Risk Management: gestione del rischio, misurazione e analisi aziendale.

Indice

Che cos'è il Risk Management? (Gestione del Rischio)

La definizione di **Risk Management**, o **Gestione del Rischio** è: un processo di azioni e attività messe in atto dalle aziende per identificare i rischi e sviluppare strategie al fine di poterli mitigare e controllare.
Il rischio è intrinseco nell'azienda e dipende da fattori disparati, sia interni che esterni. Una corretta attività di **Gestione del Rischio** (**Risk Management**) permette di gestirlo e controllarlo al fine di preservare l'organizzazione e continuare a generare valore.
Il **Risk Management** è un processo che coinvolge tutti i processi aziendali e per essere efficace deve essere integrato nella cultura dell'organizzazione, diventando quindi parte integrante dei processi.

DEFINIZIONE DI RISCHIO

"Effetto dell'Incertezza in relazione agli obiettivi" – Normativa UNI EN ISO 31000
L'effetto di cui parla la definizione è semplicemente un risultato diverso da quello atteso e può essere sia negativo che positivo e può in seguito creare in cascata successive opportunità e minacce.
Il rischio è espresso in fonti di rischio (elementi che possono originarlo), eventi (verificarsi di circostanze) e conseguenze (esito dell'evento che influenza l'obiettivo).

Che benefici porta il risk management in azienda?

Il **Risk Management** porta in azienda numerosi benefici, legati sia alla comprensione del funzionamento dei processi che alla creazione e protezione del valore aziendale.
Benefici legati alla comprensione dei processi aziendali

- Pianificazione di tutte le reali priorità
- Comprensione di come l'impresa è strutturata, dei punti di forza e dei punti deboli
- Allocazione più efficace delle risorse e del capitale in azienda
- Miglioramento dei processi decisionali

Benefici legati alla creazione e protezione del valore aziendale

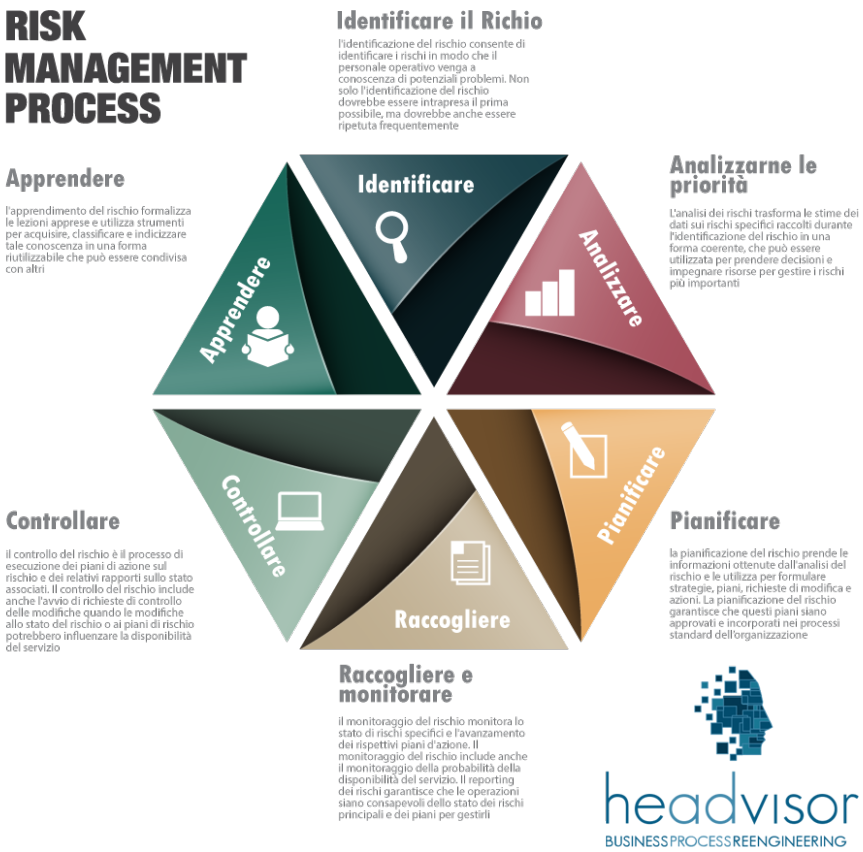
- Miglioramento della reputazione e dell'immagine aziendale
- Protezione del patrimonio e del know how
- Aumento dell'efficienza operativa

I 2 principali approcci (molto simili) alla gestione del rischio

Il **Risk Management** non è un insieme di azioni estemporanee fatte da persone disparate in azienda. È un processo organizzato e continuativo, che deve essere stabilito da esperti e portato avanti da tutto il personale aziendale, in ogni processo fatto.

Le 6 fasi del Risk Management Process

1. Identificare il rischio
2. Analizzare le priorità
3. Pianificazione
4. Monitoraggio
5. Controllo del rischio
6. Apprendimento



1. Identificare il rischio

L'identificazione del rischio consente di identificare i rischi in modo che il personale operativo venga a conoscenza di potenziali problemi.
Serve una cultura condivisa nell'identificazione di punti di fragilità o debolezza nei processi o nello svolgimento del lavoro.
Non solo l'analisi dell'identificazione del rischio dovrebbe essere intrapresa frequentemente e tempestivamente comunicata ai responsabili del **Risk Management**

2. Analizzare le priorità

L'analisi dei rischi trasforma le stime dei dati sui rischi specifici raccolti durante l'identificazione del rischio in una forma coerente, che può essere utilizzata per prendere decisioni e impegnare risorse per gestire i rischi più importanti
Vengono prese iniziative di **Gestione del Rischio** sulla base di valutazioni e priorità di gravità

3. Pianificare

La pianificazione del rischio prende le informazioni ottenute dall'analisi del rischio e le utilizza per formulare strategie, piani, richieste di modifica e azioni.
La pianificazione del rischio garantisce che questi piani siano approvati e incorporati nei processi standard dell'organizzazione

4. Raccogliere e monitorare

Il monitoraggio del rischio monitora lo stato di rischi specifici e l'avanzamento dei rispettivi piani d'azione. Il monitoraggio del rischio include anche il monitoraggio della probabilità della disponibilità del servizio.
Il reporting dei rischi garantisce che le operazioni siano consapevoli dello stato dei rischi principali e dei piani per gestirli

5. Controllare

Il controllo del rischio è il processo di esecuzione dei piani di azione sul rischio e dei relativi rapporti sullo stato associati.
Il controllo del rischio include anche l'avvio di richieste di controllo delle modifiche quando le modifiche allo stato del rischio o ai piani di rischio potrebbero influenzarne il servizio o il processo

6. Apprendere

L'apprendimento del rischio formalizza le conoscenze acquisite e utilizza strumenti per mantenere, classificare e indicizzare tale apprendimento in una forma riutilizzabile che possa essere condivisa con altri nel futuro.

Le 4 fasi di Gestione del rischio (Risk Management) secondo la norma UNI EN ISO 31000

I processi di **Risk Management** sono composti da 6 passaggi principali (quattro per la norma ISO 31000), che si ripetono in modo circolare:

1. Individuazione del rischio
2. Quantificazione del rischio
3. Valutazione del rischio
4. Controllo del rischio

1. Individuazione del Rischio (UNI EN ISO 31000)

La prima fase è l'individuazione e la catalogazione dei rischi per area di rischio, aggiungendo ad ognuno una descrizione qualitativa. L'individuazione dei rischi può essere fatta sull'intera azienda o su un singolo processo, in base alle necessità aziendali.
Chi si occupa di fare l'individuazione del rischio?
Idealmente in questa fase devono partecipare tutte le persone interessate: i dipendenti, i manager e gli esperti di valutazione del rischio, per essere sicuri di non aver mancato nulla. Servirà inoltre consultare tutti i dati e la documentazione disponibili.
Idealmente alla fine di questa fase sarà disponibile un report dei rischi completo e dettagliato.

2. Quantificazione del Rischio

La fase di quantificazione del rischio si occupa di valutare i singoli rischi, uno ad uno, per quanto riguarda la probabilità ("likehood" termine inglese utilizzato molto nel contesto risk management) che si concretizzino, oltre che le potenziali conseguenze di questa concretizzazione.
Una volta valutati i rischi singolarmente sarà necessario valutare quali conseguenze possono avere nel corso del tempo i rischi correlati tra loro o sovrapposti (= analisi dell'aggregazione del rischio).
I metodi di analisi e quantificazione del rischio dipendono dalla tipologia di azienda e di progetto, oltre che dall'approccio scelto dai consulenti aziendali, anche in base ai **KRI (Key Risk Indicator)** individuati.

3. Valutazione del rischio

La valutazione del rischio si compone di tutte le attività e le iniziative che l'azienda può mettere in campo per rispondere a tutti i rischi individuati. L'elenco di queste misure è fatto nel dettaglio e può riguardare sia misure specifiche per rischi specifici che misure generiche adattabili a vari rischi.
Le iniziative per ridurre il rischio si possono dividere in: reazioni attive preventive e reazioni passive correttive.
Una reazione attiva preventiva riduce la possibilità che si verifichi un rischio agendo sulle cause di esso (ad esempio migliorare un prodotto, riducendo i rischi di responsabilità). Una reazione passiva correttiva è invece dedicata a trasferire ad un altro soggetto le conseguenze dell'insorgenza del rischio (ad esempio sottoscrivere un'assicurazione).
Anche dopo tutte le misure che un'azienda mette in campo per evitare le conseguenze del rischio rimane comunque un rischio residuale, ovvero la possibilità che l'azienda subisca le conseguenze di un rischio nonostante le misure di controllo e prevenzione adottate.

4. Controllo del rischio

In quest'ambito si verificano l'efficienza e l'efficacia dei metodi applicati per la gestione del rischio, che sono diversi in base al tipo di rischio e alla tipologia di azienda/prodotto/progetto.

Bonus: Three Lines of Defense: Risk Management e il modello a tre linee di difesa

Il processo di **Gestione dei Rischi** per un'azienda non può (e non deve) essere interamente responsabilità di una singola persona, ma deve diventare un obiettivo condiviso da tutto il personale.
Il sistema Three Lines of Defense permette di istituire un sistema in cui tre separati "livelli" dell'azienda agiscono controllando il rischio e supervisionandosi tra loro, in modo da riuscire a prevenire, per quanto possibile, l'errore umano.

- **Prima linea**: i manager, capi reparto e gli addetti devono inserire la gestione del rischio nel proprio processo decisionale secondo le strategie fissate, devono inoltre assicurarsi che la seconda linea agisca in modo conforme al processo di **Risk Management**;
- **Seconda linea**: i lavoratori e gli operai a cui sono affidati i compiti devono svolgerli tenendo presente le logiche di **Risk Management**, assicurandosi che la prima linea prenda decisioni coerenti con esse;
- **Terza linea**: un soggetto indipendente, spesso esterno, vigila sulla prima e seconda linea periodicamente, assicurandosi che il processo di **risk management** sia attuato correttamente dalle parti;

Strategie e metodi per raccogliere eventi critici nel risk management

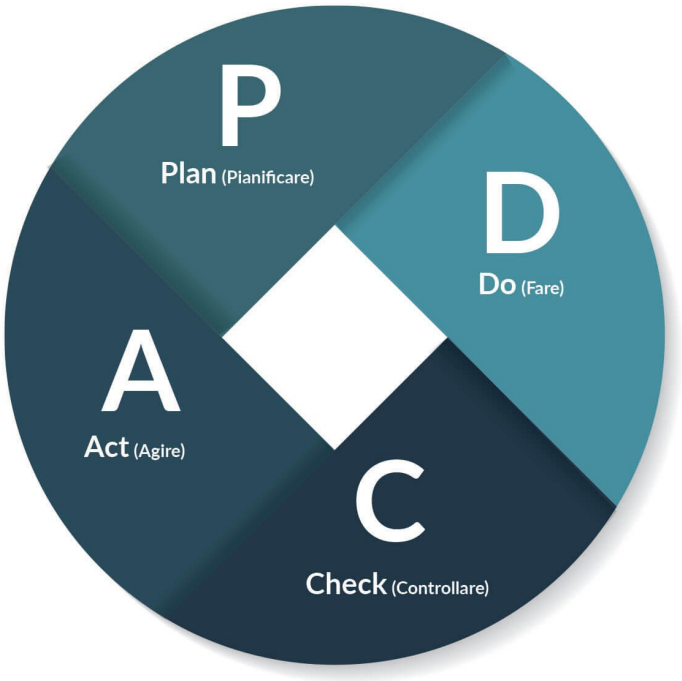
1. Brainstorming
2. Interviste strutturata o semi strutturata
3. Metodo Delphi
4. Audit con Checklist
5. Analisi preliminare dei rischi (PHA)
6. Hazard and operability study (HAZOP)
7. Hazard analysis and critical control points (HACCP)
8. Valutazione della tossicità
9. Tecnica strutturata "What If"
10. Analisi degli scenari
11. Analisi dell'impatto di business
12. Root causes Analysis (Analisi delle cause radice)
13. Failure mode and effects analysis (FMEA)
14. Analisi dell'albero degli errori
15. Analisi dell'albero degli eventi
16. Analisi causa e conseguenze
17. Analisi causa ed effetto
18. Analisi degli strati di protezione (LOPA)
19. Albero delle decisioni
20. Analisi dell'affidabilità umana (HRA)
21. Bowtie Analysis (Analisi della cravatta a farfalla)
22. Manutenzione dell'affidabilità centrata
23. Analisi dei circuiti nascosti
24. Analisi di Markov

Kaizen per il Risk Management

Il sistema Kaizen introduce il miglioramento continuo inteso come sistema di gestione della produzione in ottica Lean Production, ma è facilmente adattabile anche ai sistemi di **Risk Management**, in quanto è una filosofia di pensiero e non un insieme di norme prestabilite e immutabili.
La filosofia kaizen utilizza il ciclo di Deming o Ciclo PDCA per impostare un circolo di miglioramento continuo. Il Kaizen chiede di mettere in moto un processo di costante messa in discussione dello status quo aziendale, e quindi anche dello stato della **Gestione dei Rischi**, che porta alla verifica e al miglioramento del sistema di **Risk Management**.

Ciclo di Deming o Ciclo PDCA (Plan, Do, Check, Act)

Il **Ciclo PDCA** è un modello per il miglioramento continuo dei processi, atto ad aumentare e garantire la qualità e il valore in azienda.
Nel **Risk Management** questo modello, insieme alla **filosofia giapponese Kaizen**, si pone come sistema per implementare in azienda la filosofia del miglioramento continuo, in linea anche con la certificazione UNI EN ISO 31000.
Il **Ciclo di Deming** è diviso in 4 fasi che formano un processo ciclico:



1 Plan o Pianificazione

Quali sono i rischi aziendali? Il primo passo è identificare i rischi e catalogarli, in modo da avere un quadro chiaro sulla situazione aziendale.
Delineare i rischi permette di determinare come gestirli e ridurne i possibili effetti negativi. Non solo, in questa fase si valutano le possibil strategie di **Risk Management** da mettere in atto, per considerare quale è la più appropriata e quali sono le possibili conseguenze.
Questa pianificazione approfondita è seguita dalla fase 2: Implementazione

2 Do o Implementazione

Durante la fase di implementazione delle soluzioni di **Gestione dei Rischi** la cosa migliore è procedere a piccoli passi, implementando e mettendo in discussione le implementazioni, per assicurarsi di aver fatto le scelte giuste.
Questa seconda fase è una fase di test: serve ad accumulare esperienza e migliorare le proprie capacità come **Risk Management**, oltre alle capacità di tutti i dipendenti aziendali. La fase di implementazione può dare informazioni molto interessanti nell'ambito rischi, perché può evidenziarne di nuovi non considerati in fase di analisi e pianificazione.

3 Check o Verifica

Nella fase di verifica vengono presi tutti i problemi della fase di Implementazione e vengono analizzati, per scoprirne i punti deboli e correggerli.

4 Act o Azione

Una volta che i problemi sono noti e sono state individuate le cause della debolezza del processo di **Risk Management** si può procedere a correggerli e installare un sistema di controllo basato sullo schema PDCA.

Gli ambiti di rischio aziendale: Cyber Security

Il **risk management** nella cyber security è un processo molto importante ma anche molto complesso, in quanto è influenzato da una moltitudine di fattori, tra cui il fattore umano (più imprevedibile).
In che cosa consiste la gestione del rischio in ambito cybersecurity?
Il dipartimento IT (o l'addetto IT nelle piccole aziende) impiega una combinazione di software, strategie e corsi di formazione del personale per minimizzare i rischi legati alla rete. Ma piano piano che internet diventa una parte sempre più grande della vita aziendale (specialmente con l'integrazione dello smart working) i rischi aumentano e diventa necessario un intervento più profondo.
Ma come si gestisce il rischio in ambito cybersecurity?
Nello stesso modo in cui si gestisce negli altri ambiti aziendali: tramite una seria e approfondita analisi dei rischi possibili e una serie di misure, sia attive che passive, per evitare che i rischi si concretizzino e minimizzandone le conseguenze.

Valutazione dei rischi nell'ambito cybersecurity

Prima di creare un sistema di **risk management** è importante procedere con l'identificazione, l'analisi e la classificazione dei rischi legati all'ambito cybersecurity. Infatti solo basandosi sugli effettivi rischi aziendali è possibile stendere un programma di **risk management** efficaci.
La valutazione dei rischi di cyber security è facilitata dalla grande quantità di materiale disponibile relativo ai rischi e al funzionamento del sistema IT aziendale.
C'è da considerare che ogni parte dell'azienda gestita in modo informatico (sito web, ordini online ma anche ERP e sistemi digitali per gestire le informazioni) rappresentano un rischio intrinseco per l'azienda, che aumenta più sono "aperti" (ovvero più le persone esterne all'azienda possono interagire con essi).

Le strategie per il controllo dei rischi in ambito Cyber Security

1. **Formazione**
   Il processo di formazione è molto importante se si vogliono mitigare le possibilità che un rischio di cybersecurity accada. Questo perché, soprattutto negli ultimi anni, una delle ragioni per cui questi rischi accadono è proprio l'errore umano. Migliorare la formazione di tutto il personale permetterà quindi di ridurre le possibilità che il rischio accada.
2. **Sistemi di protezione**
   I sistemi di protezione, come antivirus e software preposti, possono essere molto utili se gestiti nel modo corretto dal dipartimento IT.

3. **Miglioramento continuo**
   Solo un sistema di miglioramento continuo può garantire veramente la diminuzione del rischio in ambito cyber security: le soluzioni prese infatti non possono essere installate e dimenticate, ma devono essere costantemente aggiornate e messe alla prova per garantire un corretto sistema di **Risk Management**

La normativa UNI EN ISO 31000 e la gestione del rischio

La norma UNI EN ISO 31000 è una normativa destinata ai gestori del rischio di qualunque attività, sia pubblica che privata, che necessitano di gestire tutti gli eventi che possano in qualche modo limitare o impattare sulla capacità di creare prodotti/erogare servizi.
Lo scopo di questa norma è fornire uno standard (e uno schema organizzativo) che permette di definire e adottare una modalità uguale per tutti per definire gli interventi volti a prevenire/mitigare gli effetti del rischio.
La norma UNI EN ISO 31000 fornisce inoltre un elenco di soluzioni riconosciute per la gestione del rischio, strumenti utili alle aziende per mettere in campo il processo di **Risk Management**.

Normativa UNI EN ISO 31000: I principi

Nella sezione "I principi" la norma UNI EN ISO 31000 descrive dettagliatamente una guida sulle caratteristiche di una **Gestione del Rischio** efficace e efficiente. Spesso le aziende che si approcciano al **Risk Management** considerano approfonditamente i dettagli dei rischi aziendali e ignorano, dando per scontate, le caratteristiche che il sistema di Contenimento dei Rischi sviluppato deve avere.
La norma UNI EN ISO 31000 identifica 8 principi su cui deve essere basato un sistema di **Risk Management** efficace. Una **Gestione del Rischio** deve essere:

1. Integrata
2. Strutturata e globale
3. Personalizzata
4. Inclusiva
5. Dinamica
6. Basata sui dati
7. Basata sul comportamento umano
8. Orientata al Miglioramento Continuo

La certificazione UNI EN ISO 31000: cosa certifica e chi sono gli enti certificatori

Per ottenere la certificazione UNI EN ISO 31000 è necessario implementare i principi e le linee guida della normativa, in ogni area della propria attività.
Per ottenere la certificazione è poi necessario rivolgersi ad un ente certificatore, che compirà un Audit indipendente dell'azienda.