ORDINE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI
MILANO

FONDAZIONE COMMERCIALISTI ODCEC di MILANO

Percorso formativo di Corporate Governance
Gestione dei rischi, problematiche
e impatti sul governo societario

SISTEMA DI CONTROLLO INTERNO E DI GESTIONE DEI RISCHI

PAOLA TAGLIAVINI

24 gennaio 2023

IL SISTEMA DI CONTROLLO INTERNO E DI GESTIONE DEI RISCHI (SCIGR)

I modelli di gestione più recenti sottolineano la centralità del rischio nel sistema dei controlli: le più recenti versioni del Codice di Autodisciplina ne hanno riconosciuto ed enfatizzato l'importanza. Il Codice di Autodisciplina fa riferimento a un sistema di controllo interno e di gestione dei rischi come sistema unitario in cui il rischio rappresenta il filo conduttore.

La definizione di SCIGR del Codice di Autodisciplina 2018 "Ogni emittente si dota di un sistema di controllo interno e di gestione dei rischi costituito dall'insieme delle **regole, delle procedure e delle strutture organizzative volte a consentire l'identificazione, la misurazione, la gestione e il monitoraggio dei principali rischi.** Tale **sistema è integrato nei più generali assetti organizzativi e di governo societario** adottati dall'emittente e tiene in adeguata considerazione i modelli di riferimento e le best practices esistenti in ambito nazionale e internazionale. " Art. 7.P.1.

La definizione di SCIGR del Codice di Corporate Governance 2020 " Il sistema di controllo interno e di gestione dei rischi è costituito dall'insieme delle regole, procedure e strutture organizzative finalizzate ad una effettiva ed efficace identificazione, misurazione, gestione e monitoraggio dei principali rischi, **al fine di contribuire al successo sostenibile della società.** " (Art. 6 XVIII)

IL SISTEMA DI CONTROLLO INTERNO E DI GESTIONE DEI RISCHI (SCIGR)

Obiettivi del SCIGR (Art. 7.P.2. Cod. 2018)

"Un efficace sistema di controllo interno e di gestione dei rischi contribuisce a una conduzione dell'impresa coerente con gli obiettivi aziendali definiti dal consiglio di amministrazione, favorendo l'assunzione di decisioni consapevoli. Esso concorre ad assicurare :

- la salvaguardia del patrimonio sociale,
- l'efficienza e l'efficacia dei processi aziendali,
- l'affidabilità delle informazioni fornite agli organi sociali ed al mercato;
- il rispetto di leggi e regolamenti nonché dello statuto sociale e delle procedure interne."

GLI ATTORI DEL SISTEMA DI CONTROLLO INTERNO E DI GESTIONE DEI RISCHI

L'organizzazione del sistema di controllo interno e di gestione dei rischi coinvolge, ciascuno per le proprie competenze: *(Art. 6 raccomandazione 32 Cod. Corporate Governance 2020)*

a. l'Organo di Amministrazione, che svolge un ruolo di indirizzo e di valutazione dell'adeguatezza del sistema;

b. il Chief Executive Officer, incaricato dell'istituzione e del mantenimento del sistema di controllo interno e di gestione dei rischi;

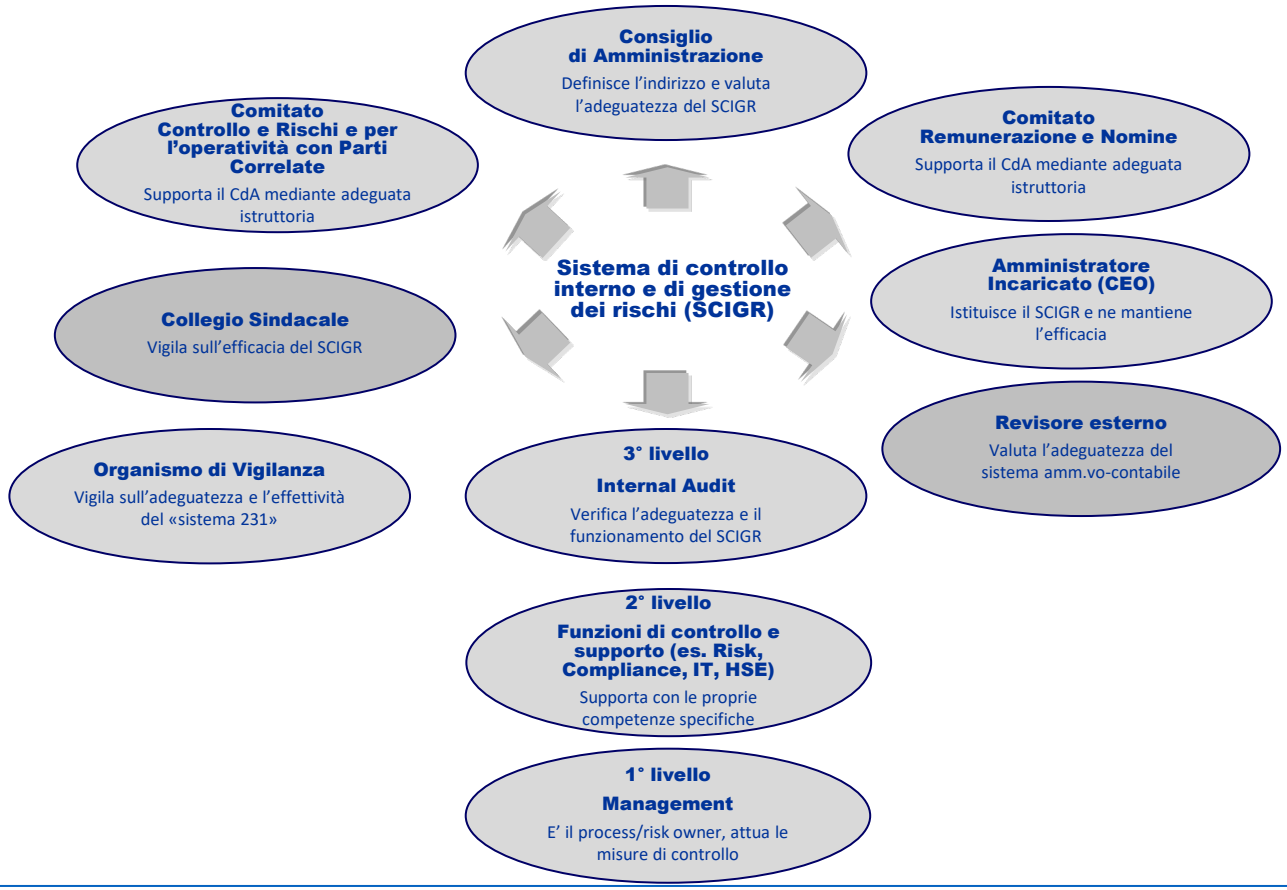
c. il Comitato Controllo e Rischi, istituito all'interno dell'organo di amministrazione, con il compito di supportare le valutazioni e le decisioni dell'organo di amministrazione relative al sistema di controllo interno e di gestione dei rischi e all'approvazione delle relazioni periodiche di carattere finanziario e non finanziario;

d. il Responsabile della funzione di Internal Audit, incaricato di verificare che il sistema di controllo interno e di gestione dei rischi sia funzionante, adeguato e coerente con le linee di indirizzo definite dall'organo di amministrazione;

e. le altre funzioni aziendali coinvolte nei controlli (quali le funzioni di risk management e di presidio del rischio legale e di non conformità), articolate in relazione a dimensione, settore, complessità e profilo di rischio dell'impresa;

f. Il Collegio Sindacale, che vigila sull'efficacia del sistema di controllo interno e di gestione dei rischi.

GLI ATTORI DEL SISTEMA DI CONTROLLO INTERNO E DI GESTIONE DEI RISCHI



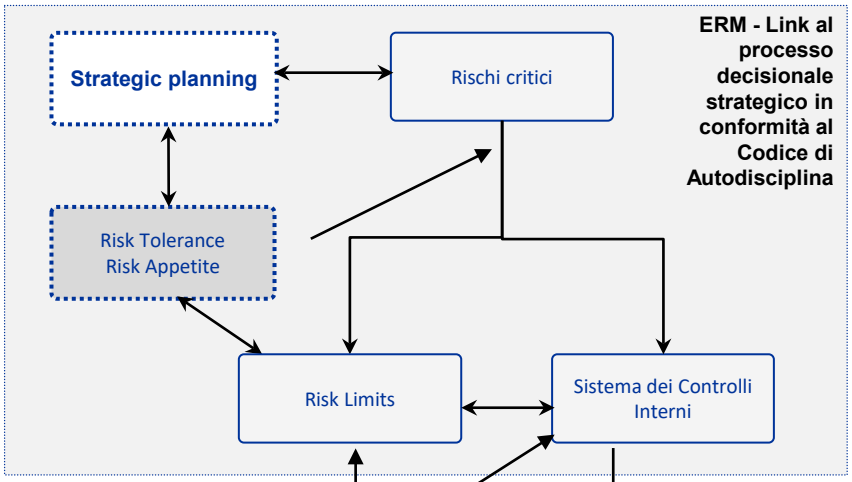
PRINCIPI DEL NUOVO CODICE di CORPORATE GOVERNANCE

L'organo di amministrazione, con il supporto del Comitato Controllo e Rischi, definisce le linee di indirizzo del sistema di controllo interno e di gestione dei rischi **in coerenza con le strategie della società** e valuta, con cadenza almeno annuale, **l'adeguatezza del medesimo sistema rispetto alle caratteristiche dell'impresa e al profilo di rischio assunto**, nonché la sua **efficacia**

- Collegamento con la strategia
- Rilevanza della coerenza tra rischio assunto e rischio sostenibile (risk appetite vs. risk capacity)
- Efficacia del SCIGR

L'EVOLUZIONE DEL RISK MANAGEMENT

DA FOCUS OPERATIVO A LINK CON LE DECISIONI STRATEGICHE



ERM

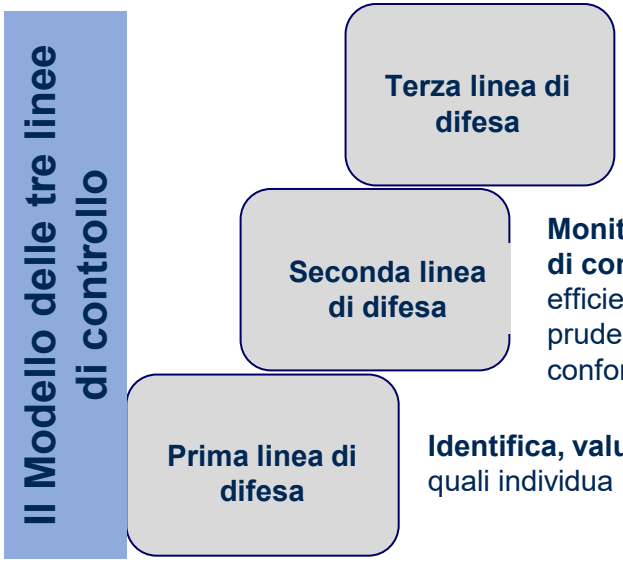
collega il processo di Risk Management alla assunzione di decisioni strategiche → **CRO**

RM tradizionale

ha un focus operativo e tipicamente porta con sé una visione a "silos " dei rischi → **RM**

IL MODELLO DELLE TRE LINEE DI DIFESA

- Il controllo deve essere esercitato attraverso linee di difesa chiare, definite e indipendenti – la business line, il risk management e l'internal audit – ciascuna delle quali gioca un ruolo rilevante nell'ambito del sistema di gestione dei rischi.
- Il modello basato su tre linee di difesa distingue tra funzioni che sono sia owner sia gestori dei rischi, funzioni che supervisionano i rischi e funzioni che forniscono una assurance indipendente.



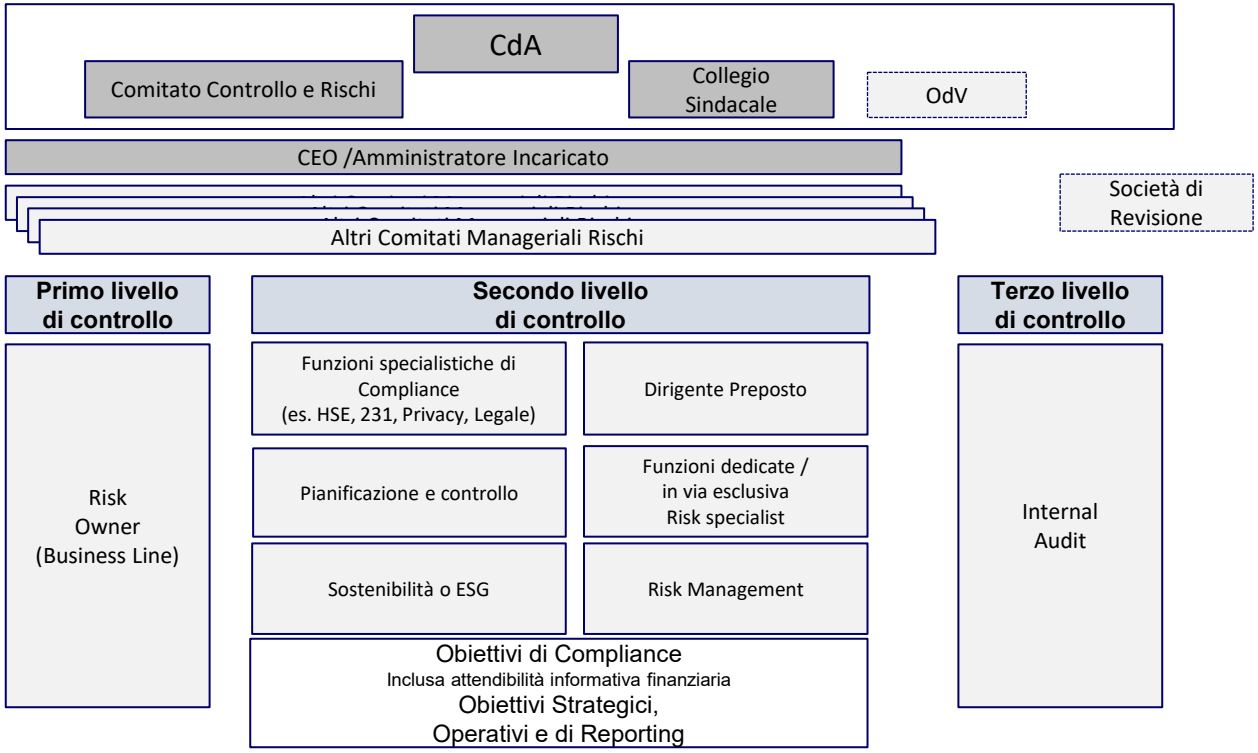
Fornisce **assurance** indipendente sull'adeguatezza ed effettiva operatività del primo e secondo livello di controllo

Monitora i rischi aziendali, propone le **linee guida sui relativi sistemi di controllo** e **verifica l'adeguatezza degli stessi** per assicurare efficienza ed efficacia delle operazioni, adeguato controllo dei rischi, prudente conduzione del business, affidabilità delle informazioni, conformità a leggi, regolamenti e procedure interne

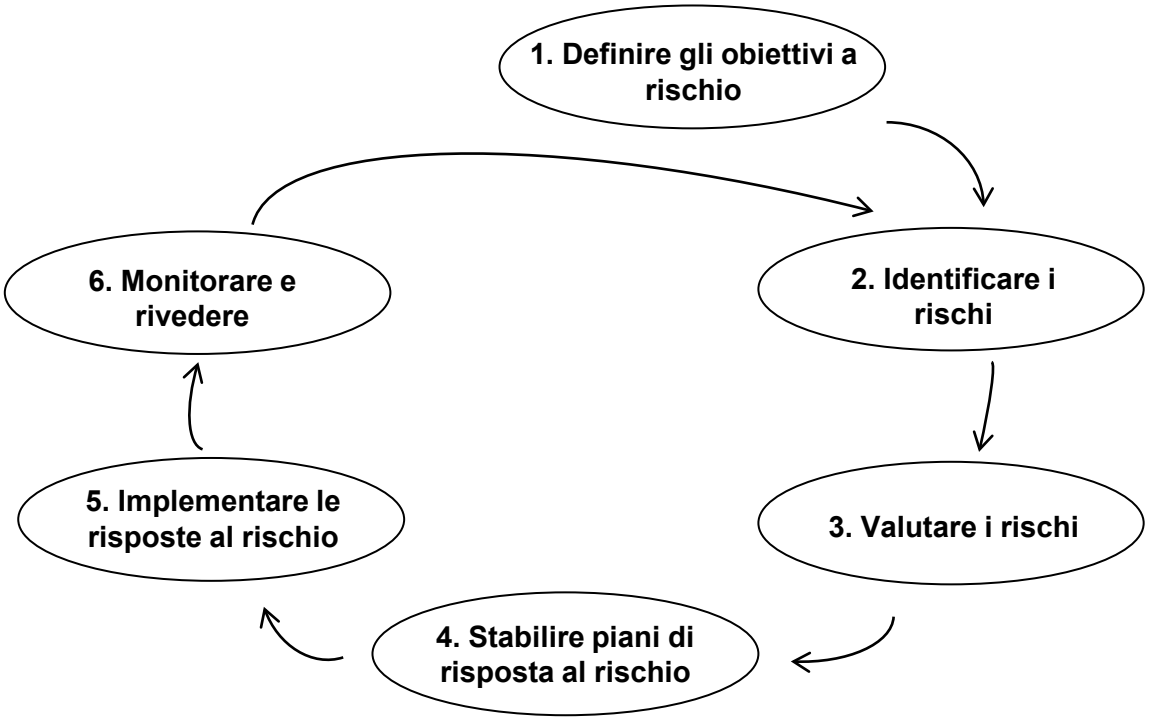
Identifica, valuta, gestisce e monitora i rischi di competenza in relazione ai quali individua e **attua specifiche azioni di trattamento**

I TRE LIVELLI DI DIFESA/CONTROLLO

ESEMPLIFICAZIONE



PROCESSO DI RISK MANAGEMENT



DEFINIZIONE DI ERM

L'Enterprise Risk Management (ERM) è un processo, posto in essere dal Consiglio di Amministrazione e dal management, impiegato come framework per la formulazione delle strategie e nello svolgimento delle attività ordinarie, progettato per:

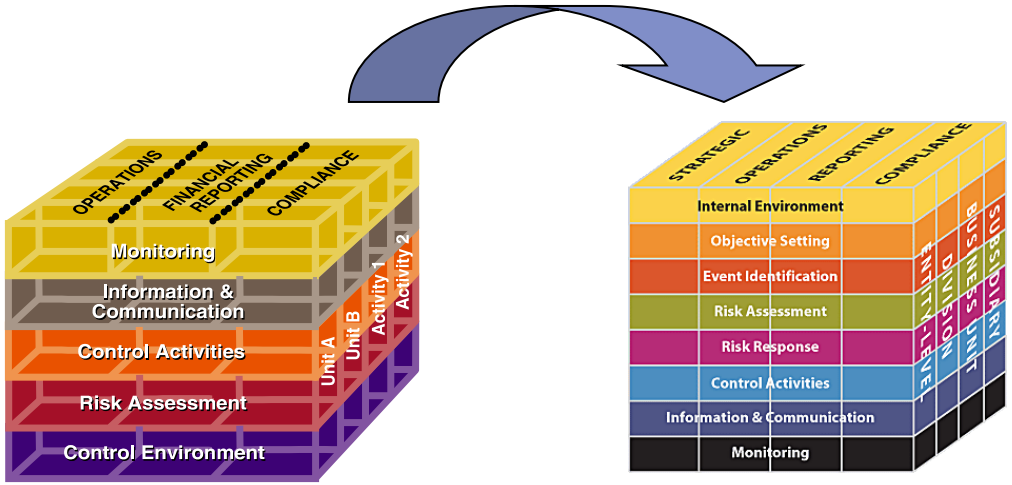
- individuare eventi potenziali che possono influire sull'attività aziendale;
- gestire il rischio entro i limiti del rischio accettabile;
- fornire ragionevole sicurezza sul conseguimento degli obiettivi aziendali.

Source: COSO Enterprise Risk Management – Integrated Framework. 2004. COSO.

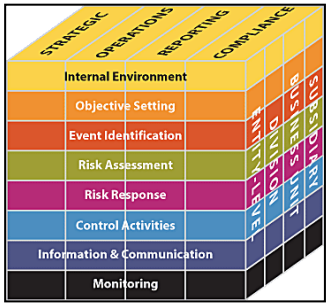
L'ERM consente al management un'efficace ed efficiente gestione delle condizioni di incertezza e dei connessi rischi ed opportunità, con conseguente possibilità di creazione di valore

COSO FRAMEWORK

Per aiutare ad assistere nell'implementazione di un processo di ERM, COSO ha sviluppato l'**ERM Integrated Framework** (2004), anche conosciuto come **COSO Cube**. Questo cubo è una evoluzione dell'iniziale COSO I framework sviluppato nel 1992



IL «NUOVO» COSO FRAMEWORK



Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues Improvement in Enterprise Risk Management

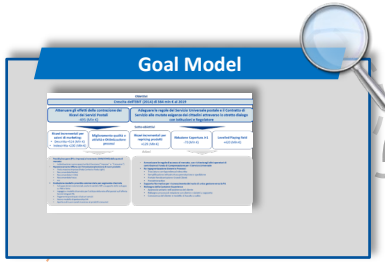
Information, Communication, & Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

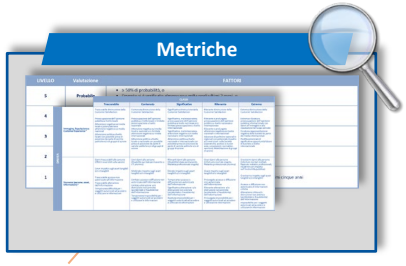
LE CATEGORIE DI RISCHI DELL'ERM

- **Tutte le categorie** di rischi di impresa sono considerati nell'**ERM**. Il catalogo di solito è strutturato nelle seguenti classi di rischio:
  - **Rischi esterni:** elementi rilevanti del contesto esterno, come regolamentazione, concorrenza, politica, che possono impattare sul perseguimento degli obiettivi aziendali
  - **Rischi strategici**: cambiamenti inattesi in elementi chiave per la formulazione o esecuzione della strategia
  - **Rischi finanziari**: cambiamenti inattesi nelle condizioni di tasso, prezzo, liquidità sui mercati
  - **Rischi operativi**: cambiamenti inattesi in elementi correlati alle operations, tipicamente risorse umane, processi, tecnologia e eventi naturali. Molti rischi specifici della categoria «operativa» sono connessi alle tematiche della più ampia compliance o corporate governance; altri richiedono una comprensione della tecnologia e delle infrastrutture che sono di supporto alle attività di core business. La loro eterogeneità di composizione li rende molto numerosi

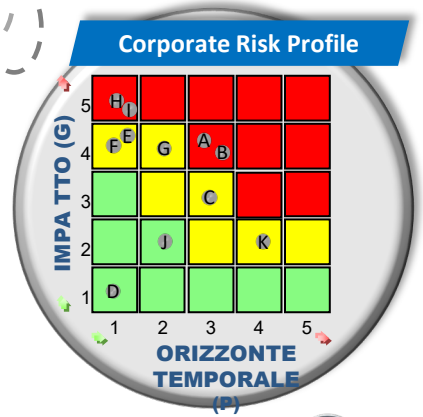
OVERVIEW COMPLESSIVA DEL PROCESSO DI RISK ASSESSMENT E DEGLI STRUMENTI

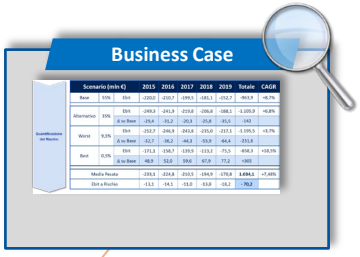


Il **"Goal Model"** contiene gli obiettivi e le direttive strategiche riportate sul Piano Strategico

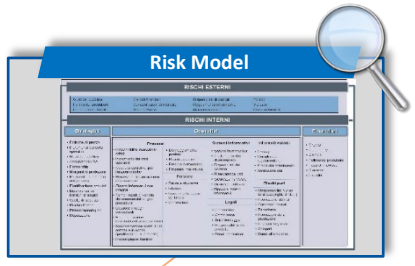


Le **"Metriche"** per valutare la probabilità del rischio e l'impatto del rischio utilizzando diversi driver (qualitativo-descrittivo, reddituale, patrimoniale, operativo, immagine e reputazione, sicurezza)





I **"Business Case"** al fine di valutare il rischio e di quantificare il relativo impatto a supporto della valutazione fornita



Il "**Risk Model**" contiene la tassonomia dei rischi sviluppata sulla base delle specificità del business Aziendale ed è articolato su due livelli: Categoria e Sotto-categoria di rischio

Il **"Risk Register"** al fine di inserire e formalizzare le informazioni relative a ciascun rischio individuato