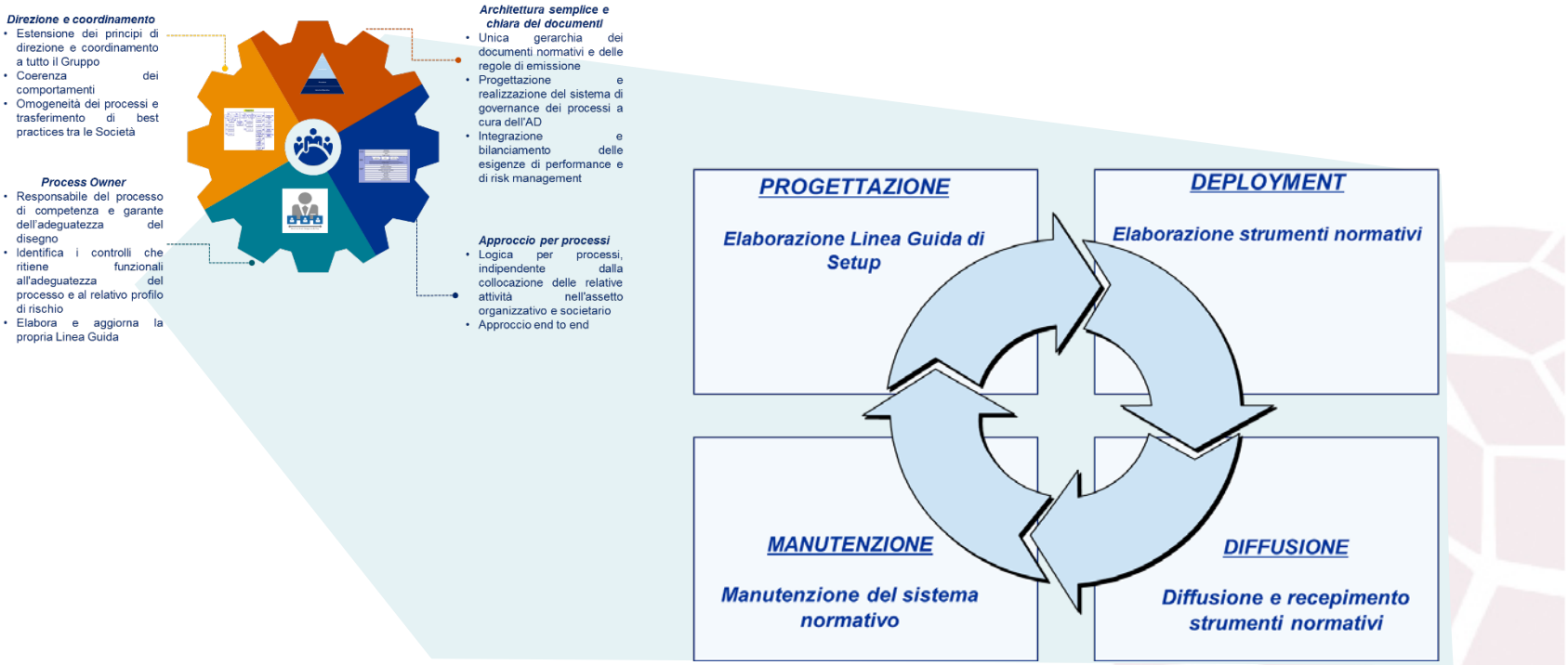
Flussi informativi e modalità di coordinamento
Identificazione dei flussi informativi dalle funzioni di controllo verso gli organi aziendali e tra le funzioni di controllo



Focus: Linee di indirizzo SCIGR

Approfondimento Sistema Normativo Integrato

Sarà compito **dell'Amministratore Incaricato del SCIGR dare attuazione alle linee di indirizzo del CdA** per l'implementazione del un Sistema Normativo Integrato:



Agenda

- Principali riferimenti
- Gli attori del Sistema di controllo interno e gestione dei rischi
- Focus: Linee di indirizzo SCIGR
- Focus: Risk Appetite e Risk Tolerance
- Focus: Il livello di controllo - modelli di presidio e processo integrato
- Focus: Compliance Trasformation e presidio dei rischi

Focus: Risk Appetite e Risk Tolerance

Risk Appetite Statement nell'ambito del processo di ERM

Una delle fasi fondamentali del processo di **Enterprise Risk Management** (c.d. Risk Management integrato) è la definizione del Risk Appetite Statement, che costituisce uno degli **strumenti di indirizzo del board** in materia di Risk Management in quanto, attraverso la definizione dei livelli di rischio desiderati e tollerati (cd. Risk Appetite, Risk Tolerance), indirizza le successive fasi di **trattamento e monitoraggio dei rischi**.

Schema concettuale del documento di Risk Appetite Statement nell'ambito del processo ERM

Documento di Risk Appetite Statement

- Determina e formalizza la **propensione** (cd. Risk Appetite) e la **tolleranza** (cd. Risk Tolerance) rispetto **ai rischi maggiormente rilevanti**
- **Strumento di indirizzo del board** per la gestione ed il monitoraggio dei rischi
- Consente di **focalizzare e strutturare** i piani di **trattamento** e l'attività di **monitoraggio** dei rischi

Piano di trattamento del rischio

- Strumento attraverso cui esplicitare le azioni di trattamento sui **rischi rilevanti**, al fine di **contenere l'esposizione** di questi ultimi **ai livelli di appetite e tolerance** determinati dal vertice aziendale
- Possono prevedere **misure finalizzate ad orientare i comportamenti** in termini di valutazione e assunzione del rischio cd. **Risk Policy** o a trasferire e ridurre il rischio in termini di **rafforzamento di sistemi di controllo**

Monitoraggio rischi

- Attività mediante la quale **monitorare l'esposizione** della Società rispetto ai rischi rilevanti in funzione dei livelli desiderati e tollerati
- Svolta mediante la **verifica dell'andamento degli indicatori di rischio definiti**, l'aggiornamento di **studi** quantitativi del rischio o attraverso **valutazione** dei Risk Owner.

Focus: Risk Appetite e Risk Tolerance

Risk Appetite Framework

Il **Risk Appetite Framework,** ovvero l'approccio metodologico da prevedere nello sviluppo del Risk Appetite statement, tipicamente è strutturato prevedendo approcci top down, funzionali a fornire una rappresentazione multidimensionale dei rischi organizzata in tipicamente in categorie omogenee rappresentative di ciascun rischio.

Tale approccio consente per ciascuna categoria di effettuare un'esplorazione dei contenuti sottostanti ai fini di ottenere il livello di dettaglio desiderato.

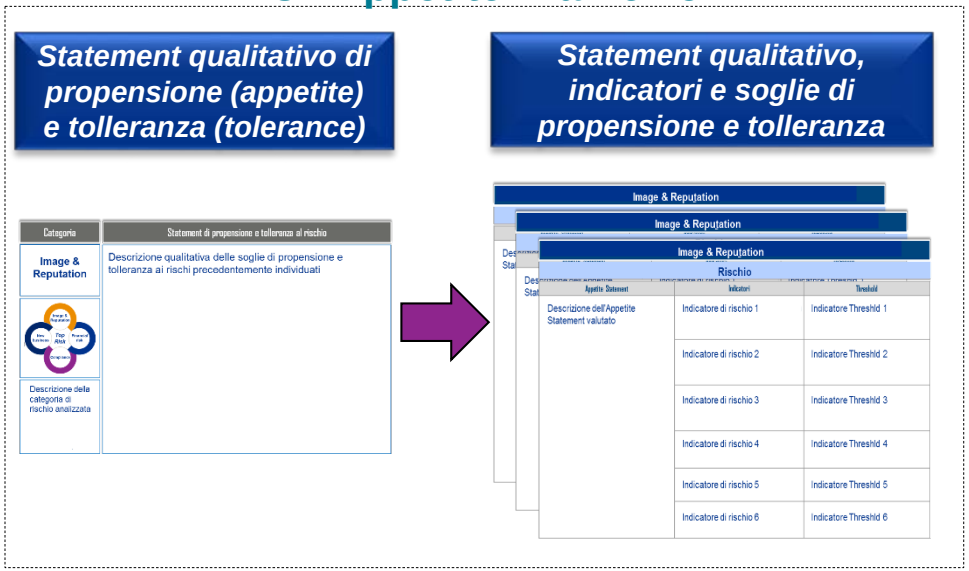
- Risk Appetite Framework -

Focus: Risk Appetite e Risk Tolerance

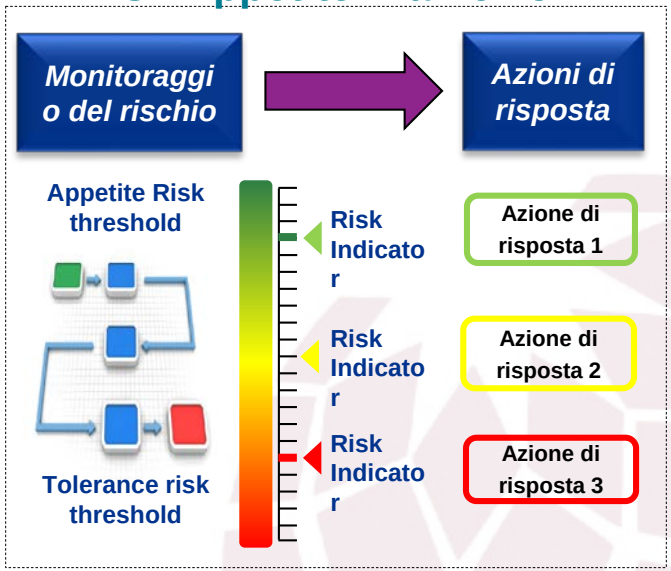
Risk Appetite Framework

Inoltre, a seconda della maturità dei modelli di Enterprise Risk Management e dell'effettivo utilizzo dello strumento di Risk Appetite Statement, quale elemento in ingresso per l'attività di *risk monitoring* e *risk treatment*, i framework ERM possono prevedere una **declinazione quantitativa delle soglie di Risk Appetite e Tolerance**, associate a ciascun Key Indicator (KI).

- Risk Appetite Framework -



- Risk Appetite Framework -



Il **costante monitoraggio** degli indicatori di rischio consente di attivare tempestivamente le azioni di risposta ed i processi di condivisione ai diversi livelli aziendali, al fine di mantenere i livelli di rischio nei limiti definiti dal board.

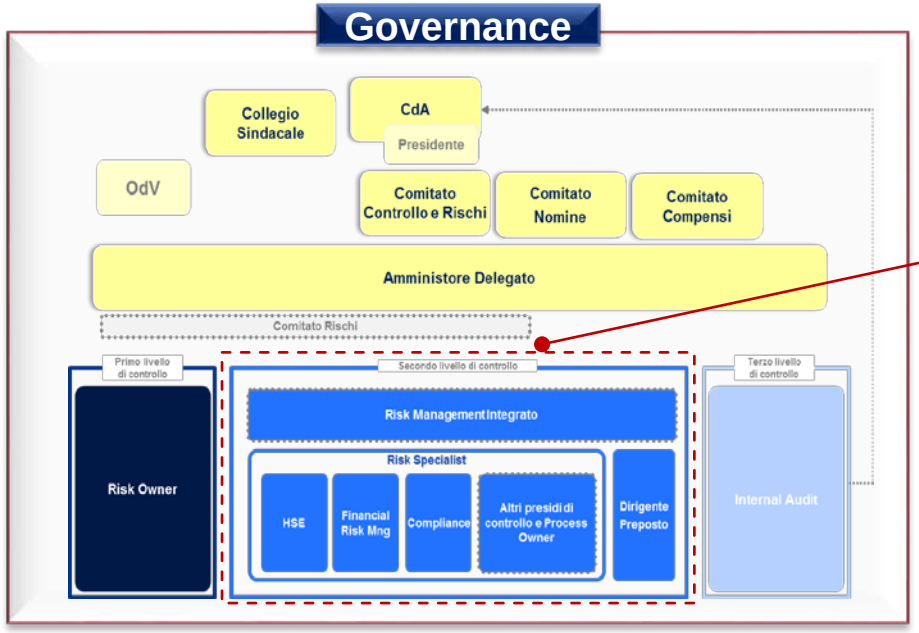
Agenda

- Principali riferimenti
- Gli attori del Sistema di controllo interno e gestione dei rischi
- Focus: Linee di indirizzo SCIGR
- Focus: Risk Appetite e Risk Tolerance
- Focus: Il livello di controllo - modelli di presidio e processo integrato
- Focus: Compliance Trasformation e presidio dei rischi

Focus: Il livello di controllo

Principali compiti

Nell'ambito dell'architettura del SCIGR particolare rilievo **assumono le funzioni con compiti di II livello di controllo**:



Principali responsabilità

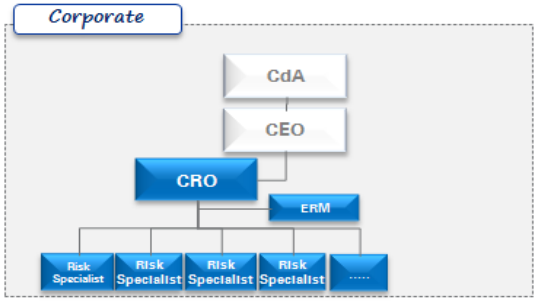
- **Monitorano i rischi aziendali**, **propongono le linee guida** sui relativi sistemi di controllo e **verificano l'adeguatezza degli stessi** al fine di assicurare efficienza ed efficacia delle operazioni, adeguato controllo dei rischi, prudente conduzione del business, affidabilità delle informazioni, conformità a leggi, regolamenti e procedure interne.
- Le funzioni preposte a tali controlli **sono distinte da quelle operative**; esse concorrono alla definizione delle politiche di governo dei rischi e del processo di gestione dei rischi.

*"Ciascun emittente stabilisce quale sia **l'assetto organizzativo più idoneo**, **in relazione alle caratteristiche dell'impresa**, a consentire un efficace presidio sui rischi: in tal modo, è possibile che il monitoraggio e la gestione dei rischi vengano affidati alla responsabilità di manager (e strutture aziendali) non dedicati a ciò in via esclusiva"*

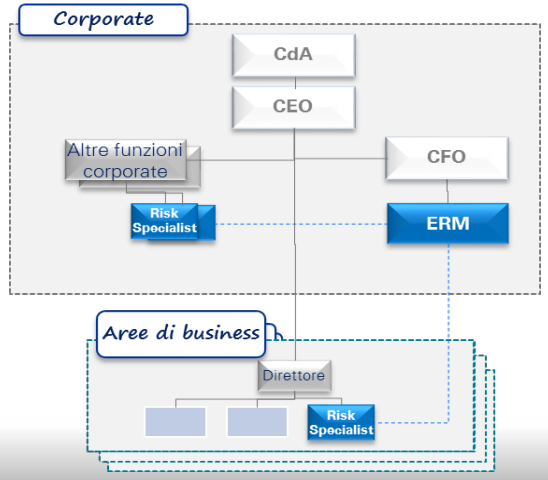
Focus: Il livello di controllo

Modelli organizzativi di presidio (1/2)

Uno dei **fattori critici di successo** per l'implementazione di un sistema integrato dei rischi è la scelta del modello organizzativo. Le **soluzioni organizzative adottate** si possono schematizzare come segue:



1. **Modello accentrato** con un CRO alle dirette dipendenze del Vertice Aziendale (AD) e con presidio diretto su le principali aree di rischio aziendale

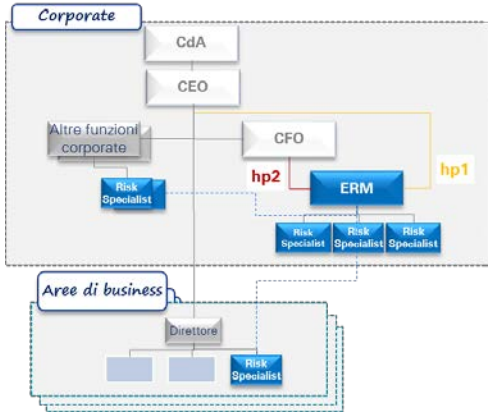


2. **Modello decentrato** con funzione centrale con ruolo di supporto metodologico, coordinamento e reporting e presenza di risk specialist nelle diverse aree di business.

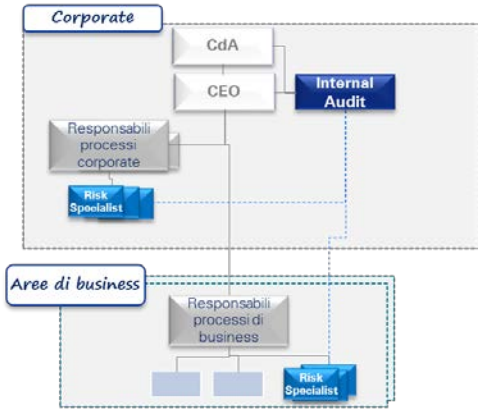
   In questo Modello la funzione centrale è collocata frequentemente **nell'area del CFO**

Focus: Il livello di controllo

Modelli organizzativi di presidio (2/2)



3. **Modello misto** con **funzione centrale alle dirette dipendenze del Vertice Aziendale (AD) o area CFO**, con presidio diretto di alcuni rischi specifici (es. strategici, reputazionali, etc.) e coordinamento di risk specialist decentrati presso le aree di business



4. Modello basato **sui processi aziendali** ossia un modello in cui sono identificati dei **Risk Specialist a presidio dei rischi specifici dei diversi processi** e **il ruolo di sintesi è spesso affidato alla Funzione di Internal Audit.** Tale modello, presente prevalentemente in ambito internazionale, è ipotizzabile in realtà in cui l'organizzazione è fortemente sviluppata per processo.

Focus: Il livello di controllo

Modelli organizzativi di presidio nel settore finanziario (1/3)

Nel **settore finanziario**, i **modelli di presidio dei rischi** sono definiti in coerenza con le normative di riferimento*. In particolare è prevista l'istituzione di due funzioni aziendali di secondo livello di controllo:

Funzione di Conformità alle norme (Compliance)

Funzione di Controllo dei rischi (Risk Management)

I responsabili delle funzioni, secondo quanto previsto dalle disposizioni di vigilanza (circ. 263, 15° agg.):

- sono collocati alle **dirette dipendenze dell'organo con funzione di gestione** o **dell'organo con funzione di supervisione strategica**;
- **non hanno responsabilità diretta di aree operative** sottoposte a controllo né sono gerarchicamente subordinati ai responsabili di tali aree;
- **sono nominati e revocati dall'organo con funzione di supervisione strategica**, sentito l'organo con funzione di controllo;
- **riferiscono direttamente** agli organi aziendali.

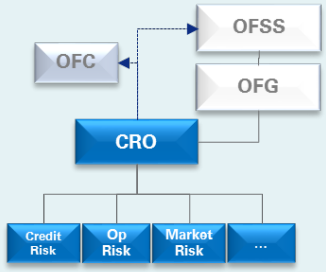
*Circ. 263 / 2006 Bankit
Circ 285 / 2013 Bankit

Focus: Il livello di controllo

Modelli organizzativi di presidio nel settore finanziario (2/3)

Con riferimento alla funzione controllo dei **rischi**:

Controllo dei rischi (Risk Management)



La funzione di controllo dei rischi **può essere variamente articolata**, ad esempio in relazione ai **singoli profili di rischio** (di credito, di mercato, operativo, modello, ecc.), purché la banca mantenga **una visione d'insieme dei diversi rischi** e della loro reciproca interazione. (…)
Specie nelle banche più complesse, può essere prevista la costituzione di specifici **comitati di gestione dei diversi profili di rischio** (ad es., rischi di credito e operativi, liquidità, etc) (…)

Circ. 263. Titolo V cap.7

La funzione di controllo dei rischi dovrebbe garantire che tutti i principali rischi cui l'ente è esposto siano **individuati e adeguatamente gestiti** dalle pertinenti unità dell'ente, e che un **quadro complessivo di tutti i rischi rilevanti** sia sottoposto all'organo gestorio.

EBA Guidelines on internal governance

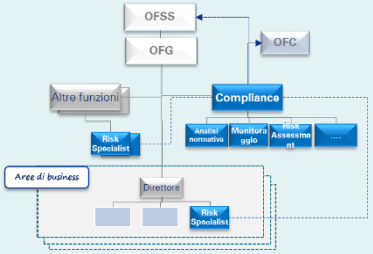
*I modelli organizzativi di presidio prevalenti sono riconducibili ad un **modello accentrato** con la presenza di un CRO, a diretto riporto dell'Amministratore Delegato, che presidia nell'ambito della propria struttura organizzativa i principali rischi della banca (I e II pilastro). Nei principali gruppi bancari sono presenti referenti di risk management a livello di società coordinati funzionalmente dal CRO della capogruppo.*

Focus: Il livello di controllo

Modelli organizzativi di presidio nel settore finanziario (3/3)

Con riferimento alla funzione conformità alle **norme**:

Conformità alle norme (Compliance)



La **funzione di conformità alle norme** presiede, secondo un approccio **risk based**, alla gestione del rischio di non conformità con **riguardo a tutta l'attività aziendale**, verificando che le procedure interne siano adeguate a prevenire tale rischio.

Per le norme più rilevanti ai fini del rischio di non conformità (es. esercizio dell'attività bancaria e di intermediazione, conflitti di interesse, tutela del consumatore), e per quelle norme per le quali non siano già previste forme di presidio specializzato all'interno della banca, **la funzione è direttamente responsabile della gestione del rischio di non conformità.**

Con riferimento ad altre normative per le quali siano già previste forme specifiche di **presidio specializzato** (ad es.: normativa sulla sicurezza sul lavoro, in materia di trattamento dei dati personali), **la banca**, in base a una valutazione dell'adeguatezza dei controlli specialistici a gestire i profili di rischio di non conformità, **può graduare i compiti della compliance** (…)

- **Presidio diretto sulla normativa "core"**
- **Presidio indiretto, tramite presidi specialistici, sulle altre normative applicabili**

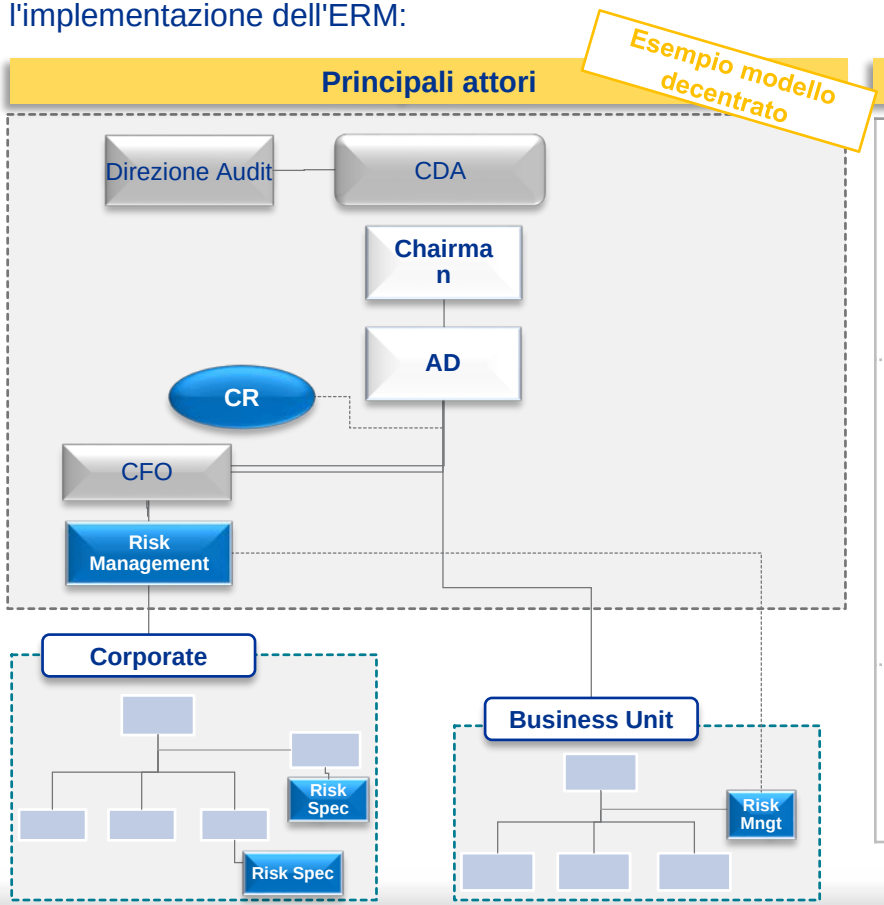
Compliance Framework

Focus: Il livello di controllo

Soluzioni organizzative adottate in Gruppi Italiani (1/3)

Di seguito le **soluzioni adottate da gruppi italiani** che hanno iniziato negli ultimi anni un percorso evolutivo per l'implementazione dell'ERM:

Principali attori



Principali responsabilità

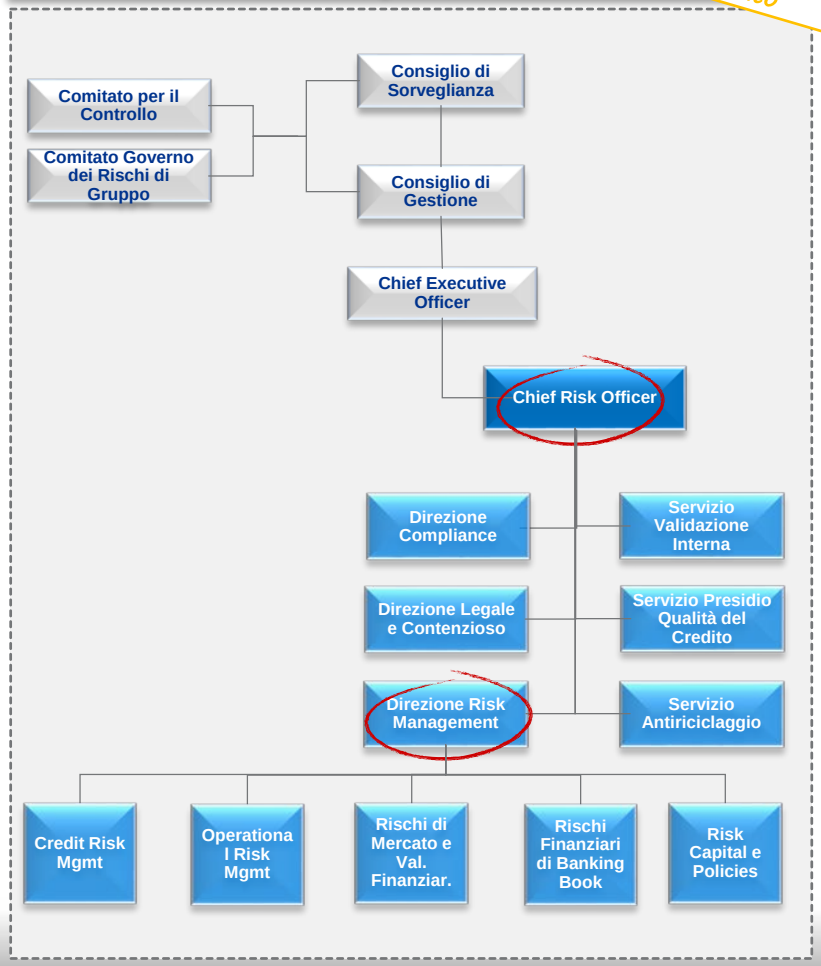
Risk Management	• Coordina il processo di Risk Management e fornisce supporto metodologico all'assessment ed al trattamento dei rischi. • Supporta il Responsabile AFC nel coordinamento del Comitato di Risk Management
Comitato Risk Management	• Presieduto dal CFO e composto dall'AD e dalle prime linee manageriali Garantisce il governo del processo di gestione dei rischi di gruppo, coordinando il piano di azioni preventive finalizzate ad assicurare la continuità operativa del business e monitorando l'efficacia delle contromisure adottate
Risk Specialist	• Supportano i responsabili di funzione nella identificazione e valutazione dei rischi e nella successiva fase di definizione dei piani di trattamento dei rischi

Focus: Il livello di controllo

Soluzioni organizzative adottate in Gruppi Italiani (2/3)

Esempio modello accentrato

Principali attori



Principali responsabilità

Chief Risk Officer

- Definire gli indirizzi e le politiche in materia di gestione dei rischi, compliance e legale;
- Coordinare e verificare l'attuazione degli stessi;
- Garantire la misurazione e il controllo dell'esposizione alle diverse tipologie di rischio;
- Assicurare il presidio della qualità del credito garantendo il rispetto degli indirizzi e delle strategie creditizie;
- Presidiare l'identificazione e il monitoraggio di eventuali disallineamenti dalle norme vigenti, nonché la sensibilizzazione delle funzioni aziendali alle normative

Direzione Risk Management

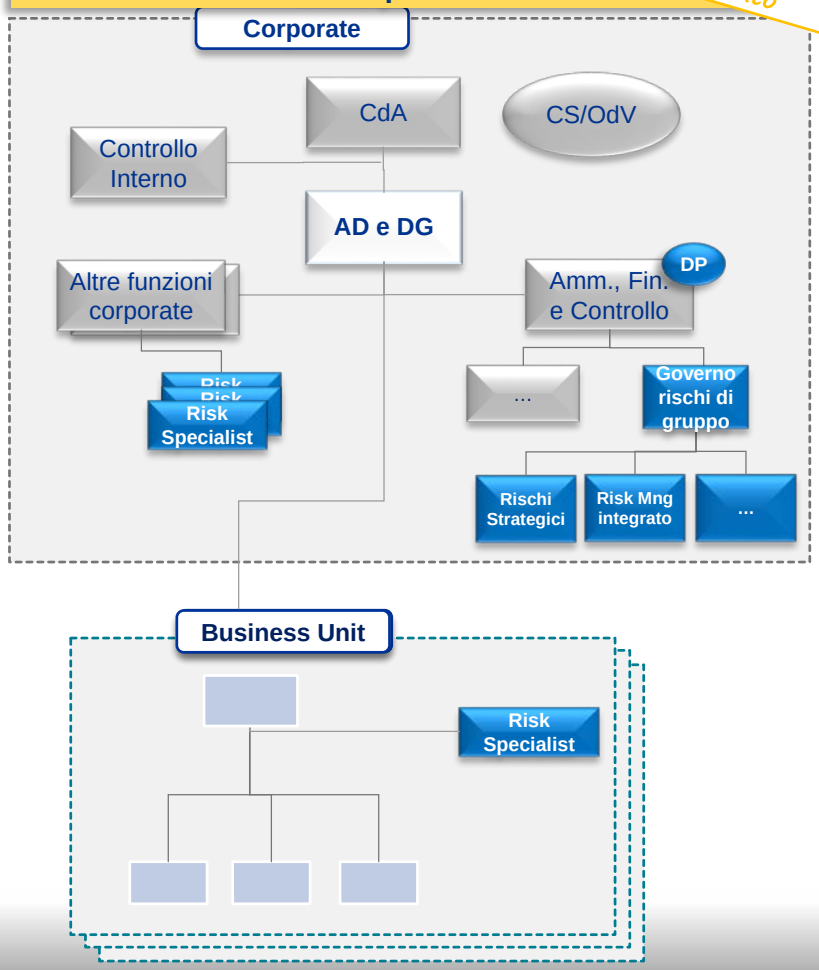
- Garantire la misurazione ed il controllo dell'esposizione alle diverse tipologie di rischio;
- Monitorare gli assorbimenti di capitale (capital requirements) supportando le funzioni preposte nell'attività di gestione attiva del capitale;
- Proporre al Vertice la definizione della struttura dei limiti operativi, in coerenza con il capitale allocato;
- Seguire gli sviluppi della regolamentazione e assicurare all'OdV le informazioni;
- Sviluppare e manutenere sistemi di misurazione, gestione e controllo dei rischi conformi alla normativa Basilea 2 ed allineati alla best practice internazionale.

Focus: Il livello di controllo

Soluzioni organizzative adottate in Gruppi Italiani (3/3)

Esempio modello accentrato

Principali attori



Principali responsabilità

Governo Rischi di Gruppo

- Garantire il processo di individuazione, valutazione e monitoraggio dei rischi del Gruppo
- Provvedere all'identificazione, valutazione, misurazione e monitoraggio dei rischi strategici
- Curare l'armonizzazione dei modelli di risk management e l'individuazione di iniziative volte a sviluppare e diffondere una cultura aziendale
- Assicurare la reportistica integrata dei rischi

Risk Specialist

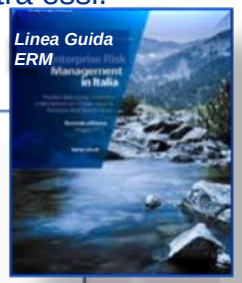
I Risk Specialist sono figure con compiti specifici e responsabilità di controllo su diverse aree/tipologie di rischio. In coerenza con il framework metodologico generale, i Risk Specialist, ove esistenti , contribuiscono, in relazione alle specifiche aree/tipologie di rischio presidiato, al processo di governo dei rischi di gruppo, ossia all'identificazione, valutazione, monitoraggio e reporting dei principali rischi in funzione delle informazioni e dei dati in loro possesso e, ove applicabile, in coerenza con i requisiti normativi e regolamentari

Focus: Il livello di controllo

Enterprise Risk Management - Linee Guida

- Il **processo di gestione integrata dei rischi (ERM)** ha la finalità di supportare il management e il CdA nell'assumere decisioni compatibili con il **profilo di rischio della società** e coerenti con gli obiettivi aziendali.
- Al fine di creare un processo integrato di gestione dei rischi, la società può dotarsi di Linee Guida ERM che:
  - definiscono i **principi di riferimento del processo**;
  - regolano le fasi dei sotto-processi e le **modalità di svolgimento delle attività**;
  - individuano **ruoli e responsabilità** dei principali attori, nonché le **modalità di collaborazione** tra essi.

Obiettivi



- Promuovere la **diffusione del risk management** nei processi aziendali al fine di garantire **coerenza nelle metodologie e negli strumenti** di gestione e nel controllo dei rischi
- Sviluppare un **linguaggio comune** e diffondere un'adeguata **cultura di gestione dei rischi**
- Fornire un **approccio omogeneo** per l'identificazione degli eventi che possono influire sull'attività della società
- Assicurare lo svolgimento delle attività **coordinando i risk specialist e gli altri attori coinvolti** nel processo

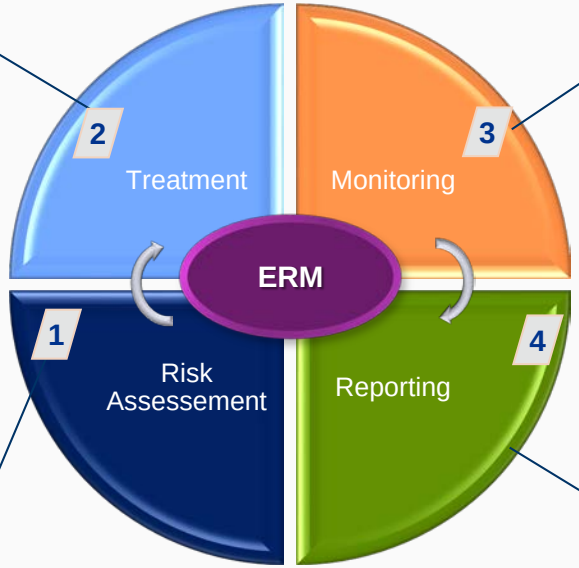
Focus: Il livello di controllo

Enterprise Risk Management - Processo

Processo

Definizione delle strategie di trattamento del rischio più opportune

Monitoraggio periodico sul livello di esposizione al rischio e sullo stato di implementazione delle azioni di trattamento

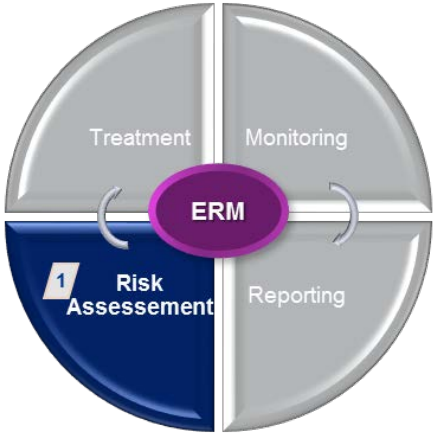


Identificazione e valutazione dei principali eventi che potrebbero influire sul conseguimento degli obiettivi aziendali

Rappresentazione ai vertici aziendali e al CdA delle informazioni relative alle attività di Risk Assessment & Treatment nonché di monitoraggio dei principali rischi

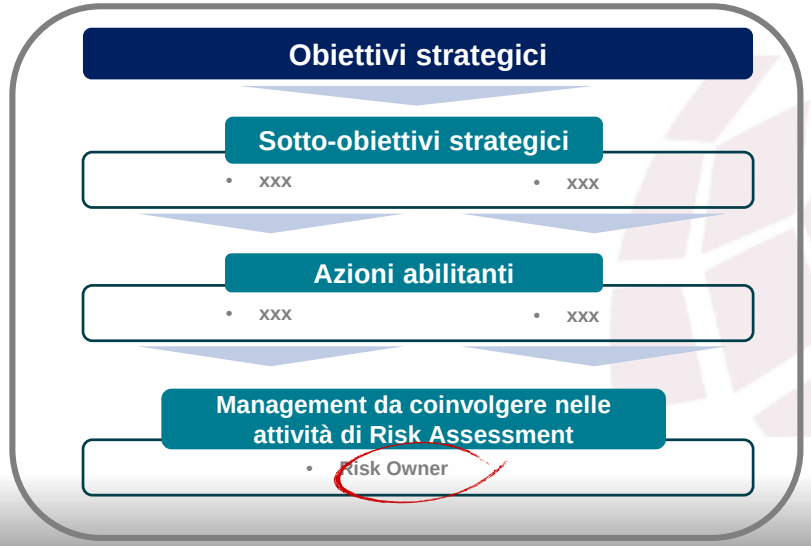
Focus: Il livello di controllo

Enterprise Risk Management - Processo: Risk Assessment (1/6)



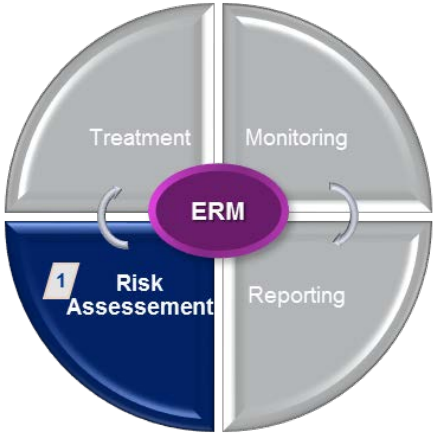
La fase di *Risk Assessment* prevede le attività di **definizione dell'ambito di Risk Assessment**: individuazione delle aree organizzative / società controllate che **contribuiscono in termini rilevanti al raggiungimento degli obiettivi previsti dal Piano Strategico aziendale** e/o **esposte potenzialmente a rischi specifici**. Tale attività permette l'individuazione del management da coinvolgere nelle attività di risk assessment (risk owner) e la definizione di un **Piano delle attività**, che include tempi e scadenze di reporting.

- Esemplificativo -



Focus: Il livello di controllo

Enterprise Risk Management - Processo: Risk Assessment (2/6)



identificazione dei rischi: attività di responsabilità del Risk Owner svolta con il supporto del Risk Management e **finalizzata all'identificazione, classificazione e descrizione** (in termini di cause e conseguenze) **dei principali eventi che potrebbero minacciare il raggiungimento degli obiettivi aziendali**. I rischi sono identificati e classificati sulla base di un modello di categorizzazione, strutturato in categorie e sotto-categorie di rischio (c.d. **Risk Model**). Il Risk Model è finalizzato a:

- supportare l'attività di identificazione dei rischi;
- garantire l'omogeneità del linguaggio;
- ottenere una visione di sintesi del portafoglio rischi.

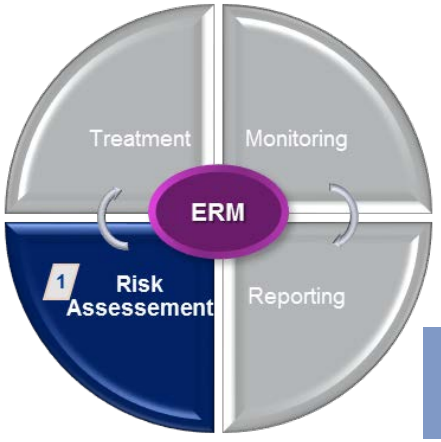
- Esemplificativo -

I Livello – Categoria di rischio

II Livello - Sotto-categoria

Focus: Il livello di controllo

Enterprise Risk Management - Processo: Risk Assessment (3/6)



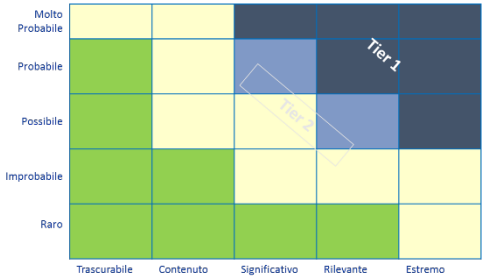
valutazione e analisi dei rischi: attività di responsabilità del Risk Owner svolta con il supporto del Risk Management e finalizzata a valutare l'entità dei rischi sulla base di:

i) **scala di probabilità**;

Cluster	Valutazione	Probabilità di accadimento (logica or)	Quantitativo
1	Raro	• L'evento di rischio non si è verificato negli ultimi 2 anni • Si prevede che l'evento non si verificherà nei prossimi 2 anni • L'evento di rischio si verifica soltanto in circostanze eccezionali (meno del 1% dei casi)	
2	Improbabile	• L'evento di rischio si è verificato a meno una volta negli ultimi 2 anni • Si prevede che l'evento di rischio si verificherà a meno una volta nei prossimi 2 anni • L'evento di rischio è improbabile che si verifichi (tra 1% e 5% dei casi)	
3	Moderato	• L'evento di rischio si è verificato a meno una volta nell'ultimo anno/più volte negli ultimi 3 anni • Si prevede che l'evento di rischio si verificherà a meno una volta nel prossimo anno/più volte nei prossimi 3 anni • L'evento di rischio può verificarsi in un certo numero di casi (tra il 5% e il 20%)	
4	Possibile	• L'evento di rischio si è verificato più volte nell'ultimo anno • Si prevede che l'evento di rischio si verificherà più volte nel prossimo anno • L'evento di rischio si verifica in una frazione certa dei casi (tra il 20% e il 50% dei casi)	
5	Probabile	• L'evento di rischio si è verificato molto frequentemente nell'ultimo anno • Si prevede che l'evento di rischio si verificherà molto frequentemente nel prossimo anno • L'evento di rischio si verifica nella maggior parte dei casi (più del 50% dei casi)	

ii) **scala di impatto**, strutturata sulla base di driver quantitativi (es- economico-finanziario;) e qualitativi (es. HSE, Immagine e Reputazione).

- Esemplificativo -



		CATEGORIE				
		Trascurabile	Contenuto	Significativo	Rilevante	Estremo
Driver	Descrittivo / Qualitativo	Impatto sugli obiettivi aziendali e sulla gestione, può essere assorbito attraverso la normale attività	Impatto sugli obiettivi aziendali e sulla gestione, può essere assorbito mediante un intervento del management per minimizzarlo	L'impatto sugli obiettivi aziendali e sulla gestione richiede un controllo gerarchico del management di dipartimento	L'impatto sugli obiettivi aziendali e sulla gestione richiede una pianificazione mirata mediante piano strategico	L'impatto sugli obiettivi aziendali e sulla gestione comporta una significativa revisione della strategia
	Economico (EBITDA)	< 0,1% (*1 mln)	< 1% (*10 mln)	< ..% (*.. mln)	< ..%(*.. mln)	> 10% (*.. mln)
	Immagine e reputazione	Impatto trascurabile Preoccupazione dell'opinione pubblica a livello locale Attenzione negativa sui media locali e potenziale base all'evento negativo sui media nazionali Attenzione politica a livelli locale con possibili reazioni di opposizione parte di parte politica e/o dirigenti di azione	Impatto Contenuto e temporaneo Preoccupazione dell'opinione pubblica a livello locale e limitata preoccupazione a livello nazionale Attenzione negativa sui media locali e nazionali con limitata attenzione negativa sui media internazionali Attenzione politica a livelli locale e nazionale con possibile presa di posizione da parte di un gruppo politico/sindacale o di azione	Impatto significativo temporaneo Significativa, ma temporanea, preoccupazione dell'opinione pubblica a livelli nazionale e/o limitata preoccupazione a livello internazionale Significativa, ma temporanea, attenzione negativa sui media nazionale e limitata internazionali Attenzione politica a livello nazionale con potenziale impatto sulla reputazione della parte di parte politica e/o dirigenti di azione	Impatto rilevante prolungato Rilevante e prolungata preoccupazione dell'opinione pubblica a livello nazionale e internazionale Rilevante e prolungata attenzione negativa sui media nazionali e internazionali Azione sui politici nazionali e regionali con potenziale impatto sulla reputazione della parte politica (opposizione, convocazione, normative, dichiarazioni, Modalità azione di gruppi di azione)	Interessamento dell'immagine e della reputazione nel lungo periodo Interesse e diffusa preoccupazione dell'opinione pubblica internazionale che danni all'immagine e alla reputazione nel lungo periodo Diffusa e sostanziale attenzione negativa sui media internazionali Azione politica a livelli nazionali e regionali con potenziale impatto sulla reputazione della parte di parte di maggioranza e internazionali Preoccupazione sulla sopravvivenza opportunità future di business - livello internazionale
	Salute e Sicurezza e Ambiente	Salute e Sicurezza: Effetti irrevocabili sulla salute L'incidente – 3 giorni di calendario di assenza dal lavoro (prima prognosi) Ambiente: Limitato disagio per il personale/popolazione (rumori / inquinamento luminoso) Non impone interventi sostanziali e l'impegno economico è trascurabile	Salute e Sicurezza: Disabilità parziale permanente (?) ferite L'incidente – 3 giorni di calendario di assenza dal lavoro (prima prognosi) Ambiente: Disagio per il personale/ popolazione (odori/rumori/ inquinamento luminoso con segnalazione da parte di singoli soggetti di disagio provenienti da interessi/valori) Contenuto ma con un'azione di coordinamento dalla risposta con impegno limitato in termini di risorse e di budget (~ 2 settimane)	Salute e Sicurezza: Disabilità permanente totale o infortuni/mortalità singoli; Malattia professionale singola Ambiente: Disagio per il personale/ popolazione (odori/rumori/ inquinamento luminoso con segnalazione da parte di singoli soggetti di disagio provenienti da interessi/valori) Comportano interventi sostanziali, con impegno di risorse significativo sul caso del danno (operazioni e di durata (> 1 mese) per il ripristino delle condizioni quo ante.	Salute e Sicurezza: Infortuni mortali multipli Malattia professionale singola Ambiente: Disagio per il personale/ popolazione (odori/rumori/ inquinamento luminoso con segnalazione da parte di singoli soggetti di disagio provenienti da interessi/valori/ industria) Impone un intervento immediato e multidisciplinare e psicologici (> 6 mesi) con un impegno economico significativo	Salute e Sicurezza: Incidente con impatto sull'incolumità pubblica Gravi emergenze mediatiche/ Interessi di più gruppi/ azione nella stessa ambito di lavoro/ o per la varietà ipotizzabili attività Ambiente: Disagio complessivo per il territorio interessato Comporta un'azione di risoluzione coordinata tra le autorità nazionali/ internazionali (P.C. VVFF, ASL etc.) e un intervento di emergenza/ecologico (> 1 anno) con un impegno economico significativo e/o impatto sanitario sulla collettività
	Security	Trascurabile danno alla persona e/o lieve impatto sugli asset tangibili e/o intangibili	Lieve danno alla persona e/o moderato impatto sugli asset tangibili e/o intangibili	Rilevante danno alla persona e/o elevato impatto sugli asset tangibili e/o intangibili	Grave danno alla persona e/o grave impatto sugli asset tangibili e/o intangibili	Gravissimo danno alla persona e/o perdite di vite umane e/o gravissimo impatto sugli asset tangibili e/o intangibili

In base alla combinazione del livello di probabilità e di impatto si determina il **livello di rischio o "risk severity"** e il conseguente posizionamento nella matrice probabilità/impatto.

Per i rischi più rilevanti è possibile svolgere degli approfondimenti (business case) al fine di fornire, ove possibile, una quantificazione del rischio in termini economico-finanziari.

Focus: Il livello di controllo

Enterprise Risk Management - Processo: Risk Assessment (4/6)

- Esemplificativo -

Cluster	Valutazione	Probabilità di accadimento (logica or)
1	Raro	▪ L'evento di rischio non si è verificato negli ultimi 3 anni ▪ Si prevede che l'evento non si verificherà nei prossimi 3 anni ▪ L'evento di rischio si verifica soltanto in circostanze eccezionali (meno dell'1% dei casi)
2	Improbabile	▪ L'evento di rischio si è verificato almeno una volta negli ultimi 3 anni ▪ Si prevede che l'evento di rischio si verificherà almeno una volta nei prossimi 3 anni ▪ L'evento di rischio è improbabile che si verifichi (tra l'1% e il 5% dei casi)
3	Possibile	▪ L'evento di rischio si è verificato almeno una volta nell'ultimo anno/più volte negli ultimi 3 anni ▪ Si prevede che l'evento di rischio si verificherà almeno una volta nel prossimo anno/più volte nei prossimi 3 anni ▪ L'evento di rischio può verificarsi in un certo numero di casi (tra il 5% e il 20%)
4	Probabile	▪ L'evento di rischio si è verificato più volte nell'ultimo anno ▪ Si prevede che l'evento di rischio si verificherà più volte nel prossimo anno ▪ L'evento di rischio si verifica in una buona parte dei casi (tra il 20% e il 50% dei casi)
5	Molto Probabile	▪ L'evento di rischio si è verificato molto frequentemente nell'ultimo anno ▪ Si prevede che l'evento di rischio si verificherà molto frequentemente nel prossimo anno ▪ L'evento di rischio si verifica nella maggior parte dei casi (più del 50% dei casi)

Focus: Il livello di controllo

Enterprise Risk Management - Processo: Risk Assessment (5/6)

- Esemplificativo -

		CATEGORIE				
		Trascurabile	Contenuto	Significativo	Rilevante	Estremo
Driver	Descrittivo / Qualitativo	Impatto sugli obiettivi aziendali e sulla gestione, può essere assorbito attraverso la normale attività	Impatto sugli obiettivi aziendali e sulla gestione, può essere assorbito ma è richiesto uno sforzo del management per minimizzarlo	L'impatto sugli obiettivi aziendali e sulla gestione richiede un coinvolgimento del management fuori dall'ordinario	L'impatto sugli obiettivi aziendali e sulla gestione comporta una contenuta e mirata revisione delle strategie	L'impatto sugli obiettivi aziendali e sulla gestione comporta una significativa ed estesa revisione delle strategie
	Economico (EBITDA)	< 0,1% (~1 mln)	< 1 % (~10 mln)	< ..% (~.. mln)	< ..% (~.. mld)	> 16% (~.. mld)
	Immagine e reputazione	**Impatto trascurabile** Preoccupazione dell'opinione pubblica a livello locale Attenzione negativa sui media locali e potenziale lieve attenzione negativa sui media nazionali Attenzione politica a livello locale con possibile presa di posizione da parte di cariche politiche e/o di gruppi di azione	**Impatto Contenuto e Temporaneo** Preoccupazione dell'opinione pubblica a livello locale e limitata preoccupazione a livello nazionale Attenzione negativa sui media locali e nazionali e/o limitata attenzione negativa sui media internazionali Attenzione politica a livello locale e nazionale con possibile presa di posizione da parte di cariche politiche e/o di gruppi di azione	**Impatto significativo ma temporaneo** Significativa, ma temporanea, preoccupazione dell'opinione pubblica a livello nazionale e/o limitata preoccupazione a livello internazionale Significativa, ma temporanea, attenzione negativa sui media nazionali e internazionali Attenzione politica a livello nazionale e internazionale con possibile presa di posizione da parte di cariche politiche e/o di gruppi di azione	**Impatto rilevante e prolungato** Rilevante e prolungata preoccupazione dell'opinione pubblica a livello nazionale e internazionale Rilevante e prolungata attenzione negativa sui media nazionali e internazionali Adozione di politiche nazionali e regionali con potenziale impatto e/o restrizioni sulla Società (operatività, accesso a nuove aree, concessioni, normative , sanzioni). Mobilitazione di gruppi di azione	**Deterioramento dell'immagine e della reputazione nel lungo periodo** Estrema e duratura preoccupazione dell'opinione pubblica internazionale con danni all'immagine e alla reputazione nel lungo periodo Duratura rappresentazione negativa della Società da parte dei media internazionali Perdita potenziale di significative opportunità future di business a livello internazionale
	Salute e Sicurezza e Ambiente	**Salute e Sicurezza:** Effetti reversibili sulla salute LTI singolo con < 30 giorni di calendario di assenza dal lavoro (prima prognosi) **Ambiente:** Limitato disagio per il personale/popolazione (odori/ rumori / inquinamento luminoso) Non impone interventi sostanziali e l'impegno economico è trascurabile	**Salute e Sicurezza:** Disabilità parziale permanente LTI plurimo LTI singolo con ≥30 giorni di calendario di assenza dal lavoro (prima prognosi) **Ambiente:** Disagio per il personale/ popolazione (odori/rumori/ inquinamento luminoso con segnalazioni da parte di singoli soggetti di disagio provenienti da interno/esterno) L'evento impone un' azione di coordinamento della risposta con impegno limitato in termini di risorse e di durata(< 2 settimane)	**Salute e Sicurezza:** Disabilità permanente totale o infortunio mortale singolo. Malattia professionale singola **Ambiente:** Disagio per il personale/ popolazione (odori/rumori/ inquinamento luminoso con segnalazioni ripetute di disagio provenienti da interno/esterno/ Autorità) Comporta un intervento coordinato, con impegno di risorse significativo sui costi del sito/unità operativa e di durata (< 1 mese) per il ripristino delle condizioni quo ante.	**Salute e Sicurezza:** Infortuni mortali multipli Malattia professionale di più persone nello stesso ambiente di lavoro e/o per la stessa tipologia di attività **Ambiente:** Disagio per il personale/ popolazione (odori/rumori/ inquinamento luminoso con segnalazioni prolungate e ripetute nel tempo di disagio provenienti da interno/esterno/ Autorità) Impone un intervento massivo e multidisciplinare e prolungato (< 6 mesi) con un impegno economico significativo	**Salute e Sicurezza:** Incidente con impatto sull'incolumità pubblica Gravi e ripetute malattie professionali di più persone nello stesso ambiente di lavoro e/o per la stessa tipologia di attività **Ambiente:** Disagio complessivo per il territorio investito Comporta un'azione di risposta in coordinamento tra le autorità nazionali/internazionali (P.C., VVFF, ASL, etc..) e un intervento di considerevole durata (> 1 anno) con impegno economico significativo che impattano anche sui costi
	Security	Trascurabili danni alle persone e/o lieve impatto sugli asset tangibili e/o intangibili	Lievi danni alle persone e/o moderato impatto sugli asset tangibili e/o intangibili	Rilevanti danni alle persone e/o elevato impatto sugli asset tangibili e/o intangibili	Gravi danni alle persone e/o grave impatto sugli asset tangibili e/o intangibili	Gravissimi danni alle persone e/o perdite di vite umane e/o gravissimo impatto sugli asset tangibili e/o intangibili

Focus: Il livello di controllo

Enterprise Risk Management - Processo: Risk Assessment (6/6)

Nella matrice è riportato il numero dei rischi distribuito in base alla valutazione di rischio residuo *(tenendo in considerazione le azioni di trattamento in essere)*

	Trascurabile	Contenuto	Significativo	Rilevante	Estremo
Molto Probabile	0	2	6	3	2
Probabile	1	6	11	2	-
Possibile	4	21	22	7	-
Improbabile	7	16	5	10	-
Raro	8	6	1	5	-

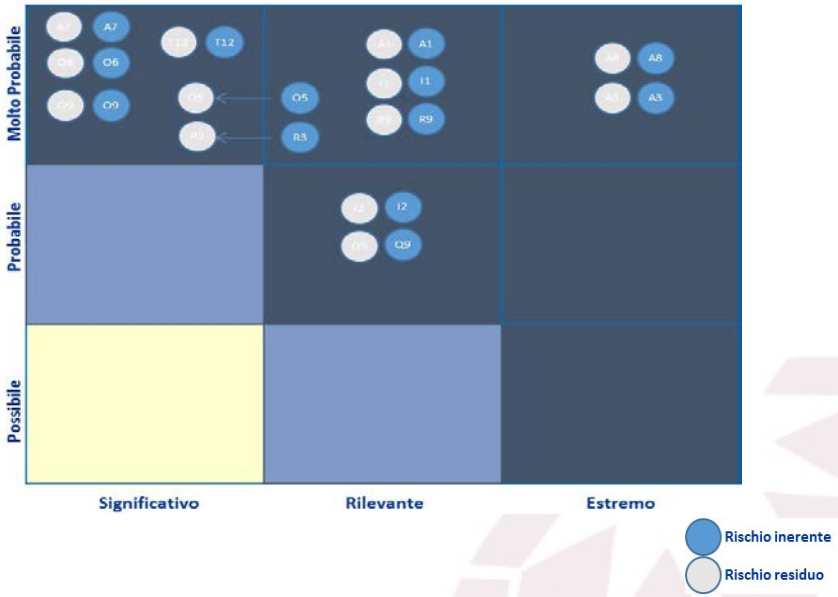
Tier 1
Tier 2
Esemplificativo

Aree di rilevanza

TIER 1:
Rischi che eccedono le soglie di accettabilità del rischio e che richiedono un'attività di gestione e monitoraggio proattiva e costante a tutti i livelli

TIER 2:
Rischi che sono in linea con le soglie di accettabilità del rischio e che richiedono un'attività di gestione e monitoraggio ad hoc

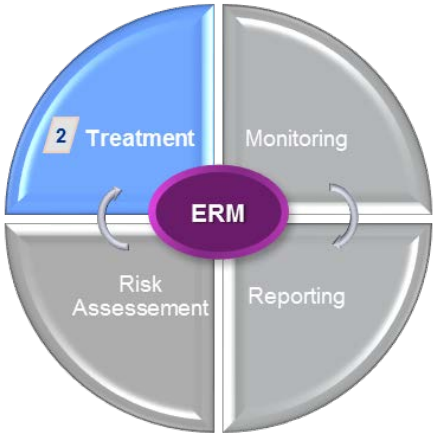
Focus Tier 1



#	Top Risks (Tier 1)
A-3	Sviluppo dei sistemi IT non in grado di adattarsi alle esigenze di business
A-1	Valutazioni non accurate nell'ambito di acquisizioni e dismissioni di asset
I-1	Climate change
R-9	Attacchi terroristici
O-5	Fuoriuscita di informazioni confidenziali
O-6	Customer Satisfaction
O-9	Comunicazione interna non coerente rispetto alla strategia aziendale
O-9	Competizione
I-2	Aumento dei contenziosi legali a seguito di partecipazione a gare d'appalto
T-9	Incidenti
..	……

Focus: Il livello di controllo

Enterprise Risk Management - Processo: Treatment

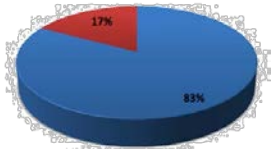


Nella fase di *Treatment* il Risk Owner identifica:

- le **azioni di trattamento in essere**, per ridurre il livello di rischio ad un livello considerato accettabile o per tradurlo in opportunità;
- sulla base della strategia di trattamento più adeguata (evitare, accettare, ridurre o condividere il rischio) e delle proposte del Risk Management, eventuali **ulteriori azioni di trattamento** da implementare, rispetto alla quali definisce il **piano d'azione** in cui sono descritte le modalità attuative della strategia di trattamento, inclusi i tempi e le responsabilità di implementazione.

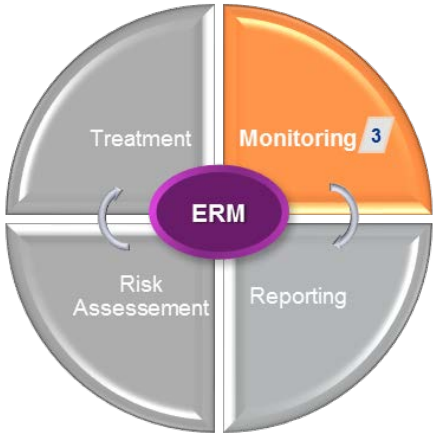
- Esemplificativo -

Treatment

Azione di trattamento	Responsabile	Data di completamento	% di completamento
• xxx	• xxx	• xxx	• xxx 

Focus: Il livello di controllo

Enterprise Risk Management - Processo: Monitoring



La fase di *Monitoring,* prevede un monitoraggio continuo da parte del Risk Management Integrato su: i) l'andamento dei rischi; ii) lo stato d'implementazione dei Piani di trattamento; iii) l'insorgere di nuovi rischi.

Tale monitoraggio presuppone la definizione e implementazione di indicatori chiave finalizzati al monitoraggio di:

- Performance (**Key Performance Indicator - KPI**);
- Rischi (**Key Risk Indicator - KRI**);
- Controlli (**Key Control Indicator - KCI**).

- Esemplificativo -

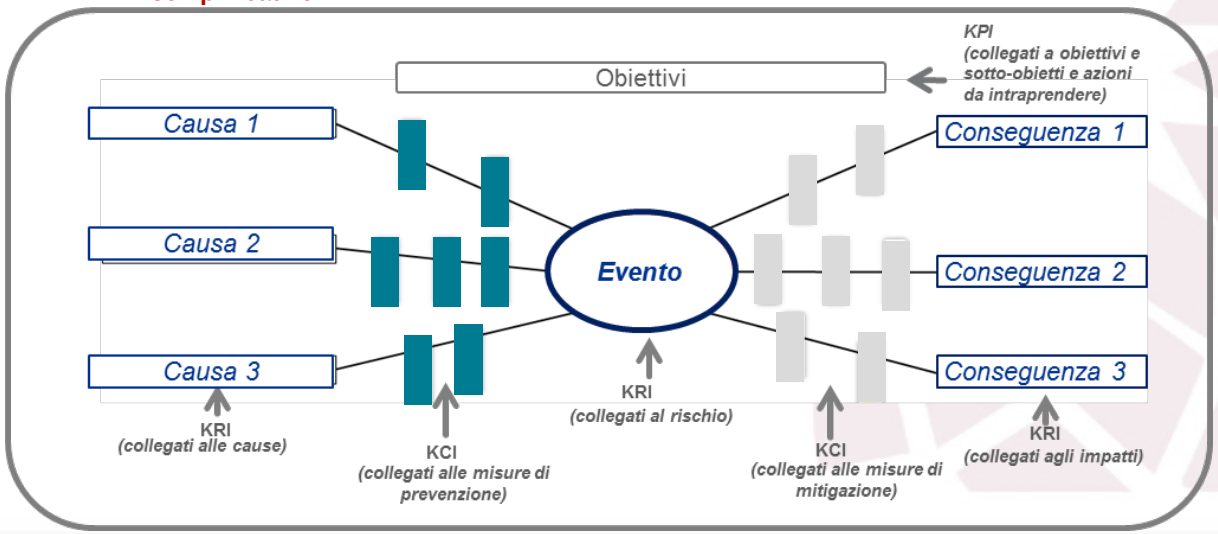
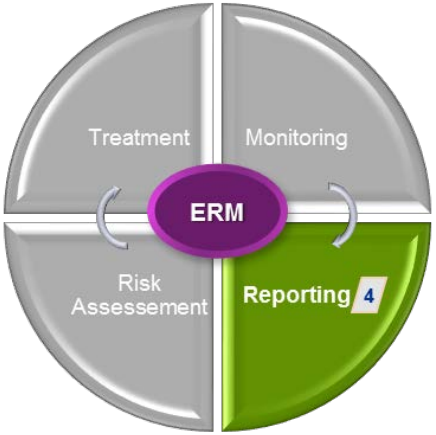


Diagramma cause-effetto ISO 31000

KRI: Key Risk Indicator
KCI: Key Control Indicator
KPI: Key Performance Indicator

Focus: Il livello di controllo

Enterprise Risk Management - Processo: Reporting

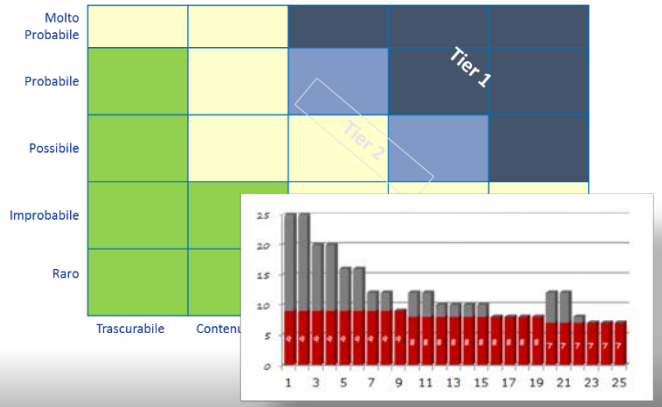


La fase di *Reporting* consente:

- ai **vertici aziendali** e **agli organismi di controllo e vigilanza (Comitato Rischi/CEO/Comitato Controllo e Rischi/CdA)**, di valutare gli esiti delle attività di Risk Assessment & Treatment nonché di monitoraggio dei principali rischi;
- al **Dirigente Preposto** di redigere i documenti contabili societari, tenendo in considerazione gli esiti del processo;
- alla **funzione Internal Audit**, di definire il Piano di Audit, tenendo in considerazione anche gli esiti del processo;
- ai **diversi livelli aziendali**, di avere la disponibilità dei dati relativi alla gestione del rischio, dei risultati ottenuti e delle azioni di miglioramento programmate.

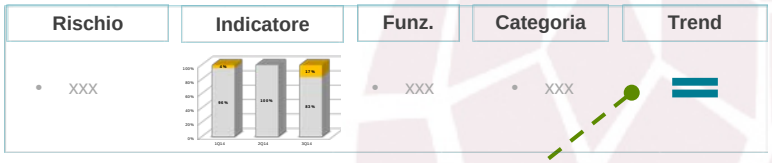
Reporting sui rischi

- Esemplificativo -



Reporting di monitoraggio

- Esemplificativo -



Indicazione dell'**andamento generale medio degli indicatori** rispetto alla precedente valutazione:

- stabile =
- in diminuzione ↓
- in aumento ↑

Focus: Il livello di controllo

Sistemi informativi di supporto al processo: Sistemi GRC

- Coerentemente con la dimensione, complessità, profilo di rischio specifico e contesto regolamentare della società, la gestione del processo e dei flussi di reporting è supportata dall'implementazione di adeguati **sistemi informativi cosiddetti GRC Tool (Governance Risk & Compliance).**

- Il principale beneficio dei sistemi GRC consiste nell'ottenere una **vista consolidata dei processi di Governance, Risk Management e Compliance**.
- La piattaforma applicativa GRC è un elemento importante per supportare il processo **di integrazione dei sistemi di risk management** e rendere efficiente il SCI.

Agenda

- Principali riferimenti
- Gli attori del Sistema di controllo interno e gestione dei rischi
- Focus: Linee di indirizzo SCIGR
- Focus: Risk Appetite e Risk Tolerance
- Focus: Il livello di controllo - modelli di presidio e processo integrato
- Focus: Compliance Trasformation e presidio dei rischi

Premessa (1/2)

Compliance transformation

La nuova **rivoluzione industriale**, che ha investito i mercati e l'economia reale, sta mettendo a dura prova i modelli di business delle imprese, stimolando le **autorità** nazionali e sovranazionali ad identificare e indirizzare i **rischi emergenti** con impatti rilevanti e di carattere sistemico (es. *anticorruzione, concorrenza*, *privacy,* …).

L'evoluzione della normativa, già significativamente mutata nell'ultimo decennio, e la conseguente necessità di adeguamento dei *compliance program* sono considerati dalle aziende oggi **fattori critici** di successo per la crescita.

Occorre, dunque, riconsiderare l'approccio complessivo alla *compliance*, sia da un punto di vista **giuridico**, assicurando la tenuta dei modelli a presidio delle singole norme, sia sotto il profilo **organizzativo**, attraverso la convergenza e il coordinamento delle funzioni di controllo, per condividere **le strategie di risposta ai rischi di non conformità** nel più ampio processo di *risk management*.

Appare, dunque, non più rinviabile per le imprese adottare un *compliance framework* che metta al centro lo sviluppo e la diffusione di una **cultura aziendale** improntata all'integrità e alla trasparenza, definendo chiaramente i **ruoli e le responsabilità** dei soggetti operanti sulle tre linee di difesa, e implementando efficaci ed efficienti **processi di gestione** della *compliance* in ottica *end to end*.

Premessa (2/2)

Survey *'La compliance transformation nelle imprese e i modelli di presidio dei rischi'*

Per comprendere in che modo le organizzazioni stanno rispondendo alle evoluzioni in ambito compliance, KPMG, in collaborazione con il centro di ricerca LUISS Dream, ha svolto una survey coinvolgendo le principali aziende italiane quotate e non quotate, finalizzata a rilevare lo stato dell'arte, le preoccupazioni e le strategie di gestione dei rischi di non conformità.

I risultati della Survey forniscono informazioni sul modo in cui le principali aziende italiane gestiscono gli aspetti di compliance ed evidenziano le principali best practice da implementare in coerenza con il profilo di rischio e la tolleranza al rischio delle loro organizzazioni.

Compliance Transformation e presidio dei rischi

Struttura della survey

La survey analizza i processi di trasformazione in atto nella gestione della compliance attraverso le componenti del **Compliance Program Framework sviluppato da KPMG a livello internazionale**.

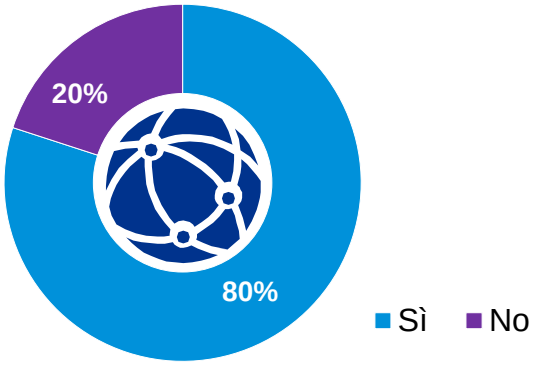
- **Governance e cultura**
- **Compliance Risk Assessment**
- **Risorse, competenze e due diligence**
- **Strumenti normativi interni**
- **Comunicazione e formazione**
- **Tecnologia e data analytics**
- **Testing e monitoraggio**
- **Gestione delle carenze e ispezioni**
- **Reporting**
- **Rapporti tra la Funzione Compliance e le altre funzioni e gli organi di controllo**

Il questionario è stato sottoposto ad un panel di società quotate e non quotate, escluse le società appartenenti al settore finanziario e assicurativo le cui attività in ambito compliance sono regolate da specifiche normative di settore. Ha previsto la compilazione di risposte multiple di tipo affermativo/negativo o di risposte multiple a 5 livelli secondo la seguente scala: pienamente d'accordo, d'accordo, neutrale, in disaccordo, fortemente in disaccordo. Ai fini della rappresentazione dei risultati, le risposte *neutrali* sono state integrate nelle percentuali con accezione negativa.

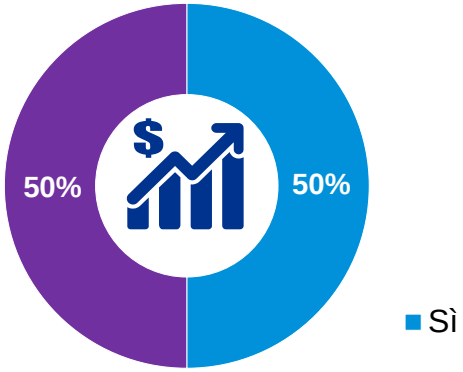
Compliance Transformation - Risultati della Survey

Profilo dei rispondenti (1/2)

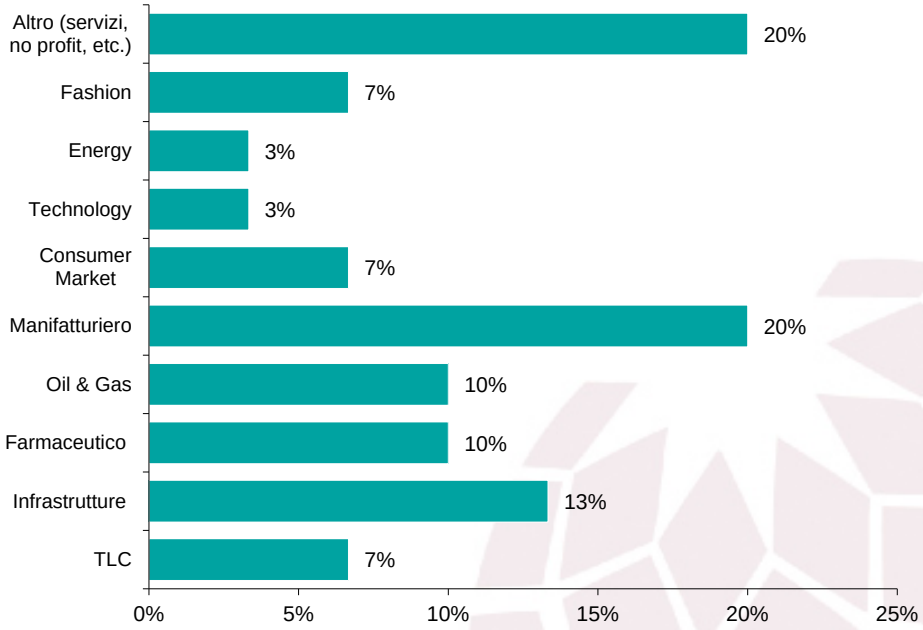
Gruppi multinazionali



Società quotate



Settore d'appartenenza



La survey ha coinvolto un panel di società (oltre 100) appartenenti a molteplici settori ad esclusione del settore finanziario e assicurativo ed è stata condotta attraverso un questionario strutturato inviato alle funzioni di controllo.

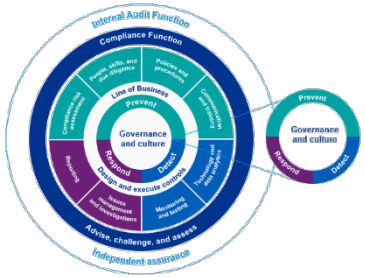
Compliance Transformation - Risultati della Survey

Profilo dei rispondenti (2/2)

Funzione di appartenenza dei rispondenti

Compliance Transformation - Risultati della Survey

Governance e cultura (1/5)



*"Governance e Cultura aziendale sono essenziali per un **compliance program efficace**. La Governance è riferita alla struttura dell'attività di compliance dell'organizzazione, mentre la Cultura della compliance è una combinazione di valori e comportamenti diffuse nell'organizzazione.* ***Sviluppare una cultura aziendale radicata nell'organizzazione, o modificarla, richiede un enorme impegno."***

I rispondenti affermano che:

Il CdA o altro comitato **esamina ed approva** annualmente compliance program **riferiti ad ambiti specifici** (**80%**)

Il CdA o altri comitati sono adeguatamente **informati** in merito all'esposizione della Società ai rischi di compliance e alle modalità di mitigazione di tali rischi (**83%**)

Il CdA ed il Vertice aziendale **sono coinvolti** nelle diverse fasi relative agli aspetti di compliance (**80%**)

Il mandato e la mission dei presidi di compliance sono **formalizzati** in documenti ufficiali (**73%**)

La Società ha inserito nella propria agenda come **priorità** la diffusione della cultura della compliance (**80%**)

Le aspettative del vertice in termini di compliance sono **recepite in documenti accessibili** a tutto il personale della Società (**73%**)

Compliance Transformation - Risultati della Survey

Governance e cultura (2/5)

I rispondenti affermano che:

Le **relazioni periodiche sul SCIGR** presentate al vertice aziendale contengono anche informazioni relative ai rischi di compliance (**93%**)

La Funzione Internal Audit svolge **audit** o altre attività di **monitoraggio indipendente** sulle modalità con cui la propria Società gestisce il rischio di compliance (**80%**), attraverso: verifiche ex D. Lgs. 231 (**79%**), testing ex L. 262/SOX (**46%**), audit su altre funzioni deputate alla gestione ed al monitoraggio dei rischi di compliance (**58%**), audit sulla Funzione Compliance. (**29%**)

I rispondenti affermano che:

La Società non ha istituito un **Compliance Committee** a livello di management (**70%**)

I presidi di compliance della Società non **partecipano attivamente** a comitati mageriali/management meeting con le funzioni operative (**40%**)

La Società non ha adottato degli **approcci** e implementato dei **tool** utilizzati dal vertice e dalle unità operative e finalizzati a rinforzare la diffusione della cultura della compliance (**33%**)

Il personale non ha percezione delle implicazioni e del **vantaggio competitivo** derivante da una forte cultura della compliance (**43%**)

I dipendenti non hanno un'elevata **consapevolezza** alle tematiche di compliance (**43%**)

Compliance Transformation - Risultati della Survey

Governance e cultura (3/5)

I rispondenti affermano che:

Il personale non ha contezza delle **aspettative/ obiettivi di compliance** della Società (**33%**)

Non esistono **incentivi e protocolli disciplinari** per la promozione del livello di cultura desiderato (**63%**). Nei casi in cui sono previsti incentivi, il **78%** dei rispondenti, afferma che gli incentivi **non danno la percezione** che la compliance avrà un impatto significativo per la loro carriera e retribuzione

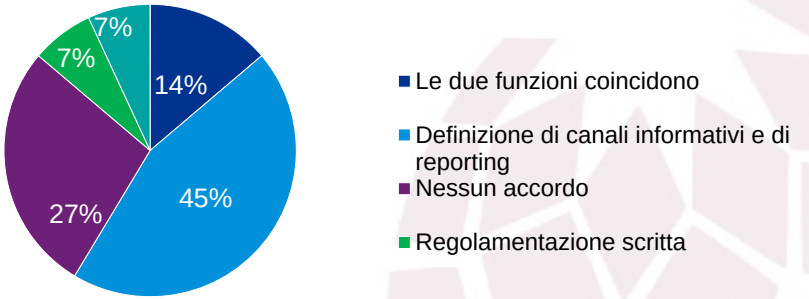
Non esistono **iniziative specifiche** finalizzate al **rafforzamento** della cultura della compliance nelle attività operative (**33%**)

Il **perimetro** delle attività e le modalità di **coordinamento** della Funzione Compliance e della Funzione Internal Audit non sono formalizzati in documenti ufficiali (**47%**)

Non esistono **flussi informativi** tra la Funzione Compliance e la Funzione Risk Management (**47%**)

Gli **esiti delle attività** svolte dalla Funzione Compliance non sono condivisi con la Funzione Risk Management e viceversa (**47%**)

Relazione tra la Funzione Compliance e la Funzione Internal Audit

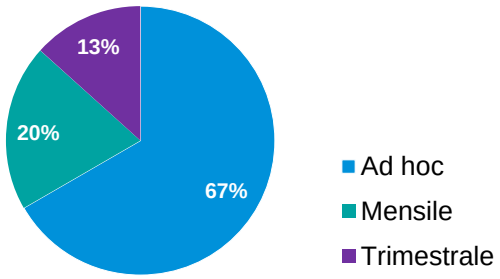


La cultura **non dovrebbe essere imposta**. I leader dovrebbero essere **modelli di riferimento** e la cultura dovrebbe essere **trasmessa a tutti i livelli** dell'organizzazione. Ogni individuo è un **"veicolo culturale"** e l'organizzazione è chiamata a rafforzare la propria cultura nelle attività operative. Inoltre, è necessario che **obiettivi**, **processi** e **azioni** dell'organizzazione siano **in linea** con i valori, l'etica e la propensione al rischio e le politiche dell'organizzazione.

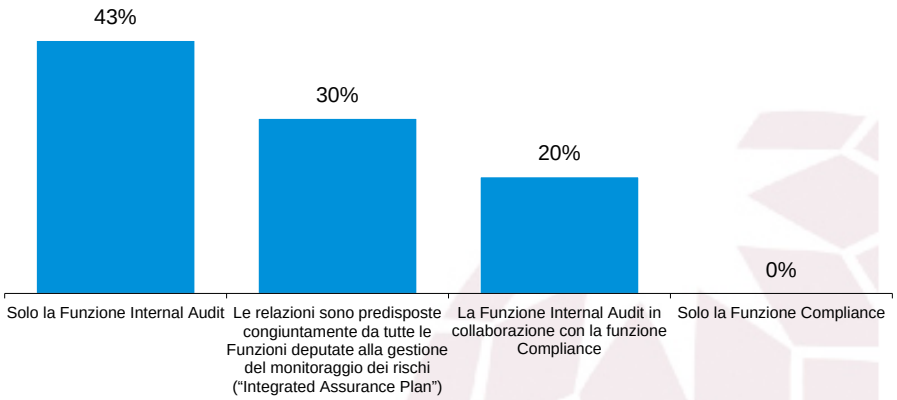
Compliance Transformation - Risultati della Survey

Governance e cultura (4/5)

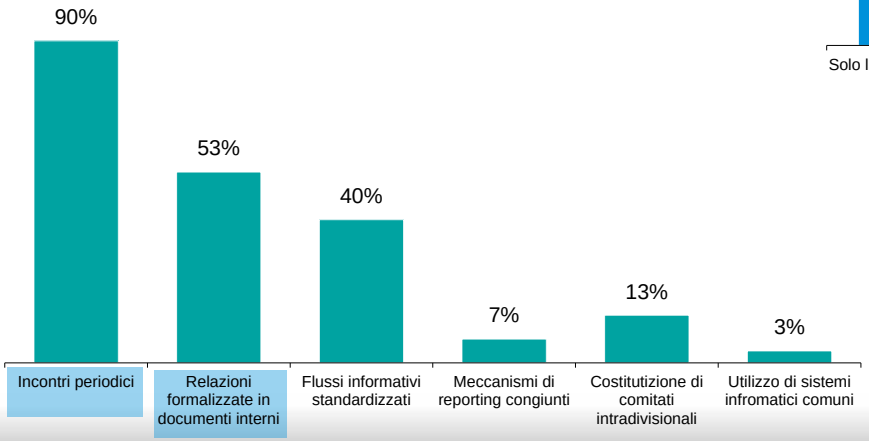
Frequenza di interazione tra Funzione Compliance e Funzione IA



Responsabile della predisposizione Relazione sul SCIGR

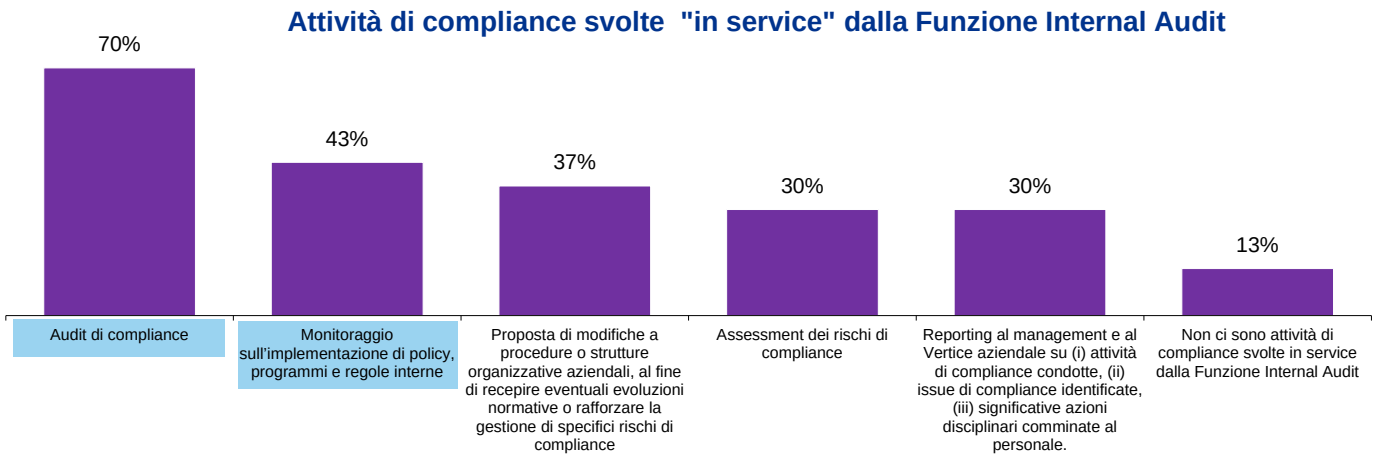


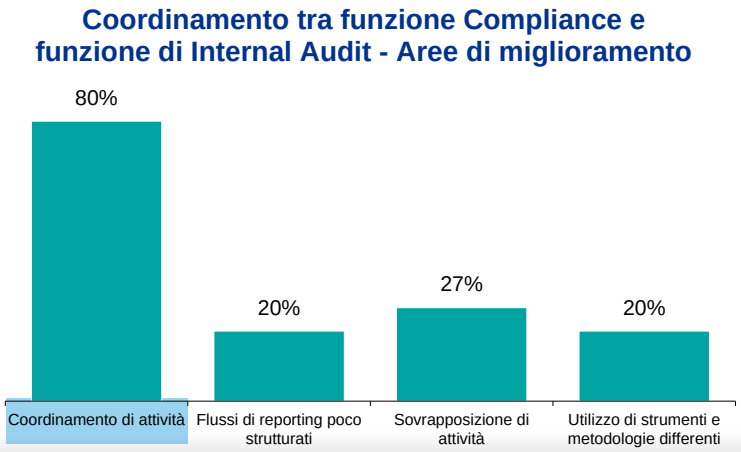
Meccanismi di coordinamento tra le funzioni di gestione e monitoraggio dei rischi



Compliance Transformation - Risultati della Survey

Governance e cultura (5/5)

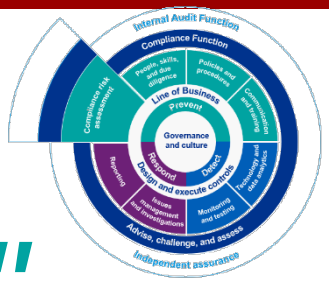




Compliance Transformation - Risultati della Survey:

Compliance Risk Assessment

*"Le organizzazioni dovrebbero **verificare periodicamente il proprio rischio di non conformità** ed implementare/adeguare il proprio compliance program al fine di **ridurre i rischi** potenziali identificati. La maggior parte delle Società coinvolte nella survey riconosce l'importanza di effettuare un compliance risk assessment mentre emerge che gli standard fissati per le valutazioni dei rischi o il livello di misurazione degli stessi risultano variabili tra le Società."*



I rispondenti affermano che:

I presidi di compliance **identificano, valutano e misurano i rischi inerenti** ed i **rischi residui** di compliance (**70%**)
Una % maggiore di rispondenti afferma (**87%**) di valutare solo se i controlli sono **adeguatamente disegnati** e se tali controlli **mitigano efficacemente** i rischi di compliance identificati

Le funzioni operative **partecipano** alla valutazione del rischio di compliance per gli ambiti di competenza (**87%**)

I rispondenti affermano che:

La Società non ha effettuato e formalizzato un **inventario delle normative applicabili** (**53%**)

Il compliance risk assessment non si basa su valutazioni **quali-quantitative** (**33%**)

Un processo di compliance risk assessment strutturato di norma include attività di definizione e implementazione di **metodologie** per la valutazione dei **rischi al livello inerente** e **residuo** e dell'adeguatezza del **sistema di controllo interno**, nonché prevede il **coinvolgimento anche del primo livello di controllo** nel processo di individuazione e aggiornamento **tempestivo** del **profilo di rischio** sulla base di evoluzioni normative e/o cambiamenti di business. La valutazione dei rischi di compliance dovrebbe confluire - in un'ottica di analisi integrata dei rischi – nel più ampio processo di risk management.

Compliance Transformation - Risultati della Survey

Risorse, competenze e due diligence

*"All'interno del compliance program, **è fondamentale prestare particolare attenzione alle risorse umane e alle loro competenze** e diffondere i **principi di responsabilità** rispetto agli obiettivi di compliance. Tali elementi sono egualmente importanti sia con riferimento alle risorse **interne** che a quelle **esterne**."*

I rispondenti affermano che:

I ruoli e le responsabilità in ambito di compliance sono definiti all'interno di **documenti organizzativi** per la prima e la seconda linea di controllo (**73%**)

La Funzione Compliance è coinvolta nelle attività relative alla **due diligence** (sulle risorse **interne** ed **esterne**) per gli aspetti di propria competenza (**73%**)

Le violazioni in ambito compliance **sono gestite in modo tempestivo** e sono applicate **sanzioni** (**77%**)

I rispondenti affermano che:

La Società non svolge **due diligence** sul **personale e sui fornitori** (**33%**)

La Funzione Compliance non è coinvolta nelle analisi per le **operazioni straordinarie** per gli aspetti di propria competenza (**53%**)

La valutazione delle **performance** non è legata al **comportamento** dei dipendenti in linea con la **cultura** aziendale e ai **valori** dell'organizzazione (**60%**)

Gli obiettivi di compliance non rientrano tra **gli obiettivi** definiti per il management (**50%**)

Le organizzazioni dovrebbero definire **incentivi,** finanziari e non, al fine di assicurarsi che il personale non commetta **violazioni** e adotti **comportamenti etici**. Tali incentivi dovrebbero **premiare soggetti che supportano i valori e la cultura** dell'organizzazione e dare la percezione che la compliance avrà un impatto significativo sulla loro **carriera e remunerazione**.

Compliance Transformation - Risultati della Survey

Strumenti normativi interni

*"Le policy e procedure aziendali sono ulteriori componenti del compliance program e rappresentano degli utili **controlli preventivi** per ridurre la probabilità di comportamenti scorretti. Le policy e procedure aziendali non dovrebbero essere concepite come documenti **"statici" e riferiti a specifiche normative.** Dovrebbero pertanto **integrare** tutti i requisiti normativi applicabili ai processi aziendali, essere **aggiornati nel tempo** e **mantenuti** a supporto di un efficace programma di compliance."*

I rispondenti affermano che:

- Le tematiche di compliance sono disciplinate nelle **policy e procedure** aziendali (**87%**)
- Le policy e procedure in ambito compliance sono allineate alla **mission** e ai **valori** della Società (**90%**)
- Le tematiche di compliance sono **incluse nel codice etico** e sono **accessibili** a tutto il personale (**93%**)

I rispondenti affermano che:

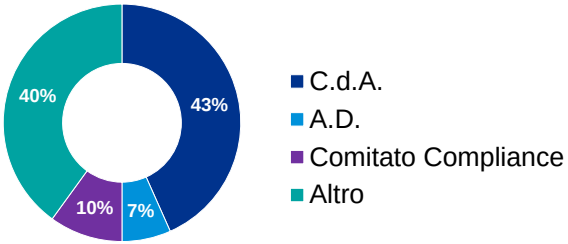
- La Società non ha adottato un **Compliance program integrato** con riferimento alla totalità degli ambiti di compliance (**63%**)
- La Società non ha una funzione incaricata dell'**aggiornamento di policy e procedure** aziendali sui temi di compliance (**37%**)

Strumenti normativi interni che regolano le tematiche di compliance e **presidi dedicati** al monitoraggio delle evoluzioni normative determinano benefici quali la **mitigazione dei rischi di compliance**, la **coerenza** nello svolgimento delle attività di compliance in tutta l'organizzazione e la **diffusione della cultura** della compliance.

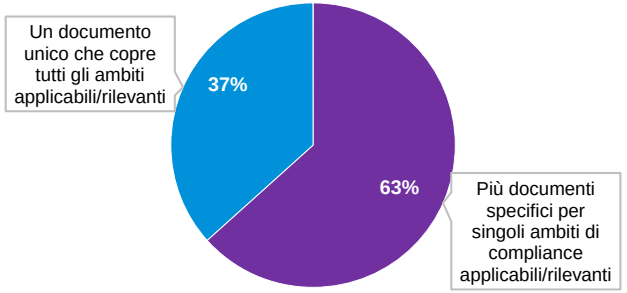
Compliance Transformation - Risultati della Survey

Strumenti normativi interni - Il compliance program

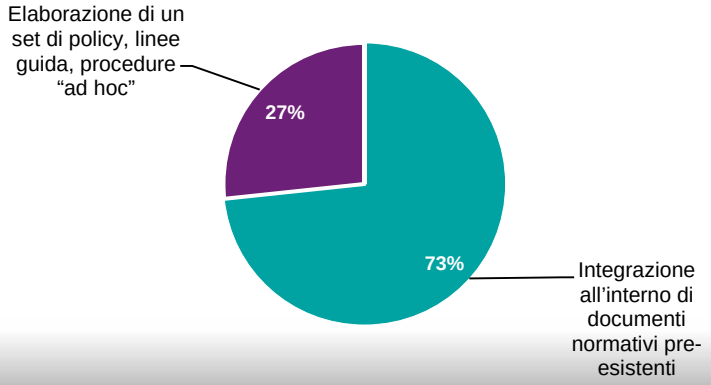
Organo destinatario del Compliance Program Integrato



Approccio utilizzato per la formalizzazione del Compliance program Integrato



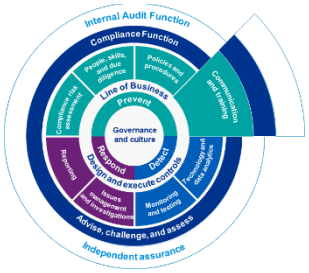
Modalità di recepimento delle evoluzioni normative



Compliance Transformation - Risultati della Survey

Comunicazione e formazione (1/2)

*"La comunicazione interna e il training del personale sono **aspetti fondamentali** per un compliance program efficace, ma il punto critico è comprendere se tali programmi di training sono **realmente** efficaci."*



I rispondenti affermano che:

Sono implementate adeguate modalità di **comunicazione** in merito a problematiche di compliance, novità e leading practice in materia di compliance, che risultano facilmente **fruibili a tutto il personale** (**70%**)

Il **programma di formazione** mira a fornire al personale una maggiore comprensione di leggi e regolamenti in vigore (**80%**)

Sono previste **iniziative formative** su specifici ambiti/modelli di compliance (**87%**). Sono inoltre erogate specifiche attività formative in ambito di compliance al vertice e ai membri degli organi aziendali (**80%**).

La formazione in materia di compliance è erogata in funzione del **ruolo** e della **responsabilità** del destinatario (**80%**).

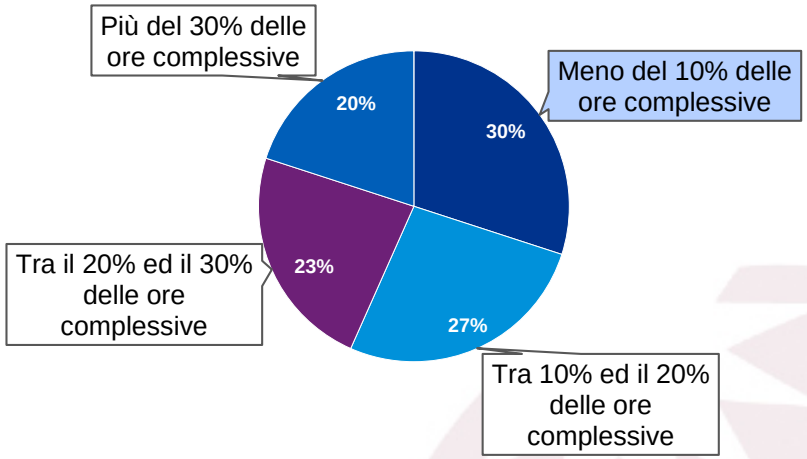
Compliance Transformation - Risultati della Survey

Comunicazione e formazione (2/2)

I rispondenti affermano che:

All'inizio del rapporto tra la propria Società e le **terze parti** non è richiesto a queste ultime di partecipare ad **iniziative di formazione su ambiti di compliance** (**57%**)

Ore di formazione sulle tematiche di Compliance

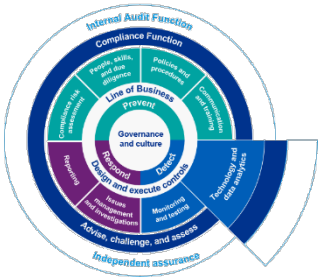


I Responsabili Compliance sono alla ricerca di modalità innovative per l'erogazione di corsi di compliance al fine di migliorare l'efficacia delle iniziative formative. A tal riguardo, le Società dovrebbero focalizzare le attività di training sulle aree **a più alto rischio**, somministrare i contenuti formativi in funzione del **ruolo ricoperto**, utilizzare **metodologie** innovative (business case), dotarsi di appositi **strumenti informatici** per monitorare i risultati dei test, includere nei corsi le **azioni correttive** identificate durante il testing.

Compliance Transformation - Risultati della Survey

Tecnologia e data analytics

*"Tecnologia e data analytics della Funzione Compliance sono **investimenti necessari** che, se adeguatamente implementati, consentiranno di ottenere un **risparmio di costi** e un **miglioramento della performance**, in quanto parte integrante della strategia e delle operazioni aziendali."*



I rispondenti affermano che:

Le attività di compliance non sono adeguatamente supportate dall'utilizzo di **strumenti informatici** (60%)

Il compliance program non si basa su **data analytics** e **strumenti informatici** per condurre analisi sui principali trend (73%)

KPI e KRI non sono integrati nel processo di **monitoraggio** e **testing** della compliance e non vengono utilizzati per le analisi di trend e per la root-cause analysis (60%)

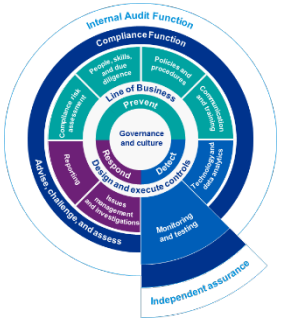
I compliance **KPI e KRI non sono integrati** nel sistema **informativo di gestione della compliance** (es. GRC - Governace, Risk and Compliance) 73%

Lo sviluppo di una solida infrastruttura tecnologica a supporto delle attività di compliance, anche attraverso data analytics, determina benefici quali la **riduzione di costi** operativi e di compliance, la **diminuzione dell'esposizione** al rischio di compliance, il **miglioramento dei processi**, l'**allocazione delle risorse** su attività rilevanti, la **maggiore reattività** nel rispondere alle richieste/ispezioni delle **Autorità**.

Compliance Transformation - Risultati della Survey:

Monitoraggio e testing (1/4)

*"L'istituzione di una **funzione centralizzata responsabile dell'attività di testing in ambito compliance** può supportare l'impresa nel **miglioramento della governance** e nel **monitoraggio** della compliance, anche attraverso un'**ottimale aggregazione dei risultati** e, conseguentemente, **un'analisi dei dati più esaustiva**."*



I rispondenti affermano che:

Sono svolti **audit di compliance** (**93%**), nel **67%** dei casi dalla Funzione Internal Audit, mentre nel **13%** dei casi dalla Funzione Compliance

I risultati delle attività di audit di compliance sono **comunicati e condivisi con il management** (**97%**) e successivamente rielaborati e comunicati **al Vertice e al CdA** (**97%**)

Gli audit di compliance sono **integrati nel Piano di Audit** presentato annualmente al Vertice aziendale (**80%**)

Gli **action plan** e le scadenze sono definiti in raccordo con il management (**93%**) e sono oggetto di monitoraggio continuo (**87%**)

Compliance Transformation - Risultati della Survey

Monitoraggio e testing (2/4)

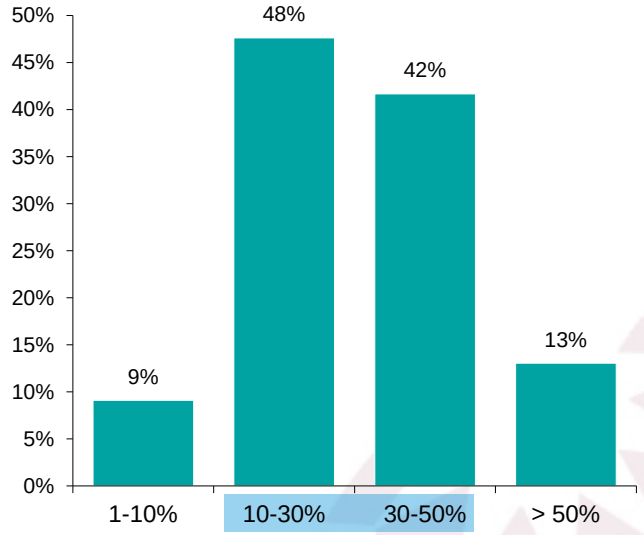
I rispondenti affermano che:

Non è stato implementato un **processo strutturato di monitoraggio** delle evoluzioni normative (**47%**)

Non vengono eseguite **periodiche valutazioni** sui contenuti del compliance program al fine di garantire l'allineamento di quest'ultimo alle evoluzioni normative nonché alle aspettative degli stakeholder (**33%**)

Non è previsto un **piano di verifica** dell'efficacia del compliance program adottato (**33%**)

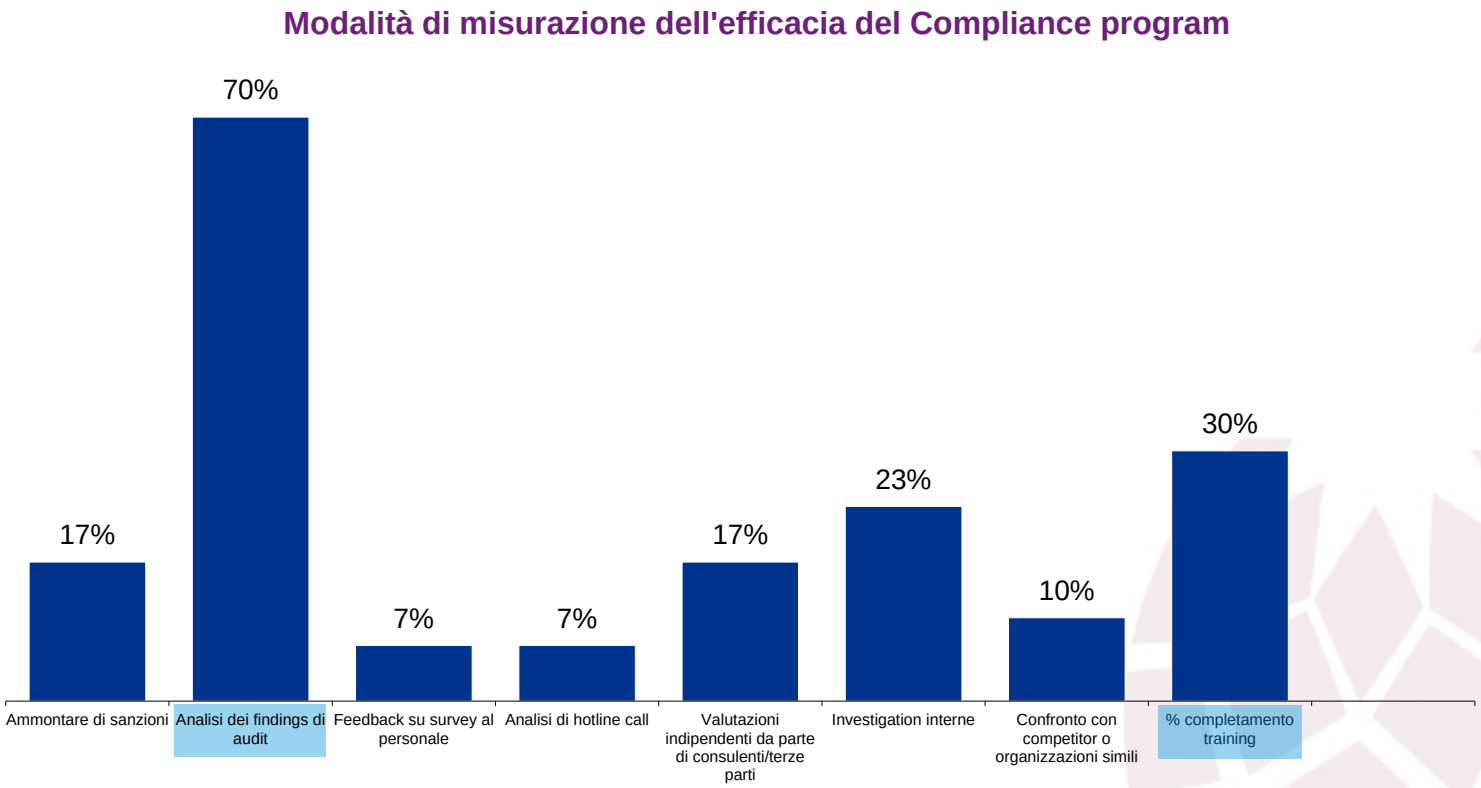
Compliance Audit - % sul totale delle attività di Audit



Per migliorare l'efficacia delle attività di monitoraggio e testing, è auspicabile che le Società definiscano chiaramente i **ruoli e responsabilità** dei tre livelli di controllo per lo svolgimento di tali attività, definiscano in modo adeguato il loro ***compliance risk universe,*** prioritizzino i principali rischi di compliance, strutturino in maniera robusta l'utilizzo dei **sistemi informatici** per mappare e consolidare le principali informazioni.

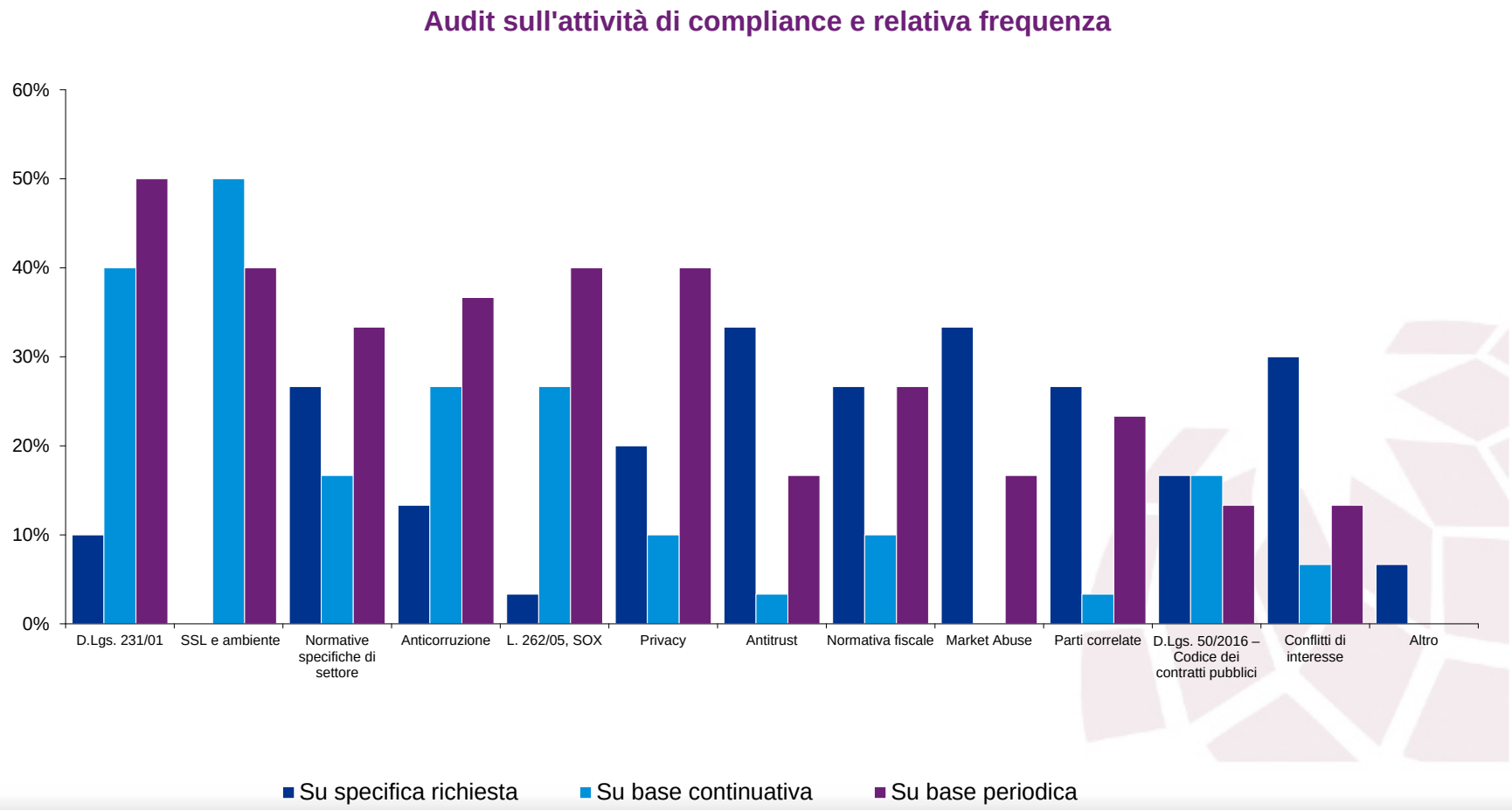
Compliance Transformation - Risultati della Survey

Monitoraggio e testing (3/4)



Compliance Transformation - Risultati della Survey

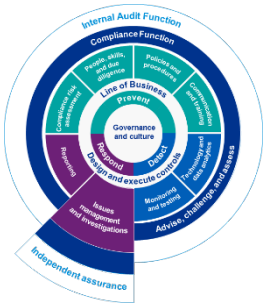
Monitoraggio e testing (4/4)



Compliance Transformation - Risultati della Survey

Gestione delle carenze e investigation

*"Anche il miglior compliance program può riscontrare **criticità** che richiedano **meccanismi efficaci di risposta**. Questi ultimi includono protocolli e modalità di verifica delle attività a rischio e in generale per la gestione complessiva delle carenze (ad es. Indagini, citazioni in giudizio o crisi d'impresa)."*



I rispondenti affermano che:

La Società non ha implementato un processo: a) per la valutazione degli impatti e le cause delle carenze; b) per la **valutazione degli impatti** trasversali nell'organizzazione; c) per la **definizione di azioni** (43%)

Non esiste un'**unità deputata a svolgere attività di investigation** che sia **separata** rispetto alle funzioni operative e che si coordina con le funzioni di controllo (73%)

Non viene effettuato un **reporting** almeno annuale al CdA sui risultati delle attività di **investigation**, includendo dati quantitativi per la valutazione dell'efficacia delle ispezioni, i fattori di rischio attuali, i rischi emergenti e le tendenze future (33%)

I **risultati delle attività di investigation** non vengono utilizzati per aggiornare coerentemente il compliance program (43%)

Al fine di migliorare l'efficacia delle attività di investigation le Società dovrebbero definire delle **metodologie** ispettive, erogare **corsi** specialistici sulle tecniche di investigation, dotarsi di adeguati **strumenti informatici**, approfondirne le cause attraverso analisi cause-effetto (**root-cause analysis**).

Compliance Transformation - Risultati della Survey

Reporting (1/2)

*"Le organizzazioni dovrebbero avere dei **meccanismi efficaci di reporting** verso le funzioni di governance, in particolare verso il **CdA**, al fine di consentire loro di supervisionare il mantenimento del compliance program nonché le attività di monitoraggio per la risoluzione delle carenze (che potrebbe richiedere anche un reporting verso l'esterno). Le funzioni con responsabilità in ambito compliance dovrebbero fornire **periodicamente** al CdA o ad altre funzioni delegate informazioni relative **all'efficienza ed efficacia del compliance program dell'impresa**."*

I rispondenti affermano che:

Il **reporting** in materia di compliance è lo strumento mediante il quale vengono comunicate al management, top management, CdA ed altri organi di controllo (CCR e CS) dati e informazioni **sull'esposizione al rischio di compliance** della Società (**83%**)

Sono previsti flussi di reporting in materia di compliance che comprendano anche informazioni in merito a **cultura della compliance, condotta, governance e altre tematiche rilevanti** (**77%**)

I rispondenti affermano che:

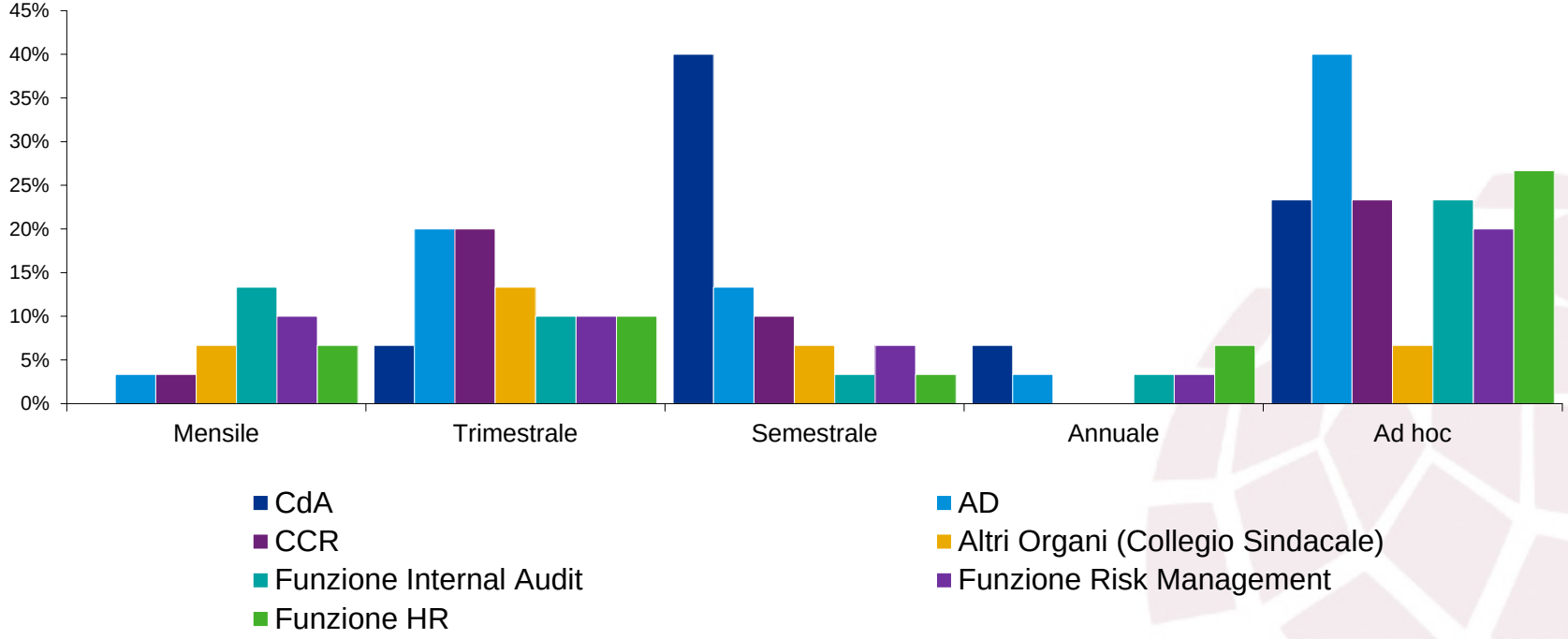
La Società non ha strutturato **un processo sistematico di reporting** in materia di compliance diretto al top management e al vertice aziendale (**37%**)

Un reporting strutturato può essere utile per comunicare informazioni preziose sullo stato di attuazione del compliance program nonché sulla sua efficacia a livello aziendale. Pertanto, il reporting dovrebbe essere **completo**, includendo non solo i **risultati del monitoraggio**, delle **attività di test** o i dati relativi ai soli **top-risk**, ma dovrebbe includere altresì informativa relativa alle **investigation**, **iniziative di formazione e certificazioni, due diligence**, **gestione delle performance**, etc. Al fine di garantire un'informativa efficace verso i vertici aziendali, il reporting sui rischi di compliance dovrebbe convergere in un documento di reporting integrato sui rischi.

Compliance Transformation - Risultati della Survey

Reporting (2/2)

Frequenza del reporting periodico in materia di compliance, per ciascuno dei seguenti destinatari



1. Ottimizzare la *governance* del modello di presidio dei rischi di compliance in ottica integrata, attraverso:

Conclusioni (1/2)

i) il rafforzamento **della cultura del rischio di compliance**, quale elemento fondamentale nelle linee di indirizzo sul sistema di controllo interno e gestione dei rischi, al fine di realizzare un sistema di regole che **attribuisce valore al rispetto rigoroso di elevati standard di comportamento**;

ii) il **coordinamento tra le funzioni di controllo** e la **convergenza dei rispettivi modelli** per assicurare una visione d'insieme dei principali rischi di compliance;

iii) l'istituzione di meccanismi di coordinamento tra i **presidi specialistici degli ambiti normativi** di riferimento (*privacy*, *antitrust*, anticorruzione,…) per garantire la collaborazione tra gli stessi e con la funzione di **compliance integrata** (ad esempio Compliance Officer);

iv) la definizione chiara dei **ruoli e responsabilità** dei principali attori operanti nell'ambito del sistema di controllo interno e gestione dei rischi – ivi inclusi gli organi di controllo – in coerenza con il **modello delle tre linee di difesa** (funzioni operative, funzioni di controllo e monitoraggio dei rischi e funzioni di internal audit);

v) la **definizione di best practice/linee guida condivise da parte delle Authority** che possano indirizzare le attività di compliance delle Aziende.

2. Migliorare nel continuo i *processi* di gestione della compliance attraverso:

3. Migliorare i *flussi informativi* di compliance, attraverso:

Conclusioni (2/2)

i) l'utilizzo dei **nuovi strumenti digitali**;

ii) lo sviluppo di metodologie sempre più efficaci di **identificazione** e **misurazione dei rischi**;

iii) l'integrazione dei **sistemi premianti** del personale **con obiettivi di *good conduct*** e l'attivazione di processi di *due diligence* e *feedback* delle terze parti;

iv) l'inserimento dei presidi di controllo nelle **procedure aziendali** (semplificandole e riducendole);

v) l'esecuzione di attività mirate e *risk based* di **monitoraggio** (più efficienti e focalizzate sulla risoluzione delle *root causes*);

vi) l'ampliamento dell'**ambito e della copertura** delle attività sottoposte a *risk oversight* da parte degli organismi aziendali.

i) la **semplificazione delle interazioni** con il management coinvolto in qualità di *risk owner;*

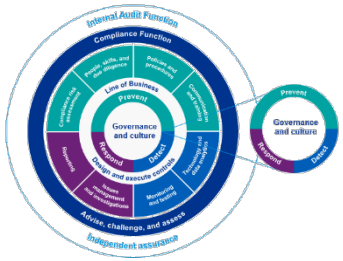
ii) un più efficace **reporting** dei principali rischi di *compliance* basato su una **tassonomia** condivisa dei rischi, dei controlli e delle rispettive metriche di valutazione.

BACKUP

Compliance Transformation e presidio dei rischi

Principali risultati della survey (1/3)

Governance e Cultura



Permettere al CdA di supervisionare i rischi di compliance. Mentre l'**83%** dei rispondenti afferma che il proprio CdA è *adeguatamente informato* in merito all'esposizione della Società ai singoli rischi di compliance e alle relative attività di mitigazione, solo per il **43%** il CdA riceve dei flussi informativi con una *vista integrata dei rischi di compliance*.

Aumentare l'integrazione delle responsabilità in ambito compliance. Il **37%** dei rispondenti dichiara che le responsabilità in ambito compliance sono *distribuite tra più funzioni* non necessariamente coordinate tra loro mentre il **63%** ha identificato una funzione responsabile della compliance. Tuttavia, solo il **10%** di questi ultimi afferma di avere una funzione dedicata *in maniera esclusiva* alla gestione di attività di compliance.
In generale per alcuni ambiti specifici, la maggior parte dei rispondenti afferma che con riferimento a specifiche normative (ad es. sulla salute, sicurezza e ambiente e Fiscale), sono presenti presidi di controllo affidati a funzioni specialistiche.

Incrementare la partecipazione attiva dei presidi di compliance all'interno di comitati manageriali. Il **70%** dei rispondenti afferma di non aver istituito un compliance committee a livello di management per acquisire o fornire informazioni in ambito compliance. Inoltre il **40%** dei rispondenti afferma che i presidi di compliance della Società non partecipano attivamente a comitati manageriali/management meeting con le funzioni operative.

Incrementare e formalizzare le modalità di interazione e coordinamento dei presidi di compliance con le alte funzioni di controllo. Il **67%** dei rispondenti dichiara che la Funzione Compliance e la Funzione Internal Audit interagiscono con frequenza *trimestrale*. Tuttavia, solo il **53%** afferma che il *perimetro* delle attività e le *modalità di coordinamento* tra le due funzioni sono *formalizzate* in documenti ufficiali.
Inoltre solo il **53%** delle Società conferma l'esistenza di *flussi informativi* tra la Funzione Compliance e la Funzione Risk Management, nonché la condivisione degli *esiti* delle rispettive attività.

Accrescere la consapevolezza del personale delle Società alle tematiche di compliance. Il **43%** dei rispondenti *valuta basso/medio-basso* il grado di sensibilità del personale alle tematiche di compliance.

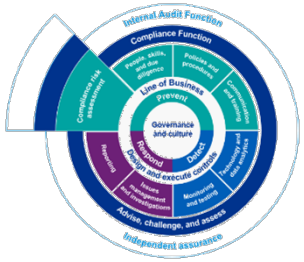
Comunicare ai dipendenti l'importanza della compliance. Il **43%** dei rispondenti afferma che il personale della Società non ha percezione delle *implicazioni* e del *vantaggio competitivo* derivante da una forte cultura della compliance. Inoltre, il **33%** afferma di non aver adottato degli *approcci* e implementato dei *tool* finalizzati a rinforzare la diffusione della cultura della compliance.

Incentivare la cultura del personale sulle tematiche di compliance. Solo il **37%** dei rispondenti sostiene di aver implementato una politica di incentivi (retributivi e non) e protocolli disciplinari per la promozione della cultura della compliance. Di questi, solo il **22%** afferma che tali incentivi danno la *percezione* al personale che la compliance può avere un *impatto significativo* per la loro carriera e retribuzione.

Compliance Transformation e presidio dei rischi

Principali risultati della survey (2/3)

Compliance risk assessment



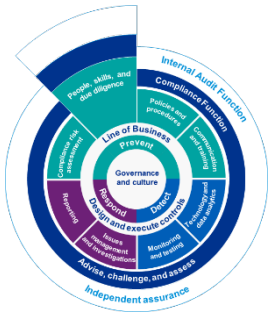
Implementare processi strutturati di compliance risk assessment. Il **33%** dei rispondenti afferma di non basare le attività di compliance risk assessment su valutazioni *quali-quantitative* sulla base di metriche predefinite.

Il **30%** dei rispondenti non identifica, valuta e misura i rischi *inerenti* ed i rischi *residui* di compliance. Una % maggiore di rispondenti afferma (**87%**) di valutare solo se i controlli sono *adeguatamente disegnati* e se tali controlli *mitigano efficacemente* i rischi di compliance identificati.

Favorire l'integrazione delle attività di compliance risk assessment. Solo il **57%** dei rispondenti dichiara di aver effettuato e formalizzato *un inventario delle normative* applicabili alla propria Società. Tuttavia, la mancata predisposizione di un *legal inventory integrato* rende più complessa l'identificazione dei rischi a cui la propria Società è esposta nonché la valutazione dei relativi controlli.

Risorse, competenze e due diligence

Definire sistemi premianti ai dipendenti che includono obiettivi di compliance. Solo il **40%** delle Società afferma che la *valutazione delle performance* è legata al comportamento dei dipendenti in linea con la cultura aziendale e ai valori dell'organizzazione . Nel **50%** dei casi gli obiettivi di compliance *non rientrano* tra gli obiettivi definiti per il management.



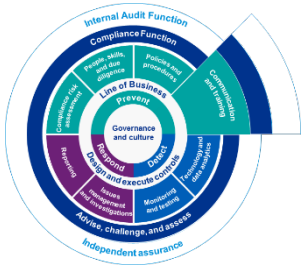
Definire procedure di verifica su risorse interne ed esterne. Solo il **67%** dei rispondenti afferma di effettuare *due diligence* sulla base di politiche e procedure predefinite attraverso verifiche sui fornitori e sui trascorsi personali dei nuovi dipendenti nonché valutazioni continue sulle performance degli stessi.

Strumenti normativi interni

Prestare maggiore attenzione alla definizione degli strumenti normativi interni in ambito compliance. Solo il **37%** dei rispondenti sostiene di aver adottato un compliance program riferito alla *totalità degli ambiti di compliance*.

Inoltre, solo il **63%** dei rispondenti afferma di avere una Funzione incaricata dell'*aggiornamento* di policy e procedure aziendali sui temi di compliance.

Comunicazione e formazione



Favorire iniziative formative al fine di incrementare le ore di formazione in ambito compliance. Mentre l'**87%** dei rispondenti afferma che sono previste iniziative formative su specifici ambiti/modelli di compliance, il **30%** dei rispondenti afferma che il proprio personale ha dedicato *meno del 10%* delle ore di formazione a tematiche di compliance nell'ultimo anno.

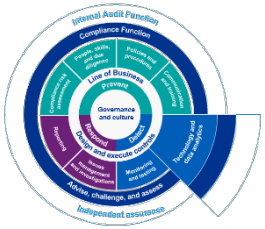
Compliance Transformation e presidio dei rischi

Principali risultati della survey (3/3)

Incrementare attività di formazione delle terze parti all'inizio del rapporto con la Società. Solo il **43%** dei rispondenti afferma che alle terze parti è richiesto di partecipare ad iniziative di *formazione* su ambiti di compliance all'inizio del rapporto con la Società.

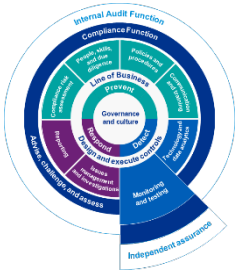
Tecnologia e data analytics

Necessità di implementare efficienti strumenti informatici e di analisi dei dati a supporto dei processi di compliance. Il **40%** dei rispondenti afferma che le attività di compliance sono supportate dall'utilizzo di *strumenti informatici.*



Solo il **27%** dei rispondenti sostiene che il compliance program si basa su *data analytics* e l'utilizzo di *strumenti informatici* per condurre analisi sui principali trend.
Inoltre, meno della metà dei rispondenti dichiara che KPI e KRI sono *integrati* a) nel processo di monitoraggio e testing della compliance (**40%**), b) nel sistema informativo di gestione della compliance (es. GRC - Governace, Risk and Compliance) (**27%**)

Monitoraggio e testing

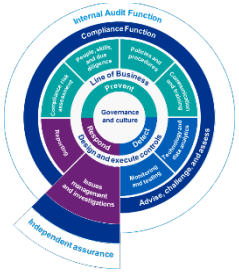


Estendere le attività di monitoraggio all'evoluzione normativa e all'effettività del compliance program. Il **53%** dei rispondenti afferma che la Società ha implementato un *processo strutturato* per monitorare e tenere traccia delle evoluzioni normative.

In particolare, il **33%** dei rispondenti sostiene che non è previsto un *piano di verifica* dell'efficacia del compliance program adottato e che pertanto non vengono eseguite periodiche valutazioni sui contenuti del compliance program al fine di garantire l'allineamento di quest'ultimo alle evoluzioni normative nonché alle aspettative degli stakeholder.

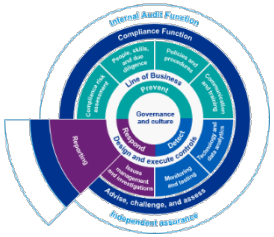
Gestione delle carenze e investigation

Integrare le modalità di gestione delle carenze tra le diverse funzioni di controllo. Solo il **57%** dei rispondenti afferma di aver implementato un processo: a) *per la valutazione degli impatti e le cause delle carenze*; b) *per la valutazione degli impatti trasversali nell'organizzazione*; c) *per la definizione di azioni correttive*.



Prevedere un'unità deputata a svolgere attività di investigation. Nel **73%** delle Società rispondenti manca *un'unità deputata a svolgere attività di investigation*. Inoltre, nel **43%** delle Società, i *risultati* delle attività di investigation non vengono utilizzati per aggiornare coerentemente il compliance program e rispondere efficacemente ad eventuali criticità riscontrate.

Reporting



Promuovere un processo di reporting strutturato e integrato in materia di compliance. Il **37%** dei rispondenti sostiene di non avere un processo *sistematico* di reporting in materia di compliance diretto al top management e al vertice aziendale.