Ing. Fabrizio Di Crosta
CONSULENZA DIREZIONALE DI IMPRESA

La Valutazione dei rischi nella ISO 9001:2015

MECSPE
TECNOLOGIE PER L'INNOVAZIONE - INDUSTRIE 4.0

17ª Edizione
22-24 marzo 2018
Fiere di Parma

CNA Emilia Romagna

Concetto di rischio: definizioni

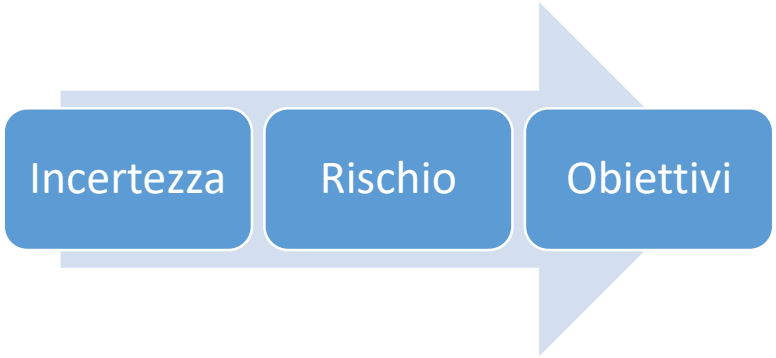
Definizioni:

- **Rischio:** Effetto dell'incertezza

[ISO 9000:2015]

- **Rischio**: Effetto dell'incertezza sugli obiettivi.

[Guida ISO 73:2009, definizione 1.1]



Concetto di rischio: definizioni

- ✓ Un effetto è uno scostamento da quanto atteso - positivo e/o negativo.
- ✓ Gli obiettivi possono presentare aspetti differenti (come scopi finanziari, di salute e sicurezza, ambientali) e possono intervenire a livelli differenti (come progetti, prodotti e processi strategici, riguardanti l'intera organizzazione).
- ✓ Il rischio è spesso caratterizzato dal riferimento a **eventi** potenziali e **conseguenze**, o una combinazione di questi.
- ✓ Il rischio è spesso espresso in termini di combinazione delle conseguenze di un evento (compresi cambiamenti nelle circostanze) e della **verosimiglianza** del suo verificarsi.
- ✓ L'incertezza è lo stato, anche parziale, di assenza di informazioni relative alla comprensione o conoscenza di un evento, delle sue conseguenze o della loro verosimiglianza.

Risk Management: definizioni

- **gestione del rischio**: Attività coordinate per guidare e tenere sotto controllo una organizzazione con riferimento al **rischio**.

- **politica per la gestione del rischio:** Dichiarazione degli orientamenti ed indirizzi generali di un'organizzazione relativi alla gestione del rischio.

- **propensione al rischio**: Approccio dell'organizzazione per valutare ed eventualmente ricercare, ritenere, assumere, o evitare il rischio.

Risk Management : definizioni

- **piano di gestione del rischio**: Schema interno alla **struttura di riferimento per la gestione del rischio** che specifica l'approccio, i componenti gestionali e le risorse da applicare alla gestione del **rischio**.

  - ✓ *I componenti gestionali comprendono tipicamente procedure, prassi, attribuzione di responsabilità, sequenza e temporizzazione delle attività.*
  - ✓ *Il piano di gestione del rischio può essere applicato ad un particolare prodotto, processo e progetto, inoltre ad una parte o all'intera organizzazione.*

Risk Management : definizioni

- **evento**: Il verificarsi o il modificarsi di un particolare insieme di circostanze.
  - ✓ *Un evento può consistere in una o più episodi e può avere diverse cause.*
  - ✓ *Un evento può consistere nel non verificarsi di qualcosa.*
  - ✓ *A volte ci si può riferire ad un evento come un "incidente" o "evento sfavorevole".*
  - ✓ *Ad un evento senza **conseguenze** ci si può anche riferire come un "near miss", "incidente", "near hit" o "close call".*

Risk Management : definizioni

- **conseguenza**: Esito di un evento che influenza gli obiettivi.
  - ✓ *Un evento può portare ad una gamma di conseguenze.*
  - ✓ *Una conseguenza può essere certa o incerta e può avere effetti positivi o negativi sugli obiettivi.*
  - ✓ *Le conseguenze possono essere espresse in modo quantitativo o qualitativo.*
  - ✓ *Le conseguenze iniziali possono aggravarsi attraverso effetti indiretti (per esempio "effetto domino").*

Risk Management : definizioni

- **valutazione del rischio**: Processo complessivo di **identificazione del rischio**, **analisi del rischio** e **ponderazione del rischio**.
- **identificazione del rischio**: Processo di ricerca, individuazione e descrizione dei **rischi**.
  - ✓ *L'identificazione del rischio implica l'identificazione delle **fonti di rischio**, degli **eventi**, relative cause e delle loro potenziali **conseguenze**.*
  - ✓ *L'identificazione del rischio può implicare l'esame di dati storici, analisi teoriche, opinioni basate su conoscenze precise e su pareri di esperti, ed esigenze dei **portatori d'interesse**.*

Risk Management : definizioni

- **analisi del rischio**: Processo di comprensione della natura del **rischio** e di determinazione del **livello di rischio**.

*L'analisi del rischio fornisce la base per la **ponderazione del rischio** e le decisioni circa il **trattamento del rischio**.*

L'analisi del rischio comprende la misurazione del rischio.

- **ponderazione del rischio**: Processo di comparazione dei risultati dell'**analisi del rischio** rispetto ai **criteri di rischio** per determinare se il **rischio** e/o la sua espressione quantitativa sia accettabile o tollerabile.

  *La ponderazione del rischio agevola la decisione circa il **trattamento del rischio**.*

Risk Based Thinking

- Il ***risk based thinking*** è un approccio alla progettazione, attuazione e documentazione del sistema di gestione finalizzato alla **prevenzione degli eventi negativi** (non conformità, reclami, ritardi di consegna, interruzioni della produttività e dei servizi, ecc.) che potrebbero accadere con maggiore probabilità e con impatto e conseguenze maggiormente negative.

- Proprio per le finalità preventive del *risk based thinking* è stato eliminato un punto specifico sulle **azioni preventive**, che dovranno confluire nel più ampio spettro delle azioni di miglioramento pianificate.

Risk Based Thinking

- La valutazione che l'organizzazione deve effettuare sui propri rischi di business avviene a valle dall'analisi del **contesto dell'organizzazione**, in quanto solo analizzando in dettaglio il contesto nel quale si muove l'organizzazione è possibile identificare i rischi reali che potrebbero influenzare i processi di business dell'organizzazione.

Risk Based Thinking

L'**organizzazione è responsabile della propria applicazione del *risk based thinking*** e può decidere se documentare, e come farlo, il processo di determinazione dei rischi

Risk-based thinking

Identificare Rischi ed Opportunità

Valutare Rischi ed Opportunità

Trattare i Rischi e cogliere le Opportunità

6.1 Azioni per affrontare rischi e opportunità

Considerando il **contesto dell'organizzazione** descritto ai punti 4.1 e 4.2 l'organizzazione deve determinare **rischi ed opportunità** che influenzano la sua attività per:

- assicurare i **risultati attesi** del sistema di gestione per la qualità
- **accrescere gli effetti desiderati** (derivanti dalle opportunità)
- **prevenire gli effetti indesiderati** (derivanti dai rischi)
- perseguire il **miglioramento continuo**.

6.1 Azioni per affrontare rischi e opportunità

- Le azioni per affrontare rischi ed opportunità devono essere pianificate secondo modalità che assomigliano molto al vecchio paragrafo sulle azioni preventive e di miglioramento.

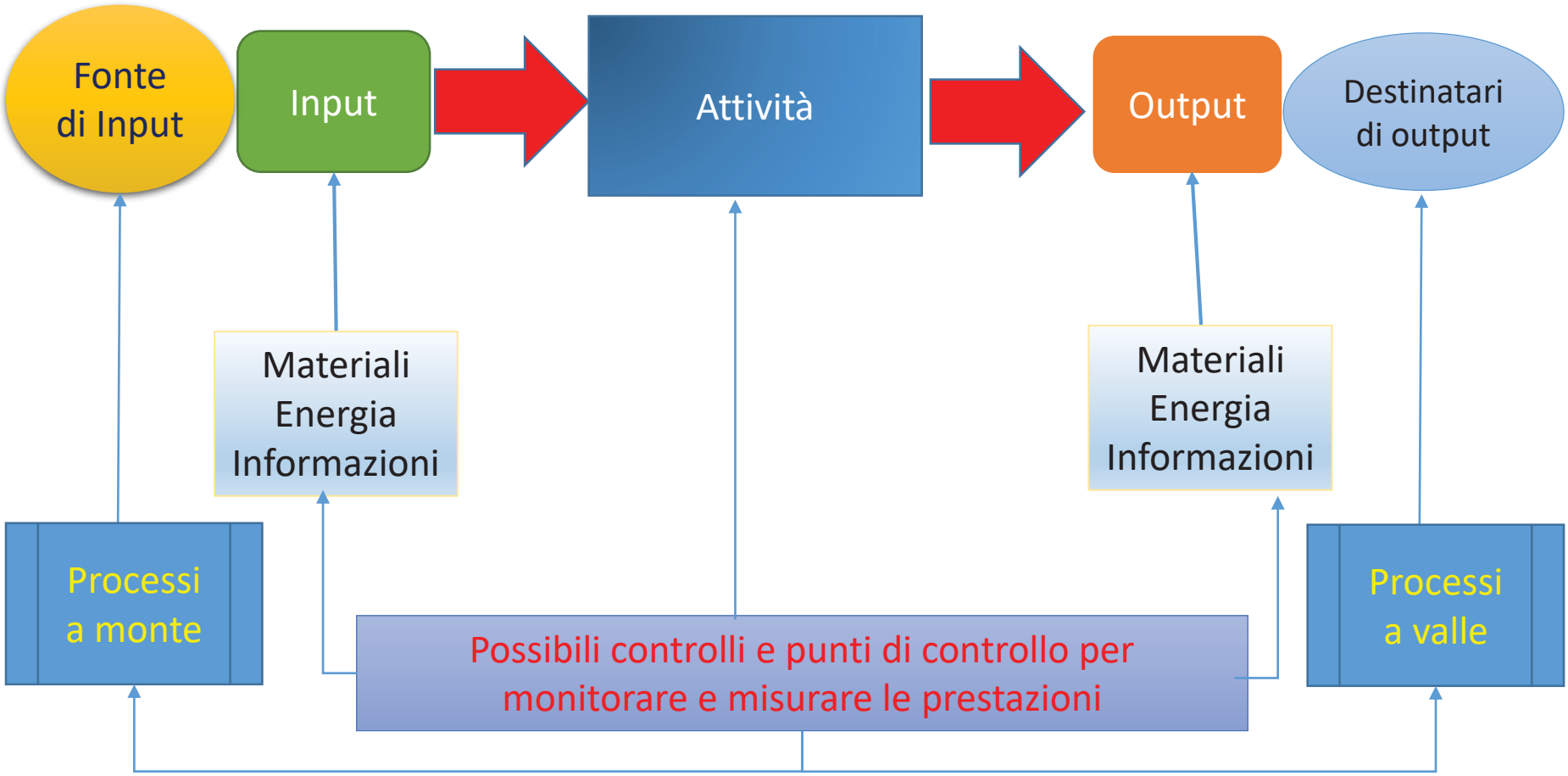
Tali azioni sono elevate di livello,

- derivano dalla valutazione di importanza di rischi ed opportunità,
- devono essere attuate integrandole nell'intero sistema e nei suoi processi e
- deve essere valutata l'efficacia di tali azioni.

6.1 Azioni per affrontare rischi e opportunità

- a fronte dell'identificazione di un rischio, l'assunzione dello stesso permette di cogliere un'opportunità di crescita
- Le opportunità possono trovarsi nell'ambito dell'innovazione di prodotto e di processo, nelle relazioni con clienti e fornitori, nella creazione di nuovi prodotti .....

Approccio per processi



Risk Management

Riferimenti normativi

- UNI ISO 31000: 2010 - Gestione del rischio - Principi e linee guida
- UNI 11230:2007 – Gestione del rischio – Vocabolario
- ISO/IEC 31010:2009 - Risk management – Risk assessment techniques
- ISO/TR 31004:2013 -Risk management -- Guidance for the implementation of ISO 31000

Risk Management

- ISO Guide 73:2009
- ISO/IEC 27005:2008 - Information technology — Security techniques — Information security risk management

Risk Management

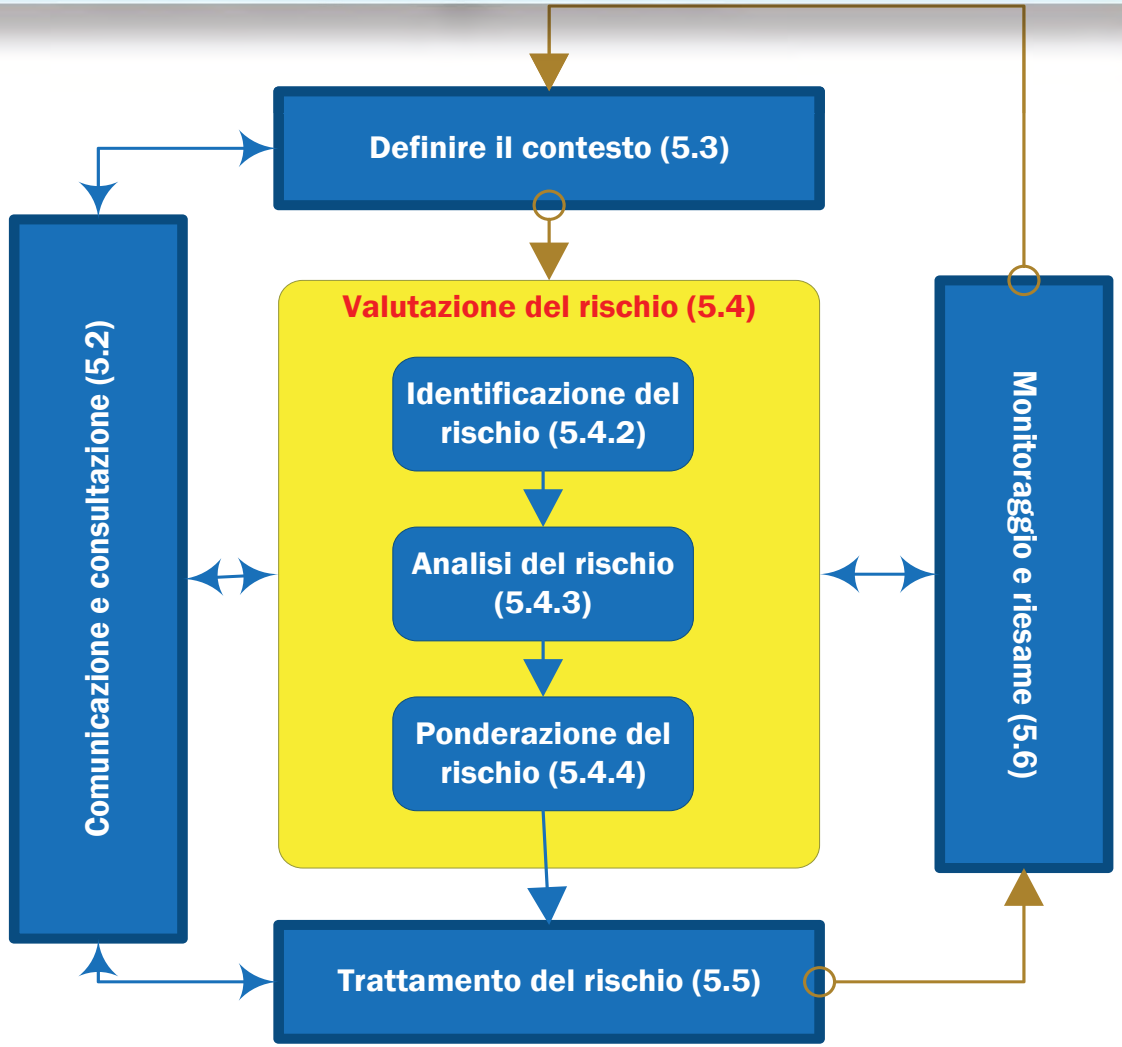
La gestione del rischio è un'attività/obiettivo a cui ogni azienda equilibrata dovrebbe tendere per minimizzare la possibili perdite a fronte di eventi imprevisti.

La Linea Guida ISO 31000 ci propone un modello di gestione del rischio e di integrazione dello stesso nel sistema di gestione aziendale.

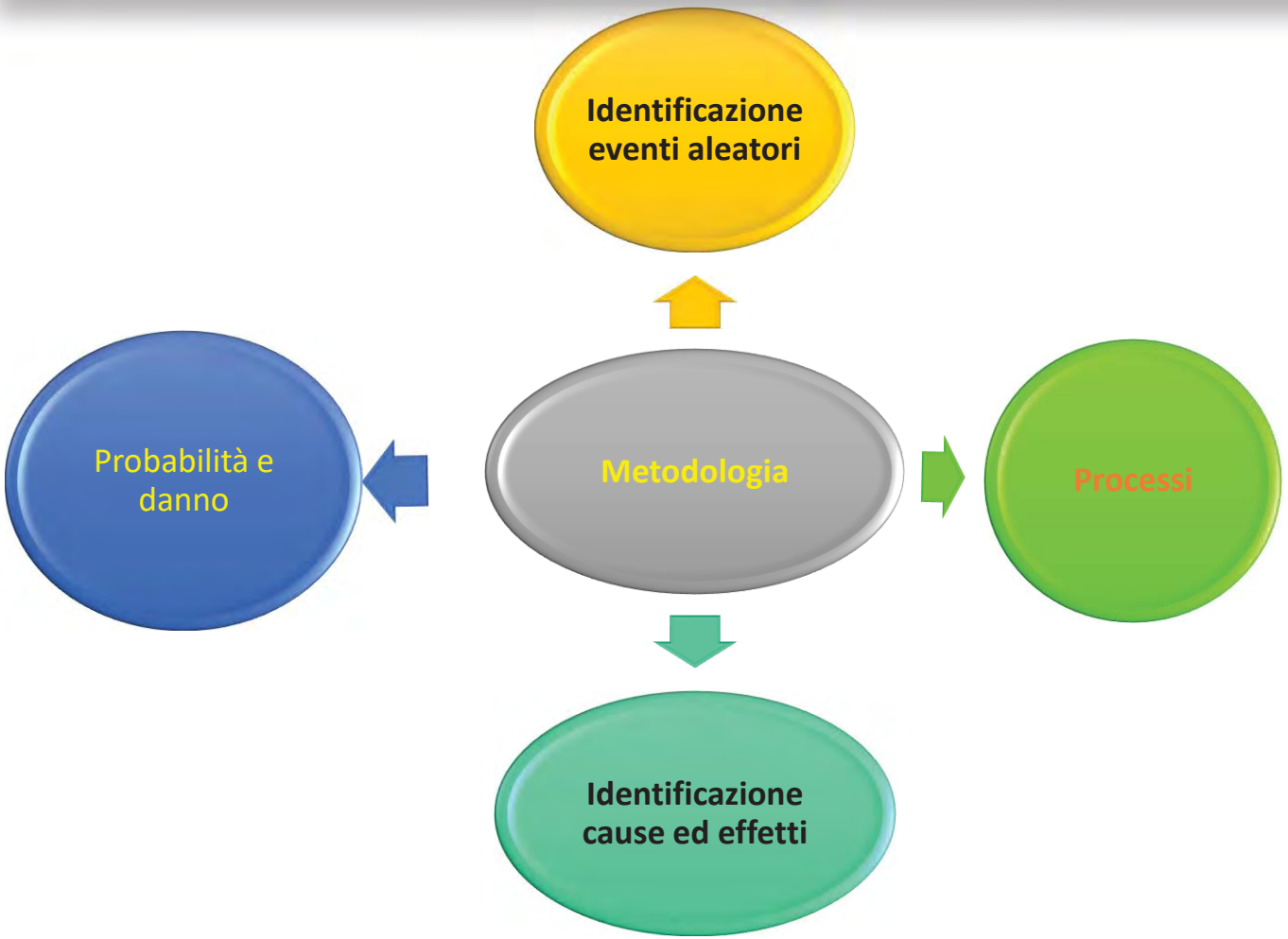
È applicabile a qualsiasi tipo di rischio (strategico, operativo, valutario, finanziario, di mercato, di *compliance*, di Paese, ecc.

Risk Management

Risk Management
Il processo



Risk Management



Risk Management

Esistono varie tecniche di ponderazione del rischio

Identificare le minacce e le vulnerabilità

Valutare gli impatti/conseguenze

Valutare le probabilità di accadimento

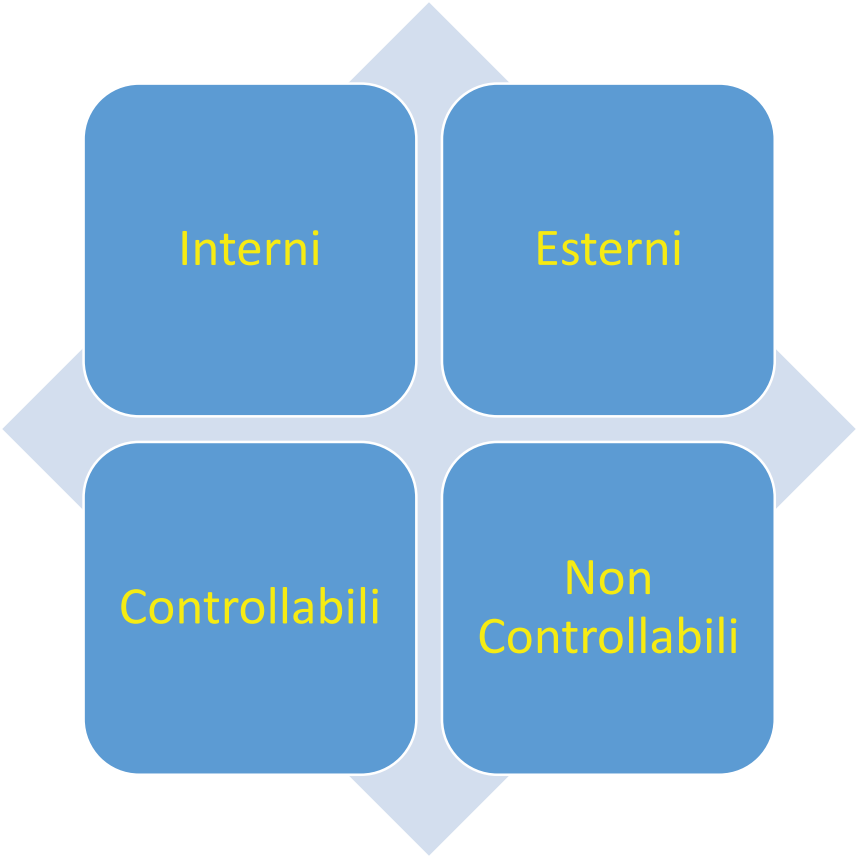
Risk Management

I rischi vengono in genere classificati in **tre gruppi** a seconda della loro origine:

- Strategici
- Operativi
- Finanziari

Risk Management

Alternativamente, a seconda della loro tipologia:



Risk Management

- **Rischi finanziari:** oscillazione prezzi materie prime, rischio tassi di solvibilità e affidabilità economico finanziaria, ecc.
- **Rischi strategici (e di contesto esterno):** rischi caratteristici del business di riferimento, la cui corretta gestione è fonte di vantaggio competitivo o, diversamente, causa di mancato raggiungimento di obiettivi (*incertezza scenario, reputazione, brand, innovazione prodotti, rischio paese ecc.*)
- **Rischi operativi:** rischi generati dall'organizzazione e dai processi (*processi, efficacia rete commerciale, risorse umane, tecnologia, Supply Chain ecc.*)
- **Rischi di compliance**: normativa regolamentare, privacy, fiscale, salute e sicurezza ecc.

Risk Management

Rischi legali (Modello 231)

Rischi ambientali (ISO 14001)

Rischi per la sicurezza sul lavoro (OHSAS 18001)

Rischi per la sicurezza delle informazioni (ISO 27001)

Rischi amministrativi (Linee guida Borsa italiana)

Rischi organizzativi (ISO 9001)

Rischi etici/responsabilità sociale (ISO 26000)

Risk Management

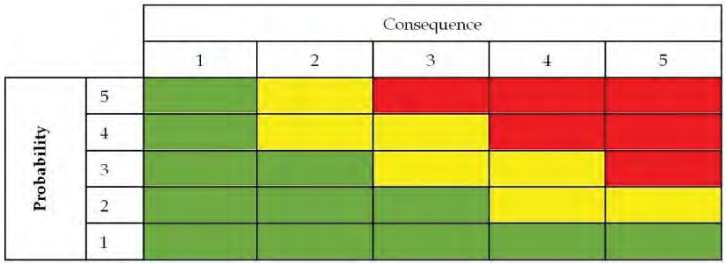
Diverse tipologie di rischi definite da schemi differenti:

- Basilea 2: 4 macro (di mercato, di credito, strategici, operativi) e 11 micro
- Assogestioni: 8 macro (strategici, finanziari, operativi,...) e 35 micro
- CO.SO. Enterprise Risk Management
- Altri *framework* specifici di settore (FMEA, sicurezza informatica, ecc.)

Risk Management

In generale ogni metodologia prevede di:

- ✓Scomporre i processi
- ✓Analizzare gli eventi
- ✓Identificare le cause
- ✓Valutare gli effetti



Risk Management

ISO 31010

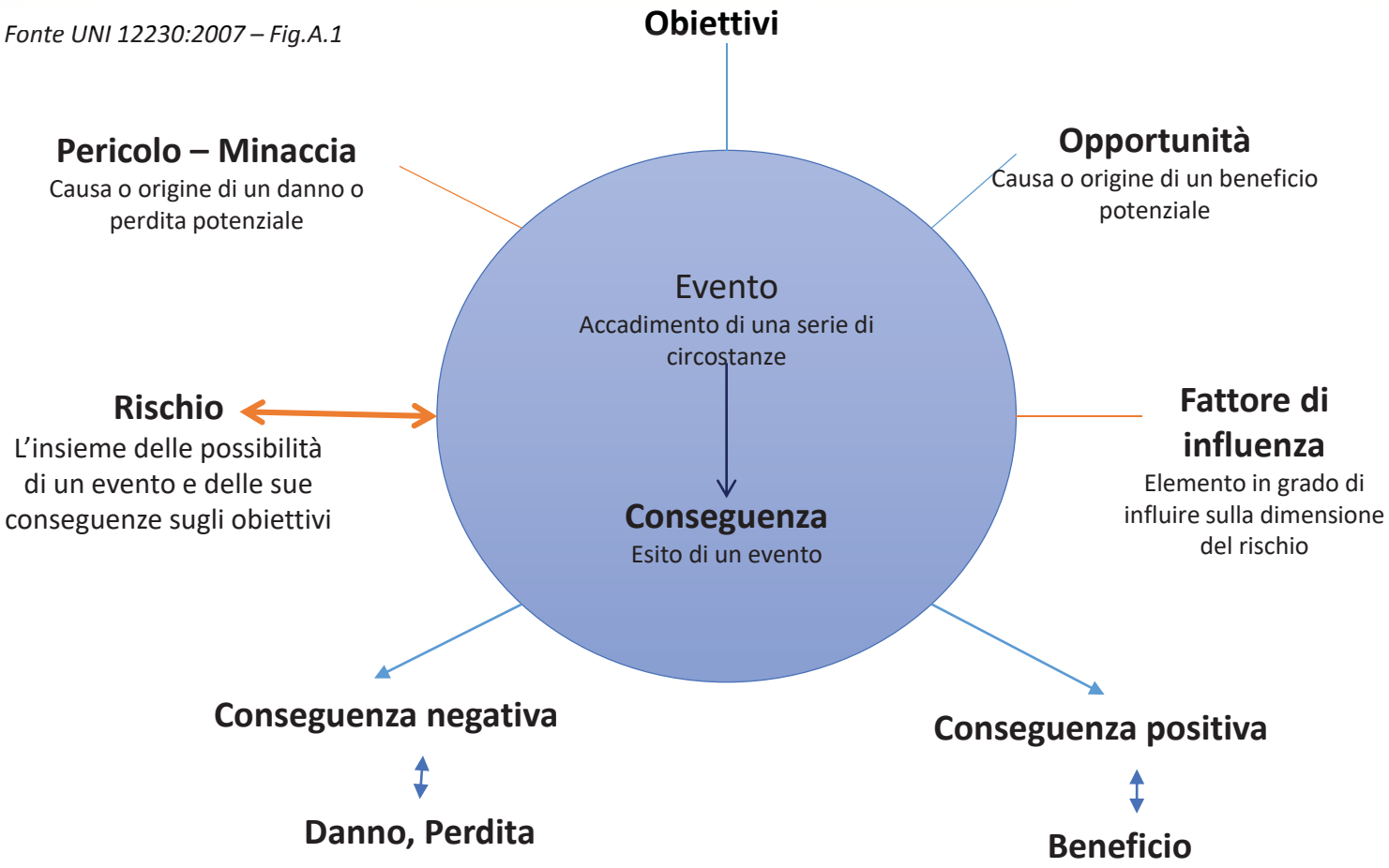
Risk Management

ISO 31010 Tecniche di risk assessment

- Per ciascuna tecnica (31) indica il livello di applicabilità rispetto alla fase
- Per ciascuna tecnica fornisce una descrizione e l'impatto di alcuni fattori quali:
  - ✓Risorse e capacità richieste per l'applicazione
  - ✓Natura e grado di incertezza
  - ✓Complessità
  - ✓Se fornisce output quantitativi
- Per ciascuna tecnica fornisce inoltre una informativa completa sulle modalità d'uso, input e output, il processo di esecuzione e i limiti

Risk Management

Fonte UNI 12230:2007 – Fig.A.1



Valutazione del Rischio

I criteri generali utilizzati considerano le seguenti variabili (minime):

- **Probabilità** di accadimento
- **Impatto** (conseguente all'accadimento) e relativa **gravità**

La combinazione di tali variabili determina **l'esposizione al rischio.**

Il confronto dei risultati dell'analisi del rischio rispetto ai criteri scelti dall'organizzazione determina la sua **espressione quantitativa** (ponderazione) e fornisce elementi per valutare l'**accettabilità** (soglia) e la **tollerabilità** (range) del rischio.

Valutazione del Rischio

- L'esposizione al rischio viene solitamente classificata come «*elevata*», «*modesta*», «*limitata*»,……. «*alta*», «*media*», «*bassa*»
- Attraverso una **matrice probabilità/impatto** possono essere individuate le varie "**aree di esposizione**" al rischio
- La definizione delle **aree di esposizione** in relazione a probabilità e impatto dipende dalle *policy* che l'azienda intende avviare in tema di rischio
- In base alle scelte aziendali/decisioni viene definita anche la "**soglia di attenzione**" (propensione al rischio) ovvero la linea di demarcazione tra i rischi che devono essere affrontati con priorità e gli altri

Livello di Rischio = Probabilità x Impatto

- Ma è opportuno considerare anche le **contromisure**, i **controlli** in essere

Trattamento del Rischio

Le strategie finalizzate a gestire i rischi si dividono in azioni per:

- **Evitare** il rischio (Elusione = annullare la probabilità di accadimento)
- **Prevenire** il rischio (Prevenzione = ridurre la probabilità di accadimento)
- **Proteggere** il rischio (Protezione = ridurre le conseguenze/la gravità dell'impatto
- **Trasferire** il rischio (Trasferimento del rischio a fornitori o terzi, es. Assicurazione)
- **Accettare** il rischio (Ritenzione = assunzione diretta e completa del rischio)

Valutazione dei rischi in pratica

- Identificare i rischi significativi per ogni processo: analisi di minacce ed opportunità ed individuazione delle vulnerabilità
- Alcuni rischi sono trasversali a più processi (rischio ICT, calamità naturali, ecc.)
- Attribuire un valore quali-quantitativo alla probabilità di accadimento dell'evento (il rischio si realizza se una minaccia si concretizza perché può sfruttare una vulnerabilità)
- Attribuire un valore quali-quantitativo alla gravità delle conseguenze dell'evento
- Calcolare il livello di rischio (Probabilità x Gravità)
- Definire le azioni di trattamento dei rischi ritenuti non accettabili

Esempio

Valutazione dei rischi

Rischi	Gravità delle conseguenze	Probabilità di accadimento	Misure di mitigazione	Indice di Rischio	Tipo azione	Azioni di trattamento
Accettare ordini per prodotti non fattibili o non rispondenti alle caratteristiche richieste dal cliente e dal mercato	5	2	1	10	Accettare	
Produrre prodotti con materiali non idonei – secondo normativa - a soddisfare le caratteristiche di durabilità e resistenza a rottura richieste	5	2	1	10	Accettare	
Concentrazione dei ricavi su pochi clienti	3	1	2	6	Accettare	
Obsolescenza delle scorte di magazzino materie prime	2	2	2	8	Accettare	
Indisponibilità di macchine per periodi prolungati causa rotture, mancanza parti di ricambio, ecc.	2	2	3	12	Accettare	
Indisponibilità di personale qualificato per condurre determinate macchine produttive	2	2	2	8	Accettare	
Produzione e vendita di pezzi non conformi che causano danni al cliente per errori al controllo in produzione e collaudo finale	5	1	2	10	Accettare	
Aumento dei prezzi della materia prima	2	2	3	12	Proteggere	
Indisponibilità di materia prima nei tempi richiesti per soddisfare le tempistiche di produzione richieste dal cliente	2	1	4	8	Accettare	
Blocco dei sistemi informativi	3	1	2	6	Accettare	
Personale insufficiente per entità e qualificazione per ricoprire ruoli gestionali-direttivi	3	1	2	6	Accettare	
Perdita di dati	3	2	3	18	Prevenire	
Perdita di riservatezza di informazioni legate al know-how aziendale, dati di clienti e di fornitori	2	2	2	8	Accettare	
Indicatori di misura dei processi errati o inaffidabili	3	2	3	18	Prevenire	
Rischi finanziari legati al credito (insoluti e ritardi di pagamento di pagamento)	2	2	2	8	Accettare	
Instabilità del mercato	2	2	1	4	Accettare	
Crisi economico-finanziaria dei clienti	1	2	2	4	Accettare	
Inaccessibilità/Inagibilità della sede a causa di disastri naturali e non	2	2	1	4	Accettare	
Rischio X	5	1	2	10		

Grazie per l'attenzione

Fabrizio Di Crosta

fabrizio@dicrosta.it

www.dicrosta.it