Riassunto libro Tsiouras

Analisi E Gestione Del Rischio (Università degli Studi di Milano)

Ioannis Tsiouras-Risk management la norma ISO 31000-2018

Le organizzazioni possono far fronte a delle incertezze, le quali possono causare dei rischi in contesti esterni o interni, questi rischi hanno un impatto sul raggiungimento degli obiettivi e possono mettere a repentaglio il business.
Le organizzazioni quindi analizzano i rischi e adottano approcci più o meno conosciuti ed efficaci.
Per affrontare questi rischi in modo sistematico, efficace ed efficiente il normatore ISO (international organization for standardization) ha emesso una serie di normative per il risk management, di cui la principale è la ISO 31000. (ha emesso anche la ISO/IEC Guide 73)

L'uomo gestisce il rischio sia in modo consapevole (stabilisce approcci strutturati e li applica) che inconsapevole, la gestione del rischio è vitale per l'uomo.
Quando si prende una decisione, solitamente questa viene presa in modo istintivo (raramente in modo sistematico), segue una definizione degli obiettivi con una stima delle conseguenze, gli obiettivi vengono confrontati coi risultati delle conseguenze dell'azione e successivamente si può decidere.
Nella fase di confronto tra gli obiettivi e le conseguenze stimate si possono creare degli scostamenti, questo fa si che ci siano delle modifiche alle azioni da compiere. La valutazione comprende diversi scenari, si deve quindi scegliere lo scenario che contiene meno incertezze e minor rischio.
L'incertezza è dovuta alla mancanza della "conoscenza assoluta" della situazione a cui ci si riferisce, anche se si approfondisce qualcosa non si riuscirà mai ad avere una conoscenza assoluta e quindi ci sarà sempre la presenza di un'incertezza.

La norma ISO/IEC Guide 73 fornisce un vocabolario base dei termini del risk management per aiutare le organizzazioni a comprendere meglio e aumentare la consapevolezza in ambito di risk assessment.

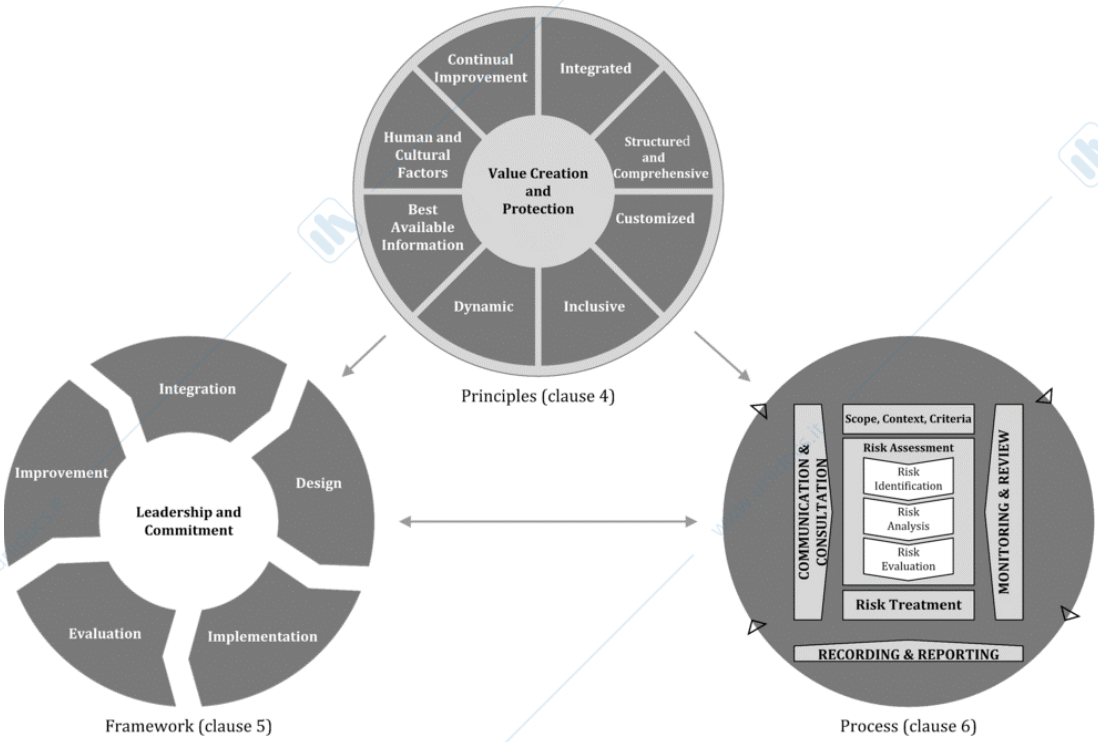
La ISO 31000:2018 (il cui titolo è *Risk management-Guidelines*) è una normativa che può essere applicabile a tutte le tipologie di organizzazioni (manifatturiere, commerciali, di servizi, organizzazioni governative) di qualsiasi dimensione. Può essere anche applicata a qualsiasi contesto che abbia bisogno di una gestione del rischio.
La ISO 31000 è una linea guida che propone un framework per il risk management senza esporre in modo approfondito i concetti e senza fornire un supporto operativo, da solo indicazioni di massima.
La norma potrebbe essere adottata per impostare il framework per il risk management ed il processo di risk management. Essendo una linea guida, quanto è scritto nella norma non è un requisito, quindi non può essere utilizzata per effettuare audit o per emettere certificazioni.
Il risk management può essere applicato a tutta l'organizzazione ma anche ad un singolo processo, una singola attività. Può essere applicato anche a più livelli (strategico, gestionale o tattico, operativo).
Il successo della gestione dei rischi dipende dall'efficacia della gestione del framework per il risk management. Il framework gestisce la struttura e fornisce le risorse necessarie per l'integrazione coi processi dell'organizzazione.
L'applicazione efficace del processo di risk management dipende da alcuni fattori chiave, come la definizione del contesto di applicazione e del campo di applicazione (estensione dei confini del processo, comprende l'identificazione completa delle "parti interessate" o stakeholder e delle loro esigenze, aspettative e requisiti, comprende gli obiettivi da soddisfare e i criteri per l'accettazione dei rischi).
I benefici di una corretta applicazione del framework sono elencati nella norma ISO 31000.
Alcuni elencati qui sotto:

1. Aumenta la probabilità di raggiungere gli obiettivi
2. Incoraggia la gestione proattiva
3. Aumenta la consapevolezza sulla necessità dell'identificazione e della gestione dei rischi
4. Assicura la soddisfazione dei requisiti legali e regolamentari, come anche i requisiti delle norme sui sistemi di gestione (ISO 9001, ISO 14001, ISO 22301, ISO 27001, e altre)

5. Migliora la confidenza e la fiducia degli stakeholder
6. Migliora l'applicazione dei controlli
7. Migliora l'allocazione e l'utilizzo efficace delle risorse
8. Migliora l'efficacia e l'efficienza operativa
9. Migliora la prevenzione e la gestione degli incidenti

La governance guida l'organizzazione, le sue relazioni con il mondo esterno e nel mondo interno, le regole, i processi, gli approcci e le pratiche necessari per raggiungere i suoi obiettivi.
La risk governance è il modo in cui l'organizzazione gestisce i rischi che incontra, è dunque un'impostazione strategica dei processi di risk management e decision making.
Generalmente la governance si riferisce alle azioni, processi, practices e approcci attraverso i quali il management opera, controlla, prende decisioni e le mette in atto.
Il risk governance è la struttura di governo per:

- Stabilire i principi per la gestione dei rischi
- Creare e gestire il framework necessario per effettuare il deployment dei principi su tutti i processi dell'organizzazione
- Rendere applicabile e gestire con efficacia il processo di risk management



Il rischio da un punto di vista filosofico e antropologico è inevitabile ma sotto un apparente controllo può essere dominabile. Anche da un punto di vista ingegneristico il rischio non è del tutto eliminabile ma si può controllare e ridurre. Il termine "rischio", in letteratura tecnica è una "condizione o situazione che può causare eventi sfavorevoli". Nella norma ISO 31000 il rischio è espresso in termini di fonti di pericolo e di potenziali eventi favorevoli e sfavorevoli. Gli eventi sfavorevoli possono portare a danni (non è detto, sicuramente sono un pericolo ma non è detto che portino a danni) mentre quelli favorevoli ad opportunità e possono portare al raggiungimento dell'obiettivo. Se un evento pericoloso possiede la potenzialità di causare danno, il rischio è legato alla probabilità (o alla frequenza) del verificarsi dell'evento sfavorevole e della severità (magnitudo) delle sue conseguenze.
Pertanto, con "analisi del rischio" si intende l'individuazione delle cause di un evento e delle sue conseguenze.

Il rischio è legato all'incertezza di un evento, questa aumenta con la crescita della complessità della situazione e in questi casi bisogna ridurre al minimo gli approcci intuitivi e adottare degli approcci sistematici e strutturati (organizzativo-ingegneristici).
La definizione di rischio che viene presa in considerazione è quella della ISO Guide 73, che definisce il rischio come l'effetto dell'incertezza sugli obiettivi.
La definizione è composta dai 3 termini chiave: effetto, incertezza e obiettivi.

- Effetto: deviazione rispetto alle aspettative (positivo o negativo, può portare a minacce o opportunità)
- Incertezza: legata alla conoscenza di un processo, un'entità, un evento o di una situazione
- Obiettivi:
    - Riguardare ambiti diversi
    - Essere applicati a diversi livelli
    - Essere espressi come risultati desiderati, come scopo o come un criterio

Il rischio è legato al grado di esposizione dell'obiettivo all'incertezza della situazione. Il rischio dipende da questi due elementi:

- Dall'incertezza, intesa come conoscenza di un evento e delle relative condizioni di contorno
- Dall'esposizione dell'obiettivo all'incertezza, intesa come impatto, magnitudo.
  L'impatto può essere:
    - Totale: l'obiettivo non si raggiunge per niente. Danno 100%
    - Parziale: la perdita dell'obiettivo è solo parziale

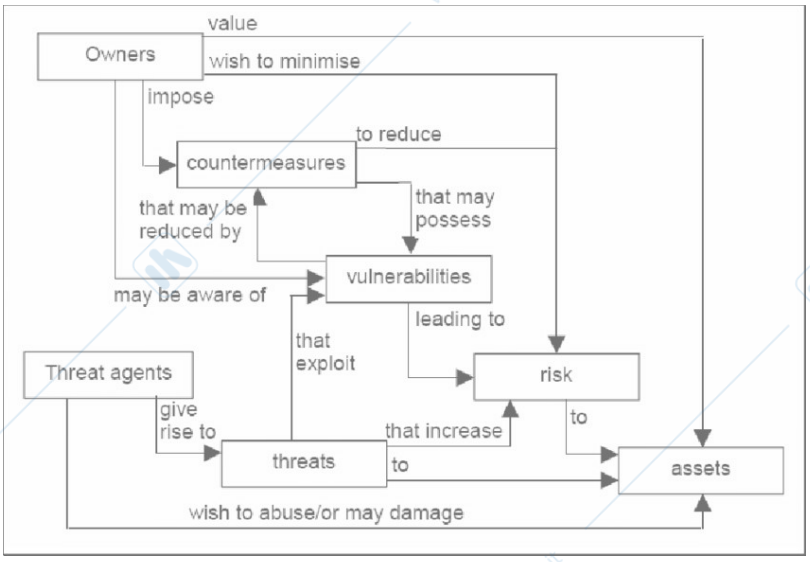
Il rischio dipende quindi dall'interazione tra la fonte di pericolo e l'esposizione dell'obiettivo (Bene) alla fonte di pericolo. La presenza di entrambi può provocare un impatto.
Pertanto, possiamo esprimere l'Entità di Rischio (R) con la seguente formula:

$$R = f(P, D)$$

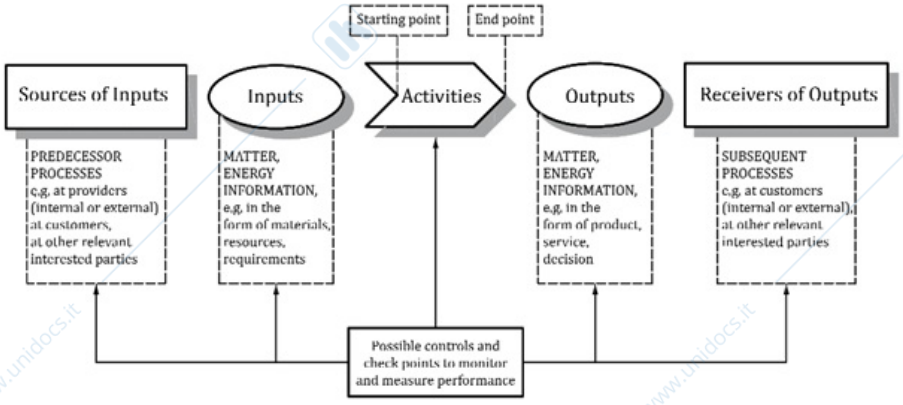
P = probabilità o frequenza dell'incidente
D = legato alle conseguenze (impatto)
f = funzione scelta per combinare P e D, dipende dal modello scelto per l'analisi del rischio

Se si conosce il valore dell'obiettivo in una situazione normale e si conoscono le minacce che incombono su di esso, è possibile stimare il rischio e decidere opportunamente, intraprendendo misure (controlli) per salvaguardare il bene e quindi raggiungere l'obiettivo.
Quasi in tutte le situazioni un obiettivo ha un proprietario, che si preoccupa di soddisfarlo. Per assicurare il raggiungimento dell'obiettivo (con un rischio naturale, in quanto il rischio non è mai pari a 0) è necessario analizzare il contesto in cui si opera, identificare i fattori che possono provocare ostacoli e agire di conseguenza.
Il ruolo del proprietario è critico, in quanto è sua responsabilità attribuire un valore all'obiettivo e scegliere la strada migliore per raggiungerlo. Le entità e i comportamenti da analizzare sono:

1. L'obiettivo, che deve essere soddisfatto
2. Il proprietario dell'obiettivo
3. Le fonti di pericolo (agenti portatori di minacce)
4. Le vulnerabilità (debolezze) che possono essere esplorate dalle minacce
5. Le minacce, sollevate dalle fonti di pericolo, che possono esplorare le vulnerabilità
6. Le misure (controlli) che il proprietario deve adottare per ridurre al minimo i rischi

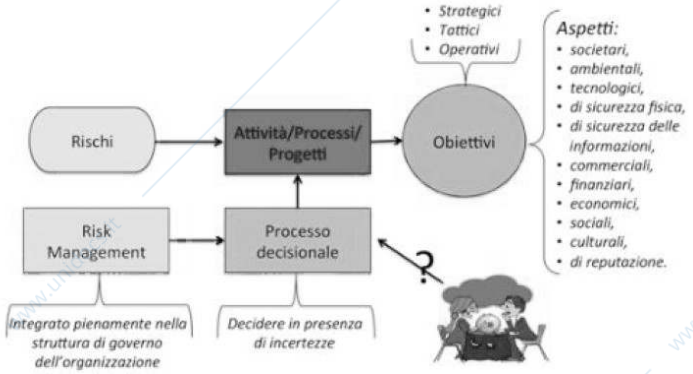


Esistono sempre fonti di pericolo che attraverso agenti possono portare a minacce.
Il numero e la tipologia delle minacce variano nel tempo e sono parzialmente note, anche le vulnerabilità presenti nel contesto dell'obiettivo variano nel tempo e sono note parzialmente.
Le minacce e le vulnerabilità sono parametri probabilistici, si sviluppano con una certa probabilità o frequenza.
Poiché l'incidente dipende da questi parametri è anch'esso un evento probabilistico.
Le norme sui sistemi di gestione richiedono che l'organizzazione conosca bene il proprio contesto e identifichi i fattori di rischio che possono portare ad eventi negativi e anche quelli che possono portare ad eventi positivi.
Il risk-based thinking spinge l'organizzazione a stabilire un approccio sistemico e preventivo per affrontare i fattori di rischio, limitare le conseguenze negative e aumentare quelle positive. Per fare questo bisogna accertare, valutare e trattare in modo continuo i fattori di rischio.
Qualora la situazione permettesse di raccogliere dati e procedere all'analisi e alla valutazione del rischio si può procedere come nel CASO DI STUDIO 1.
Qualora la situazione non permettesse di raccogliere dati, la metodologia potrebbe essere eseguita con meno rigore facendo una valutazione qualitativa e non quantitativa come nel CASO DI STUDIO 2.
I vantaggi che si ottengono con l'approccio per i processi (capacità di concentrarsi sui processi chiave e sulle opportunità) si moltiplicano se viene integrato il risk-based thinking.
L'approccio per i processi permette la definizione degli obiettivi, delle responsabilità e delle autorità sul processo, contribuisce alla conoscenza del processo e delle sue risorse, permette di individuare le interdipendenze con gli altri processi e di assicurarne la gestione efficace ed efficiente, il risk-based thinking aumenta la probabilità che tutto questo accada.



Il risk-based thinking considera il rischio parte integrante dei processi, del sistema di gestione e del modo di prendere una decisione. La gestione del rischio è quindi un modo per gestire i processi, le attività, l'organizzazione.
Con questo pensiero basato sul rischio la gestione delle situazioni indesiderate diventa proattiva e non reattiva.

Il processo per la gestione dei rischi è il risk management che supporta ogni manager a prendere decisioni in presenza di incertezze.



Le decisioni prese in qualsiasi livello di importanza e di significatività hanno un impatto sul raggiungimento degli obiettivi e sono caratterizzate da un grado di incertezza, questo avviene perché le decisioni si prendono in base alla conoscenza che si ha della situazione e del suo contorno e questa non è mai totale.
Il grado di incertezza dipende dalla qualità, quantità, dall'integrità (completezza) e dalla provenienza delle informazioni. Non sempre i dati sono disponibili per fare previsioni e nei casi in cui non lo sono è impossibile identificare i rischi e si è costretti a prendere decisioni in assenza di informazioni.
Se il risk management è integrato nell'organizzazione si nota dal linguaggio parlato e scritto dei manager, nella formulazione delle politiche, degli obiettivi e nella gestione dei processi, delle attività.
Gli auditor, persone incaricate di valutare l'efficacia del processo di risk management, cercano evidenze sul grado di integrazione di questo processo con il processo decisionale. Queste evidenze vengono cercate durante le interviste con i manager e con la valutazione del loro impegno.
Le conseguenze dell'incertezza legata al concetto di rischio riguardano la percezione, la consapevolezza e l'accettabilità di questo. La percezione del rischio dipende da molteplici fattori non quantificabili né perfettamente identificabili quali il contesto culturale, sociale, ideologico e fattori soggettivi, psicologici ed emotivi.
La percezione e la consapevolezza sono elementi essenziali per il processo decisionale, l'accettabilità è un problema più complesso e dipende dalla libertà di scelta e dalla valutazione del rapporto costi/benefici.
Un'organizzazione per avere successo dovrebbe essere gestita attraverso la risk governance, che dovrebbe essere gestita in modo sistematico e trasparente. La norma ISO 31000 ha individuato otto principi che possono essere utilizzati per migliorare le prestazioni, l'efficacia e l'efficienza del risk management.
La creazione di valore e la sua protezione costituiscono la "vision" del risk management (crea valore attraverso il raggiungimento degli obiettivi e il miglioramento delle performance).

figura 2 Principi

Il risk management è parte integrante dei processi e delle attività dell'organizzazione, è una delle responsabilità della direzione.
L'efficacia del processo decisionale dipende dalle decisioni elementari che vengono prese ai vari livelli, queste decisioni elementari dipendono da chi decide e dalla condizione d'incertezza in cui queste vengono prese. Le scelte e le decisioni prese dal manager dipendono molto dalla conoscenza al contorno che si ha della situazione in merito. Il risk management aiuta a fare scelte consapevoli.
Gli elementi di input del processo di gestione del rischio devono basarsi su informazioni accertate. Il processo di risk management è un processo che va personalizzato in base ad ogni organizzazione e ai rischi che corre. Il coinvolgimento degli stakeholder è molto importante, assicura che la gestione dei rischi rimanga aggiornata e permette di avere i loro punti di vista.
Il risk management sente e risponde al cambiamento continuo, questo è un obiettivo permanente e i miglioramenti ottenuti dovrebbero essere comunicati e pubblicati.

Il framework (infrastruttura) permette di integrare il processo del risk management nel sistema di gestione aziendale, l'integrazione dovrebbe avvenire per ogni contesto e livello (strategico, tattico, operativo).
L'impostazione del framework dovrebbe seguire l'approccio Plan-Do-Check-Act (non viene esplicitamente richiamato nella ISO 31000 ma è evidente che segua questo approccio).

PLAN (stabilire)	Progettare il framework
DO (fare)	Implementare il framework e applicare il processo di risk management
CHECK (monitorare e riesaminare)	Monitorare e riesaminare il framework e il processo di risk management
ACT (mantenere e migliorare)	Mantenere e migliorare il framework

Tutti i ruoli rilevanti nell'organizzazione dovrebbero essere legati da una forte leadership riguardo al risk management e dimostrarlo con la crescita delle persone e dei gruppi nell'ambito del risk management.
L'alta direzione per dimostrare l'impegno dovrebbe:

- Stabilire e approvare la policy per il risk management
- Assicurare che la policy sia compatibile con la direzione strategica dell'organizzazione
- Assicurare che la policy sia allineata alla cultura dell'organizzazione
- Assegnare ruoli, responsabilità e autorità ai livelli dell'organizzazione per il risk management
- Assicurare l'integrazione del processo di risk management con i processi strategici, tattici e operativo
- Mettere a disposizione risorse adeguate per il risk management
- Stabilire indicatori per misurare le prestazioni del risk management
- Assicurare la soddisfazione dei requisiti legali e regolamentari
- Comunicare i benefici ottenuti a tutti gli stakeholder
- Assicurare la continua adeguatezza del framework per il risk management
- Promuovere il continuo miglioramento
- Dare supporto ai ruoli di responsabilità per dimostrare la loro leadership e il loro impegno

L'alta direzione dovrebbe:

- Definire i criteri e i livelli di accettazione dei rischi
- Condurre esami periodici per verificare l'adeguatezza, idoneità, efficacia ed efficienza del processo di risk management
- Dimostrare il suo impegno verso il miglioramento continuo

Prima di iniziare con qualsiasi attività di risk management è bene definire il contesto interno ed esterno dell'organizzazione, questo contesto è soggetto a continui cambiamenti quindi deve essere monitorato continuamente. Per capire il contesto è necessario approfondire:

Il contesto esterno nel quale l'organizzazione opera e affronta le sfide	L'analisi del contesto esterno dovrebbe prendere in considerazione: Nell'analisi del contesto esterno possono essere identificate varie situazioni critiche con incertezze di vario genere che possono sollevare rischi. Questi rischi devono essere gestiti seguendo il processo di risk management.
Il contesto interno dell'organizzazione	L'analisi del contesto interno dovrebbe prendere in considerazione: Nell'analisi del contesto interno possono essere identificate varie situazioni critiche con incertezze di vario genere che possono sollevare rischi. Questi rischi devono essere gestiti seguendo il processo di risk management.
Capire le esigenze e le aspettative degli Stakeholder	Durante l'analisi del contesto esterno e quello interno si identificano, come abbiamo visto, i relativi stakeholder (parti interessate). Per ogni stakeholder è necessario determinare le sue esigenze e aspettative e trasformarle in requisiti per l'organizzazione. Gli stakeholder, in funzione della loro importanza per il business dell'organizzazione, possono essere classificati in: forti, meno forti e deboli.
La metodologia per il risk management	La metodologia che viene usata per effettuare l'analisi, la valutazione e il trattamento dei rischi.
I criteri dei rischi	Rilevare e stabilire la propensione al rischio (risk appetite) dell'organizzazione e i criteri e i livelli di accettazione dei rischi.
Comunicazione	I canali che devono essere usati per comunicare con gli stakeholder interni ed esterni.

L'alta direzione dovrebbe definire l'impegno impiegato nel risk management attraverso una politica o un'altra dichiarazione.
L'impegno dovrebbe essere appropriato agli scopi dell'organizzazione, assicurare il collegamento tra gli obiettivi, le politiche operative e la politica per la gestione dei rischi, stabilire le responsabilità e le autorità

per la gestione dei rischi, mettere a disposizione le risorse necessarie, essere comunicato e pubblicato, essere disponibile agli stakeholder, definire il modo per gestire i conflitti di interesse, essere riesaminato per valutare la sua idoneità nel tempo. L'alta direzione dovrebbe rimarcare il fatto che il risk management è uno dei bisogni primari e definire i proprietari dei rischi (chi ha la responsabilità di prendere le decisioni). L'organizzazione dovrebbe offrire le risorse per la gestione del risk management e periodicamente controllare che le risorse siano adeguate e disponibili.

Gli argomenti che l'organizzazione dovrebbe prendere in considerazione possono essere almeno i seguenti:

- le risorse necessarie per ogni attività del risk management;
- i processi, i procedimenti, gli strumenti che dovranno essere usati nel risk management;
- le informazioni documentate (procedure, processi, approcci documentati);
- i piani per la formazione.

Il personale coinvolto nel processo di risk management deve possedere le conoscenze necessarie, questa competenza deve essere acquisita tramite un adeguato grado di istruzione, esperienza, abilità.
Per fare questo l'organizzazione dovrebbe:

- individuare e definire le competenze necessarie per il personale che svolge attività che impattano sul risk management;
- fornire l'addestramento o adottare altre azioni per soddisfare queste esigenze;
- valutare l'efficacia delle azioni intraprese;
- assicurare che il personale sia consapevole della rilevanza e dell'importanza delle proprie attività e di come esse contribuiscono al raggiungimento degli obiettivi del risk management;
- conservare le informazioni documentate sul grado di istruzione, sull'addestramento, sulle capacità e sull'esperienza del personale.

Il processo di risk management dovrebbe prevedere una continua comunicazione con gli stakeholder interni ed esterni, offrendo una gamma completa di rapporti sulle prestazioni della gestione dei rischi. La comunicazione dovrebbe essere impostata come un processo a due vie e per un'efficace comunicazione dovrebbero esserci frequenti report sulla gestione dei rischi e sul suo aggiornamento.

L'organizzazione dovrebbe determinare i canali di comunicazione e di reporting con gli stakeholder interni, per un'efficace comunicazione bisognerebbe implementare un piano. Il piano dovrebbe stabilire:

- Cosa comunicare (obiettivi, informazioni, risultati)
- Quando comunicare (quando preparare i report)
- Con chi comunicare (alta direzione, ruoli, dipendenti)
- Chi dovrebbe comunicare
- Le modalità di consultazione con gli stakeholder interni

L'organizzazione dovrebbe determinare anche i canali di comunicazione e di reporting con gli stakeholder esterni (ad esempio clienti, eventuali partner, la comunità locale, i media). Questa comunicazione diventa essenziale soprattutto in situazioni di crisi o in caso di eventi che possono mettere in difficoltà l'organizzazione. Anche in questo caso bisognerebbe implementare un piano, che stabilisce quello che deve essere comunicato agli stakeholder esterni e in quali occasioni. La comunicazione verso l'esterno dovrebbe essere fatta in modo da aumentare la fiducia degli stakeholder esterni nei confronti dell'organizzazione.

Per l'implementazione del framework si dovrebbe:

- definire una strategia compresi i tempi di implementazione;
- applicare la politica per la gestione dei rischi;
- assicurare la conformità ai requisiti di legge e ai requisiti regolamentari;
- assicurare l'allineamento del processo decisionale, compreso il processo di sviluppo e l'impostazione degli obiettivi con i risultati del processo di gestione dei rischi;
- pianificare ed erogare attività di addestramento e di formazione;
- mettere in atto attività per mantenere le competenze necessarie;
- comunicare e consultare gli stakeholder per assicurare l'adeguatezza del framework per la gestione dei rischi.

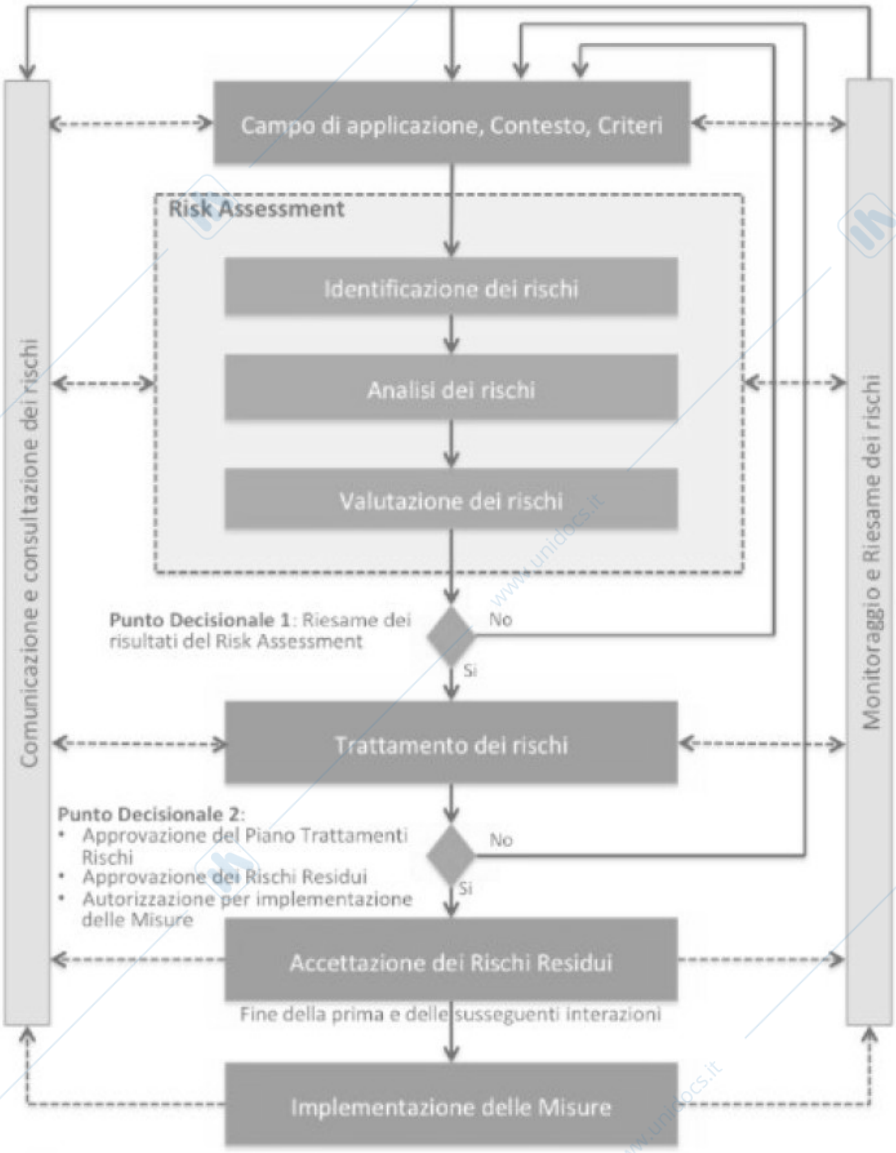
Ogni implementazione del processo è un'istanza, tutte le volte che viene implementato dovrebbe essere eseguito secondo un approccio stabilito.
Il processo di risk management dovrebbe produrre risultati consistenti, validi, ripetibili e comparabili e dovrebbe essere implementato a tutti i livelli dell'organizzazione e a tutte le funzioni.

Il processo del Risk Management:
Questo processo coinvolge in modo sistematico l'applicazione delle procedure, delle politiche e delle best practices nella comunicazione, nella consultazione, nella definizione di contesto, nella valutazione, nel monitoraggio, nel riesame, nella registrazione e nelle attività di reporting dei rischi.
Il processo di risk management è composto dalle seguenti fasi:

1. Comunicazione e consultazione
2. Campo di applicazione, contesto e criteri per il Risk Assessment
3. Risk Assessment:
    - Identificazione dei rischi
    - Analisi dei rischi
    - Valutazione dei rischi
4. Trattamento dei rischi
    - Selezione delle opzioni per il trattamento dei rischi
    - Identificazione delle misure da implementare
    - Identificazione delle misure esistenti
    - Calcolo dei rischi residui
    - Preparazione del piano trattamento dei rischi
5. Accettazione dei rischi
6. Implementazione delle misure
7. Monitoraggio e riesame
8. Registrazione e reporting

Ogni istanza è un'applicazione del processo, per trattare un determinato evento o fattore di rischio favorevole o sfavorevole.
La prima volta che viene applicato il processo di risk management i passaggi 1 e 7 vengono saltate, queste vengono fatte in modo continuo durante tutto il processo.
Lo scopo di queste attività di comunicazione e consultazione è quello di personalizzare il processo e di rendere efficace il Risk Assessment e il Risk Treatment, pertanto è necessario stabilire:

- Il campo di applicazione
- Il contesto (esterno e interno): stabilire i confini entro i quali verrà applicato il processo di risk management
- I criteri per la gestione dei rischi



La comprensione del contesto esterno è molto importante per verificare se gli obiettivi e gli stakeholder siano stati considerati in modo esaustivo. Il contesto esterno potrebbe includere:

- La situazione economica e finanziaria
- La posizione di mercato
- I clienti e requisiti contrattuali
- Il comportamento della concorrente a livello internazionale, nazionale e regionale
- Gli impegni e i rapporti col mondo esterno
- L'ambiente fisico
- La tecnologia, la connettività e la trasmissione dati
- L'ambiente culturale e sociale
- La gestione delle alleanze
- I fattori guida e le tendenze
- Le leggi per le associazioni di categoria
- Le relazioni con gli stakeholder, le loro percezioni e i loro valori
- La comunicazione con le autorità locali
- I subappaltori
- I vicini

Il contesto interno è invece quello nel quale si opera per soddisfare gli obiettivi, questo dovrebbe essere stabilito se no le organizzazioni non avendo un ambiente definito non riescono ad operare in modo concreto. Il contesto potrebbe includere:

- La governance, la struttura organizzativa, i ruoli, le responsabilità e i rapporti reciproci
- Le politiche, gli obiettivi e le strategie messe in atto per soddisfarli
- La capacità delle risorse, le conoscenze e le competenze
- I rapporti con gli stakeholder, le loro percezioni e i loro valori
- La cultura dell'organizzazione
- I sistemi informativi, i flussi di informazione e il processo decisionale formale e informale
- Le norme, le linee guida e i modelli a disposizione dell'organizzazione
- La forma ed estensione delle relazioni contrattuali

Il campo di applicazione del risk Management potrebbe occupare solo una parte dell'organizzazione, è pertanto molto importante definire questi confini entro i quali si vuole applicarlo.
Il campo di applicazione prende in considerazione i fattori identificati nel contesto interno ed esterno, i requisiti degli stakeholder, le leggi e i regolamenti applicabili, gli obiettivi da soddisfare, le strategie di applicazione e tutte le informazioni inerenti agli obiettivi.

Dopo aver analizzato il contesto interno ed esterno si procede con l'analisi

I risultati dell'analisi dovrebbero stabilire:

- l'estensione e i confini del contesto di applicazione del processo di Risk Management;
- le esigenze e le aspettative degli stakeholder e i requisiti di legge e dei regolamenti applicabili;
- i processi, le attività e i progetti, prodotti e servizi e beni coinvolti, le loro interfacce, interazioni e dipendenze, tempi, ubicazioni ed eventuali organizzazioni esterne coinvolte;
- i ruoli, le responsabilità, le autorità e i rapporti reciproci nell'ambito del processo di Risk Management;
- le risorse coinvolte (competenze, informazioni, infrastrutture e le tecnologie);
- l'approccio e la metodologia per il risk assessment e risk treatment;
- il modo di eseguire la valutazione della performance e dell'efficacia del Risk Management;
- i momenti decisionali e le modalità del processo decisionale;
- i criteri per la gestione dei rischi;
- le giustificazioni relative a eventuali esclusioni dal campo di applicazione.

L'esperienza vede due approcci possibili per il risk assessment:

- L'approccio analitico
- L'approccio empirico, che usa la matrice del rischio o matrice di probabilità

L'approccio analitico sfrutta in modo dettagliato la funzione R=f (P, D), l'entità di rischio R è associata ad un determinato fattore di rischio, cioè ad una determinata minaccia che esplora e sfrutta una determinata vulnerabilità. Minaccia e vulnerabilità sono cause di un evento (sfavorevole o favorevole). L'approccio

analitico richiede una analisi e stima delle probabilità delle cause e la loro combinazione quindi l'applicazione risulta essere più difficile.

L'approccio empirico risulta più semplice, è quello che useremo.

I criteri dovrebbero riflettere i valori, gli obiettivi e le risorse dell'organizzazione.

Alcuni criteri potrebbero essere imposti o derivati dalle leggi o regolamenti, dai clienti, o da altri requisiti applicabili.

Inoltre, i criteri per la gestione dei rischi dovrebbero essere coerenti con la politica del Risk Management, dovrebbero essere definiti prima di iniziare ad applicare il processo di Risk Management e dovrebbero essere riesaminati in modo continuo.

Nella definizione dei criteri di gestione dei rischi si dovrebbe prendere in considerazione almeno i seguenti fattori:

- la natura e la tipologia delle cause degli eventi sfavorevoli/favorevoli, le loro conseguenze e le modalità di misurazione delle conseguenze;
- la definizione dei vari livelli di probabilità/verosimiglianza;
- i tempi di misurazione delle probabilità e le conseguenze;
- come sono determinati i livelli dei rischi;
- il punto di vista degli stakeholder;
- come devono essere combinati i rischi parziali multipli in un rischio aggregato.

La conseguenza è la forza che l'impatto ha avuto dopo che si è verificato un determinato evento collegato ad uno specifico fattore di rischio, il quale se si manifesta può ostacolare/facilitare il conseguimento degli obiettivi.
Pertanto occorre definire una scala con i diversi valori delle conseguenze, la granularità della scala dipende dal livello di dettaglio che si vuole avere.

La probabilità dell'evento dipende dalla frequenza con cui l'evento si è verificato, bisogna fare anche una scala delle probabilità.

Uno degli strumenti con cui si lavora è la matrice dei rischi o matrice di probabilità:

Conseguenze (D)	Probabilità (P)				
	Molto bassa (1)	Bassa (2)	Media (3)	Alta (4)	Molto Alta (5)
Molto Basso (1)	1	2	3	4	5
Basso (2)	2 B	4	6	8	10
Medio (3)	3	6	M 9	12	15
Alto (4)	4	8	12	16 A	20
Molto Alto (5)	5	10	15	20	25

I livelli da 1 a 4 rappresentano il rischio accettabile (rischio residuo accettabile RRac), da 5 a 14 il rischio è da ridurre e >15 il rischio è da ridurre immediatamente.

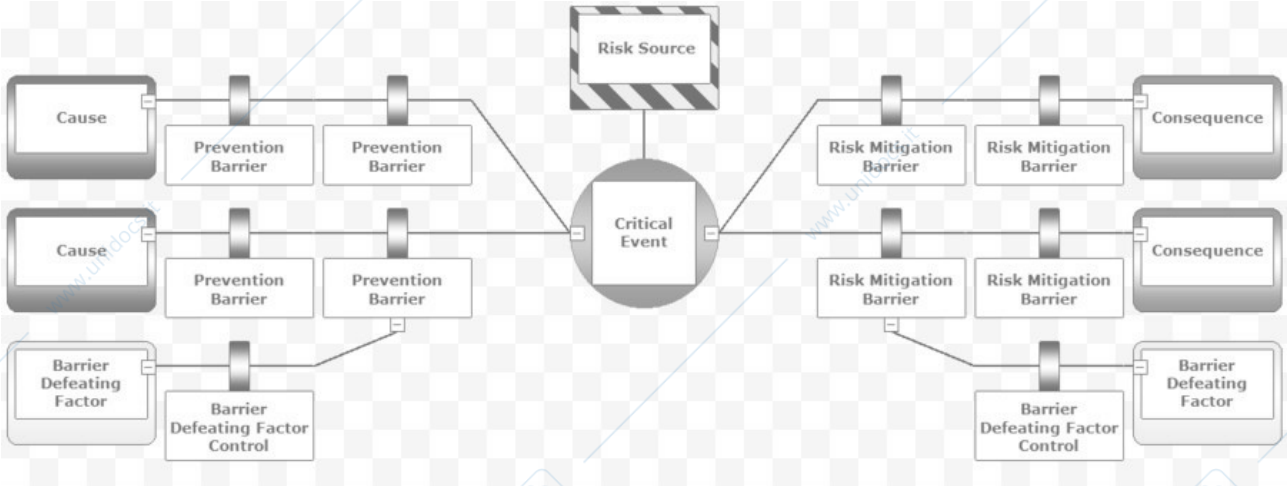
Durante l'individuazione dei rischi, nel livello di risk assessment, l'organizzazione dovrebbe individuare le fonti degli eventi (sfavorevoli e favorevoli), gli eventi stessi, gli agenti portatori delle cause, le cause stesse, le aree di impatto, gli scenari di concatenamento delle cause e le loro conseguenze. Bisognerebbe tenere in considerazione anche eventuali fonti, fattori e agenti esterni.
Lo scopo dell'attività di identificazione dei rischi è quello di generare una lista di tutti i fattori che possono ostacolare/facilitare il raggiungimento degli obiettivi.
Questo va fatto al più presto perché più tardi vengono scoperti, più è possibile che l'impatto sugli obiettivi sia maggiore. L'identificazione delle fonti di rischio dovrebbe essere fatta di continuo, è fondamentale che l'organizzazione metta in atto strumenti e tecniche adeguate per identificare i rischi.

Un evento sfavorevole avviene nel momento in cui una causa, per esempio una minaccia (M) esplora e sfrutta un'altra causa, cioè una vulnerabilità (V); l'evento sfavorevole potrebbe portare a delle conseguenze e provocare un effetto indesiderato.

L'evento, dunque, potrebbe considerarsi come la combinazione delle due cause, cioè una minaccia con una vulnerabilità.

Correlazione causa-evento-impatto: immaginiamo uno scenario in cui una mano spinge delle pedine e queste cadono. La spinta della mano contro le pedine è la causa minaccia, l'instabilità delle pedine è la causa vulnerabilità e la caduta è l'evento sfavorevole.

Una tecnica veloce e facile da usare nell'identificazione e analisi dei rischi è la tecnica Bow-Tie: si svolge disegnando un diagramma con la forma di un farfallino, si identifica prima di tutto l'evento sfavorevole o favorevole. Al centro abbiamo l'evento, a sx le cause, a dx le conseguenze. Si possono collegare più Bow-Tie (una conseguenza può essere la causa di un altro evento) per vedere le dipendenze tra i vari elementi.



L'analisi dei rischi è un'attività nella quale si valutano le potenziali conseguenze (D) e le probabilità che l'evento sfavorevole o favorevole accada (P). La probabilità P è una combinazione della probabilità della minaccia e della probabilità della vulnerabilità. Quindi P = f (Pm, Pv).
La probabilità della vulnerabilità esprime con quanta facilità si riesce a sfruttarla, la probabilità della minaccia (inteso come frequenza con cui si presenta la minaccia) è la probabilità con la quale si riesce a sfruttare una vulnerabilità.
A questo punto si identificano tutte le possibili minacce e le possibili vulnerabilità, è consigliabile analizzare singolarmente ogni vulnerabilità per capire se può essere sfruttata da più minacce, il che porta a rischi ulteriori.

Ogni rischio così identificato è un rischio parziale: Ri = f (Pv, Pm, D) = f (P, D)
Indicazioni molto importanti sono espresse nella norma ISO 31010.

Dopo l'analisi dei rischi si procede con la loro valutazione, lo scopo è quello di calcolare i rischi e di effettuare la comparazione tra i livelli dei rischi riscontrati e i criteri di accettazione di questi.
In alcuni casi la valutazione dei rischi può portare all'esecuzione di ulteriori analisi, può anche portare a decidere di non modificare niente al momento della valutazione.
Ogni rischio parziale viene calcolato guardando la matrice dei rischi, ogni rischio dovrebbe essere calcolato singolarmente e indipendentemente dagli altri.
Questo può essere utile per identificare le situazioni più gravi delle altre, quelle che bisogna trattare con urgenza.
La decisione di accettare o meno viene presa secondo i criteri di accettazione dei rischi. I rischi parziali che sono stati valutati di entità bassa e sono cioè tollerabili possono anche non essere trattati a meno che non si riconosca qualche beneficio. Questa valutazione dei rischi che valuta rischio per rischio fa in modo di non avere una valutazione totale di quello che è il rischio complessivo, la ponderazione di tutti i rischi parziali forma il cosiddetto Rischio Aggregato (Ragg), calcolato in funzione del contesto e della tipologia degli incidenti. Il rischio aggregato è la media ponderata che viene calcolata sommando i rischi parziali, ognuno moltiplicato per un numero che denota il suo "peso" e dividendo tutto per la somma dei pesi (combinazione lineare convessa dei dati in analisi).

$$R(Aggr) = \frac{\sum_{i=1}^{n} fiRi}{\sum_{i=1}^{n} fi}$$

fi è il peso, Ri il rischio parziale. Nel caso tutti i rischi abbiano lo stesso peso si fa una media aritmetica.
Esistono anche altre formule per calcolare il rischio aggregato.

Il livello di confidenza con cui si calcola il Ragg dipende dalla conoscenza che si ha della situazione stessa e del suo contorno. Il Ragg in ogni caso da solo un'informazione su tutti i rischi che incombono e aiuta a decidere le opzioni da seguire ma non aiuta con la riduzione o eliminazione del rischio. La riduzione deve avvenire lavorando singolarmente su ogni rischio.
L'attività di valutazione termina con l'elenco dei rischi parziali con i rispettivi livelli stimati e con la priorità con la quale bisogna intervenire.

Prima di iniziare con l'attività di trattamento dei rischi occorre riesaminare i risultati che provengono dalla fase precedente. Questo è il Punto Decisionale 1 (valutazione critica costruttiva, se si verificano degli scostamenti è necessario tornare indietro e confrontarsi con quanto stabilito in precedenza. Durante la valutazione è necessario coinvolgere tutti gli stakeholder interessati i quali dovranno dare la loro approvazione per passare alla parte di trattamento dei rischi).

Il trattamento dei rischi è un processo ciclico che si svolge attraverso:

- Selezione delle opzioni per il trattamento dei rischi
- Identificazione delle misure da implementare
- Identificazione delle misure esistenti
- Calcolo dei rischi residui
- Preparazione del piano trattamento dei rischi

Il trattamento dei rischi si sviluppa con la scelta di 1 o più tra queste opzioni:
Modificare i rischi, accettare i rischi, evitare i rischi, condividere o trasferire i rischi.
La scelta di queste opzioni dipende dal valore del Ragg e sulla base dei costi per l'implementazione e conseguenti benefici.
In linea generale bisogna preferire le opzioni che con il costo minore offrono i maggiori benefici.
L'obiettivo è quello di fare in modo che il rischio residuo diventi accettabile.

La selezione delle opzioni del trattamento dei rischi deve tener conto dei costi e i tempi per l'attuazione delle misure, i criteri di gestione dei rischi, i requisiti legali, regolamentari e contrattuali, gli aspetti tecnici, ambientali e culturali. Esistono molti vincoli che possono influenzare la scelta delle misure.
Le misure prese possono essere di tipo preventivo, per evitare certe situazioni di rischio sfavorevole o per sollecitare situazioni che vedono come protagonisti i rischi favorevoli.
Le misure di mitigazione invece per ridurre/aumentare le conseguenze al verificarsi di un evento.
Il risultato di questa fase è un elenco di possibili misure, con i loro costi, benefici e priorità di implementazione.
La decisione di accettazione dei rischi, senza ulteriori azioni e rinunciando a qualsiasi evento deve essere presa qualora i rischi siano accettabili assumendo la responsabilità nel caso di conseguenze.
A volte questa scelta deriva dalla non conoscenza o sottovalutazione dei rischi presenti, dall'inconsapevolezza del management e da una carenza metodologica nell'analisi del rischio.

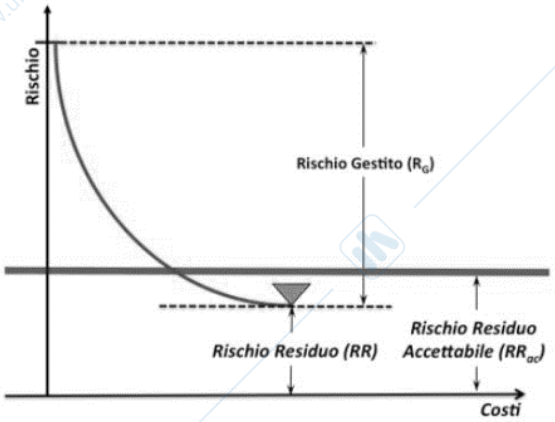
Quando i rischi sono considerati troppo alti si può scegliere di eliminarli del tutto, non svolgendo più l'attività che poteva creare questi rischi o apportando modifiche all'attività (si potrebbe decidere di spostare l'attività in una località diversa, dove queste minacce non esistono).

La condivisione dei rischi implica una decisione di condividere (trasferire) determinati rischi con soggetti esterni, è importante conoscere i limiti di trasferimento del rischio (la condivisione dei rischi può crearne di altri o modificare dei rischi esistenti quindi potrebbe essere necessario un trattamento migliore). Quindi si può dire che è possibile la condivisione della responsabilità per gestire i rischi ma non è condivisibile l'impatto che viene creato.
La scelta dell'opzione/opzioni permette di procedere con la pianificazione delle misure per il trattamento.
Nel caso in cui l'opzione decisa sia quella di eliminare del tutto il rischio, si procederà con le azioni che permetteranno questo obiettivo, se no si decide come proseguire in modo opportuno.

Esistono linee guida che propongono Misure efficaci in funzione della situazione contingente. Queste guide possono essere le norme nazionali o internazionali, come per esempio le norme ISO, le UNI normativa italiana, le NIST Americane, le DIN Tedesche, le BS Gran Bretagna e altre linee guida emesse dalle varie associazioni di categoria.

A titolo di esempio si cita qui, per il contesto della sicurezza delle informazioni, l'Annex A della norma ISO/IEC 27001, il quale contiene un elenco di Obiettivi di Controllo e di Controlli (Misure) del tipo fisico-ambientale, organizzativo e logico (per i sistemi informatici). La descrizione in dettaglio di questi controlli è sviluppata nella norma ISO/IEC 27002.

Nel caso in cui il contesto non è coperto da nessuna fonte normativa, si riuniscono le persone responsabili per decidere insieme come proseguire.
Solitamente l'uomo è abituato a proteggere i propri averi, nel campo dei sistemi (più specificatamente quelli informatici), gli amministratori introducono una serie di procedure e meccanismi di protezione. Questi ultimi a volte sono inefficaci ma aiutano comunque a gestire una certa quantità di rischio, lo possiamo quindi chiamare Rischio Gestito (Rg). Questo rischio gestito deve essere preso in considerazione per calcolare i rischi residui (Rr).
In questa fase si valutano anche le misure in atto con la loro effettiva adeguatezza, efficacia e coerenza con le nuove misure che saranno implementate.
Maggiore è la riduzione del livello dei rischi, maggiore è il numero delle misure da applicare e di conseguenza maggiori sono i costi.



Si può accettare un livello di rischio definito come Rischio Residuo Accettabile (RRac), la quantità di rischio ridotto porta ad avere un Rischio Residuo (RR), se RR>RRac è necessario applicare altre misure. Il RRac non è da considerarsi in senso statico, costituisce la soglia minima al di sopra della quale il rischio deve essere ridotto.

Il Piano di Trattamento dei Rischi è il documento che pianifica l'implementazione delle Misure.

Il Piano di Trattamento dei rischi dovrebbe contenere le seguenti informazioni:

- le ragioni per la selezione delle opzioni di trattamento e i benefici attesi;
- l'elenco delle Misure da implementare e la priorità di implementazione;
- l'elenco delle Misure esistenti;
- il calcolo dei Rischi Residui;
- i responsabili per l'approvazione del Piano Trattamento dei Rischi;
- i responsabili per l'attuazione del piano (implementazione delle Misure);
- le competenze necessarie e il piano del training o altre azioni per soddisfare queste esigenze;
- eventuali azioni proposte;
- le risorse necessarie per l'implementazione delle Misure. Le risorse possono riguardare le persone impegnate, il loro impegno, le attrezzature HW, SW, processi, procedimenti, ecc., ma soprattutto l'impegno economico, cioè l'investimento necessario.
- le modalità per misurare l'efficacia delle Misure da implementare ed eventuali vincoli da rispettare;
- le modalità di registrazione (par. 7.9);
- i tempi e la schedulazione (chi fa che cosa e quando deve essere fatto).

I rischi residui devono essere documentati e sottoposti a monitoraggio da parte delle persone coinvolte nel processo di risk management.

Il proprietario dei rischi (che in genere coincide con il proprietario degli obiettivi) è la persona che dovrebbe gestire il Punto Decisionale 2.
Il piano di trattamento dei rischi descrive come i rischi devono essere trattati per soddisfare i criteri di accettazione, è importante per il proprietario tenere sotto controllo tutte queste cose e modificarle in caso di bisogno.
L'accettazione dei rischi non è solo la verifica del fatto che i rischi stiano sotto la soglia di RRac, tutto dipende dal contesto e dalla situazione da affrontare. Se siamo in una situazione in cui non si guarda la soglia di accettazione del rischio per prendere una decisione, il proprietario deve documentare la situazione e giustificare la decisione di ignorare i normali criteri di accettazione del rischio.

Il Punto Decisionale 2 viene completato con:

- l'approvazione del Piano di Trattamento dei Rischi;
- l'approvazione dei Rischi Residui;
- l'autorizzare dell'implementazione delle Misure.

Questo deve essere documentato.
Alla conclusione del Punto Decisionale 2 si può procedere con l'implementazione delle misure che sono state stabilite nel Piano di trattamento dei rischi, al fine di raggiungere gli obiettivi preposti.
Si potrebbe definire (nel caso in cui sia possibile) la modalità di misurazione dell'efficacia delle misure stabilite.

Il monitoraggio e il riesame sono elementi fondamentali nel processo di risk management in quanto i rischi non sono statici e le situazioni al contorno sono anch'esse in continuo cambiamento, è necessario che queste azioni di controllo siano eseguite costantemente, magari anche con il supporto di entità esterne che forniscono informazioni riguardo le nuove minacce e vulnerabilità.

Il monitoraggio e il riesame devono comprendere tutti gli aspetti del processo di risk management, al fine di:

- svolgere riesami regolari sull'efficacia del processo di risk management tenendo in considerazione i risultati degli incidenti, i risultati delle misurazioni dell'efficacia delle Misure, i suggerimenti e le informazioni di ritorno di tutte le parti interessate;
- ottenere ulteriori informazioni per migliorare il processo del risk management;
- analizzare e apprendere da eventi (compreso dai mancati incidenti), dai i cambiamenti, dalle tendenze, dai successi e dagli insuccessi;
- misurare l'efficacia e l'efficienza delle Misure per verificare che i requisiti siano stati soddisfatti.
- rilevare cambiamenti del contesto esterno e interno, compresi i cambiamenti ai criteri dei rischi e il rischio in sé, che può richiedere la revisione dei trattamenti e delle priorità di rischio; e
- identificare i rischi emergenti.

Le attività di monitoraggio devono affrontare i seguenti aspetti:

- legali e regolamentari;
- fisico- ambientale, organizzativi e logici;
- concorrenziali;
- approccio del risk assessment;
- riesame degli obiettivi da raggiungere;
- i criteri di valutazione dei rischi
- i criteri di accettazione dei rischi;
- i costi di implementazione e di gestione delle Misure;
- le competenze richieste.

Con il monitoraggio e il riesame bisogna garantire la disponibilità perenne delle risorse per il risk management offerte dall'organizzazione e bisogna documentare il tutto, per utilizzarlo come elemento di ingresso all'attività di riesame successiva.

Le attività del risk management dovrebbero registrate e tracciabili e costituiscono le fondamenta per l'efficacia, l'efficienza e il miglioramento continuo del processo di risk management e del framework.
Le registrazioni possono essere in qualsiasi formato e devono essere controllate e conservate dal proprietario degli obiettivi.
Le decisioni riguardanti le registrazioni dovrebbero tenere conto:

- le esigenze per l'apprendimento continuo
- i benefici del riutilizzo delle informazioni
- i costi e gli sforzi che sono stati eseguiti
- i requisiti legali, operativi e normativi
- il metodo di accesso, la facilità di recupero e i supporti di memorizzazione
- il periodo di conservazione
- la sensibilità delle informazioni

In ogni caso, ogni istanza del processo, cioè ogni applicazione del processo di risk management, dovrebbe prurre informazioni documentate relative:

- agli obiettivi da raggiungere e i relativi proprietari
- al contesto esterno ed interno dell'istanza, il campo di applicazione e l'estensione dei confini, le aspettative degli stakeholder, nonché i requisiti per leggi e regolamenti, i processi interni attraverso i quali devono essere soddisfatti gli obiettivi, le loro interfacce e le loro dipendenze e quelli eseguiti da ente al di fuori dei confini di applicazione dell'istanza;
- ai ruoli, le responsabilità e le relative autorità;
- ai proprietari dei rischi;
- ai criteri di gestione dei rischi (valutazione degli impatti, valutazione delle probabilità, livelli dei rischi e accettazione dei rischi);
- al risk assessment (identificazione, analisi e valutazione dei rischi);
- alle attività del **Punto Decisionale 1**;
- alle attività di trattamento dei rischi con il Piano di Trattamento dei Rischi;
- alle attività di accettazione dei rischi (risultati del **Punto Decisionale 2**);
- all'implementazione delle Misure;
- alla valutazione dell'efficacia e dell'efficienza delle Misure.

CASO DI STUDIO 1: IL TESORETTO

Prendiamo in considerazione il caso di una famiglia. Supponiamo che il capofamiglia abbia accumulato un tesoretto di 40.000,00 €. Questo tesoretto potrebbe essere anche un oggetto (orologio, gioielli, ecc.) pari al valore che abbiamo specificato. Supponiamo che per un determinato periodo, per varie ragioni che non stiamo a specificare, il capofamiglia sia costretto, per qualche sua ragione, a tenere il tesoretto o l'oggetto nel suo appartamento.

Il proprietario del tesoretto, dunque, è il capofamiglia.

L'obiettivo del proprietario è di proteggere il tesoretto conservandolo integro.

L'appartamento della famiglia è ubicato al primo piano (app. 5) (fig. 17) di una palazzina nella periferia nord di una città dell'Italia settentrionale. La palazzina è composta da 8 appartamenti, occupati da famiglie italiane.

La composizione degli abitanti della zona è mista di italiani e stranieri.

La famiglia del piano terra (app. 2) ha due figli maschi di cui il maggiore spesso si trova immischiato in situazioni poco chiare con la giustizia.

I portatori d'interesse esterni sono i negozi della zona che possono avere il desiderio di avere il proprietario del tesoretto come loro cliente. Questi portatori d'interessi, apparentemente, non sono a conoscenza dell'esistenza del tesoretto.

Non esistono requisiti di legge o di altri regolamenti.

Le potenziali minacce possono essere sollevate da eventuali malviventi della zona e dal figlio dell'appartamento 2, che, nel momento in cui vengono a conoscenza dell'esistenza del tesoretto, possono sollevare interesse e cercare di rubarlo.

Il contesto interno è limitato al nucleo familiare che è composto da 3 persone: il marito (capofamiglia), la moglie e il figlio di 22 anni.

Il capofamiglia è il proprietario di un esercizio che dista circa 5 km dall'abitazione. La moglie lavora come dipendente in una società assicuratrice in centro della città. Il figlio ha rifiutato di seguire il padre nella sua attività ed è in cerca di occupazione.

Gli stakeholder interni sono i componenti della famiglia che sono informati dell'esistenza del tesoretto e la loro aspettativa è quella di conservare il tesoretto.
Le potenziali minacce possono essere sollevate dal figlio perché è disoccupato e quindi senza stipendio.

Per rendere l'esempio di facile comprensione, immaginiamo una situazione molto semplice. Immaginiamo che il tesoretto sia nascosto in un cassetto in una delle stanze dell'appartamento. Cassetto e stanza sono sprovvisti di serratura.

La porta d'ingresso nell'appartamento è blindata con serratura a combinazione che conoscono tutti i membri della famiglia.

La stanza dell'appartamento dove si trova il tesoretto è il salone che ha una finestra verso l'esterno (fig. 18).

Sulla base della metodologia descritta nel capitolo precedente per i criteri di valutazione dell'impatto/danno, decidiamo di adottare la scala con i seguenti valori, anche se il valore del tesoretto non arriva al valore Molto Alto:

- Molto Basso: 1 (D_1), che corrisponde a € 10.000,00.
- Basso: 2 (D_2), che corrisponde a € 20.000,00.
- Medio: 3 (D_3), che corrisponde a € 30.000,00.
- Alto: 4 (D_4), che corrisponde a € 40.000,00.
- Molto Alto: 5 (D_5), che corrisponde a € 50.000,00.

I vari livelli indicano l'entità del danno che l'oggetto potrebbe subire. Il danno potrebbe variare dal valore Molto Basso fino al valore Alto che è pari a 40.000,00 €. Un furto potrebbe danneggiare l'oggetto completamente, quindi potrebbe essere rubato, ma potrebbe essere solo danneggiato.

Per la valutazione delle probabilità usiamo la seguente scala:

- Molto Bassa: 1
- Bassa: 2
- Media: 3
- Alta: 4
- Molto Alta: 5

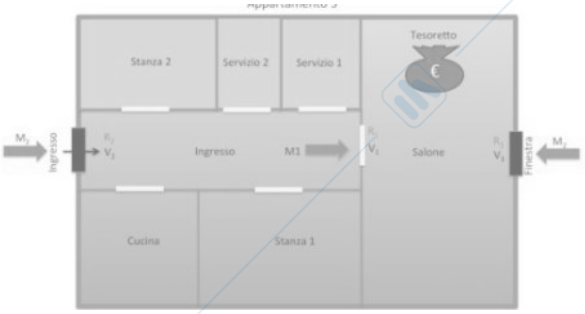
Per i criteri di valutazione dei rischi adottiamo la tabella del par. 7.3.5 (fig. 9).

Per i criteri di accettazione dei rischi adottiamo la tabella del par. 7.3.5 (fig. 10).

Il **Rischio Residuo Accettabile** (RR_{ac}), quindi, deve essere Basso (livelli da 1 a 4).

La violazione del tesoretto ha come conseguenze valutabili in un Danno (D) che può essere diretto e a volte indiretto. Sulla scala dell'Impatto/Danno, stabilita nell'ambito della metodologia (par. 8.4), il massimo Impatto/Danno che si può avere è pari al valore Alto (D=4), cioè 40.000,00 €.

La fig. 19 illustra una potenziale configurazione delle minacce e delle vulnerabilità della situazione dell'appartamento dove si trova il tesoretto.



È evidente che il proprietario del tesoretto, nel scegliere questa soluzione dimostra di non essere consapevole dei rischi che incombono sul tesoretto. Per abitudine, ha ignorato l'esistenza delle vulnerabilità dell'appartamento, credendo di averlo sistemato in ambiente sicuro e ignora i rischi che possono incombere sul tesoretto stesso.

Gli strumenti che possono essere utilizzati per l'identificazione delle minacce e delle vulnerabilità sono riportati nell'Appendice A e sono sviluppati nella norma ISO 31010.

Nel nostro caso si potrebbe utilizzare la tecnica del Brainstorming, delle Checklists o effettuare delle interviste al proprietario del tesoretto e anche alla moglie per analizzare la situazione.

I risultati di quest'analisi ci ha portati a scoprire tre Vulnerabilità (V_1, V_2 e V_3) e due tipi di potenziali Minacce (M_1 ed M_2). Le tre Vulnerabilità possono essere esplorate e sfruttate dalle Minacce.

La Vulnerabilità V_1 è la porta del salone, dove si trova il tesoretto.

La Vulnerabilità V_2 è la porta d'ingresso nell'appartamento.

L'analisi successiva dovrebbe essere fatta per scoprire se esistono nei pressi del palazzo e dell'appartamento eventuali agenti portatori di minacce . Gli agenti, nel nostro caso, possono essere ladri, intenzionati a venire in possesso del tesoretto. Potrebbero però esserci anche altri agenti portatori di minacce che per ora non sono evidenti, ma comunque questo non significa che in futuro non si manifestino per aggredire il tesoretto in una forma diversa. Potrebbe esserci per esempio un agente che potrebbe sollevare la minaccia umidità, oppure infiltrazioni d'acqua per via del tetto rovinato. Per ora, queste minacce non sono evidenti, quindi non vengono prese in considerazione. In ogni caso è da tenere presente in eventuale analisi futura.

Nell'analisi del contesto interno abbiamo individuato come potenziale agente il figlio della famiglia. Il ragazzo essendo disoccupato potrebbe essere spinto a commettere il furto parziale o totale del tesoretto (Minaccia M_1). Potrebbe essere spinto a prelevare dal tesoretto una parte o tutto. Per evitare che sia scoperto subito magari decide di prelevare periodicamente importi piccoli; in ogni caso potrebbe alla fine sottrare un importo pari a D3= 30.000,00 €. Questa è una delle ipotesi, in quando potrebbe decidere di rubare tutto l'importo. Nel nostro esempio ipotizziamo un danno pari al 75 % del tesoretto. La Vulnerabilità che questa minaccia è portata a usufruire è la V_1, cioè la porta del salone.

Nell'analisi del contesto esterno abbiamo individuato come potenziale agente i membri della famiglia del primo piano o altre persone del quartiere che potrebbero venire, in qualche maniera, a conoscenza del tesoretto e spingersi a commettere il furto (Minaccia M_2). In questo caso il potenziale danno si ipotizza al 100%, cioè, pari a D_2= 40.000,00 €. Questa minaccia potrebbe sfruttare sia la Vulnerabilità V_2 (la porta d'ingresso), sia la Vulnerabilità V_3, la finestra del salone che si affaccia verso la strada.

Ogni accoppiamento tra una minaccia e una vulnerabilità è un evento sfavorevole che può creare un incidente (fig. 19).

Gli strumenti che possono essere utilizzati per effettuare l'Analisi dei rischi sono riportati nell'Appendice A e sono sviluppati in dettaglio nella norma ISO 31010.

Nel nostro caso si potrebbe utilizzare la tecnica dell'analisi delle Cause Radici, l'analisi Causa – Effetto e anche altre.

Durante il lavoro d'identificazione abbiamo deciso di considerare i due livelli di Impatto:

- D3= € 30.000,00, individuato, nella scala delle Conseguenze, come Medio (M=3);
- D4= € 40.000,00, individuato, nella scala delle Conseguenze, come Alto (A=4);

Sulla base di quanto si è detto precedentemente possiamo pensare di avere la seguente combinazione tra minacce e vulnerabilità che possono provocare incidenti: (M_1,V_1); (M_2,V_2); (M_2,V_3).

Il passo successivo è quello di stimare la probabilità con la quale si manifestano i tre incidenti. Nel par. 8.4 è stata stabilita una scala convenzionale per i livelli di probabilità degli incidenti.

Dopo un approfondimento adeguato supponiamo le seguenti probabilità degli incidenti che incombono sul tesoretto (v. par. 7.4.3):

- P_{11}=($P_{V1}P_{M1}$)= Molto Alta (5) (probabilità che il figlio rubi una parte del tesoretto);
- P_{22}=($P_{V2}P_{M2}$)= Alta(4) (probabilità che malviventi tendino a entrare nell'appartamento attraverso la porta d'ingresso) (*);
- P_{23}=($P_{V2}P_{M3}$)= Media (3) (probabilità che malviventi tendino a entrare nell'appartamento attraverso la finestra).

(*) L'esistenza della porta blindata è una misura esistente che riduce una parte del rischio. Questa riduzione del rischio sarà presa in considerazione più avanti. In questo momento si sta valutando la probabilità che possa avvenire l'incidente

senza le misure esistenti.

In linea generale qui termina l'attività di Analisi dei rischi. L'attività successiva è quella di valutare ogni rischio parziale e calcolare il Rischio Aggregato (R_{Agg}) che incombe sul tesoretto.

Nota Bene: i valori dell'Impatto/Danno (D) e delle Probabilità (P) degli incidenti sono stabiliti sulla base dei ragionamenti che sono stati fatti dal gruppo di lavoro composto dalle persone coinvolte durante l'analisi. Questi valori possono cambiare in funzione del livello di conoscenza del contesto esterno e quello interno. Più le persone sono esperte nel valutare questi due parametri, più i valori si avvicinano alla realtà. Ma come abbiamo detto precedentemente, la conoscenza della realtà non si potrà mai avere al 100% e questo porta sempre a commettere errori sulle stime.

Valutiamo ora i Rischi Parziali (R_i), cioè quei rischi dovuti a ogni singola minaccia che potrebbe esplorare e sfruttare una determinata vulnerabilità.

Sulla base dei risultati dell'analisi precedente i Rischi Parziali che incombono sul tesoretto sono i seguenti (fig. 19):

- $R_1 = f(P_{11}, D_1)$, rischio dovuto al furto da parte del figlio;
- $R_2 = f(P_{22}, D_2)$, rischio dovuto al furto da parte di malviventi attraverso la porta d'ingresso;
- $R_3 = f(P_{23}, D_2)$, rischio dovuto al furto da parte di malviventi attraverso la finestra.

Quindi, si ha la seguente situazione:

- D_3= € 30.000,00, Impatto/Danno: Medio (M=3);
- D_4= € 40.000,00, Impatto/Danno Alto (A=4);
- $P_{11}=(P_{V1}P_{M1})$= Molto Alta (MA=5);
- $P_{22}=(P_{V2}P_{M2})$= Alta (A=4);
- $P_{23}=(P_{V2}P_{M3})$= Media (M=3).

Utilizzando la Matrice dei Rischi (fig. 9) e i Criteri di accettazione dei rischi (fig. 10) si può procedere con il calcolo dei Rischi parziali (R_i) (fig. 20):

- $R_1=f(P_{11},D_1)=f(5,3)=15$: Entità di rischio = Alta, Priorità Alta, Rischio da ridurre immediatamente.
- $R_2=f(P_{22},D_2)=f(4,4)=16$: Entità di rischio = Alta, Priorità Alta, Rischio da ridurre immediatamente.
- $R_3=f(P_{23},D_2)=f(3,4)=12$: Entità di rischio = Media, Priorità Media, Rischio da ridurre.

Conseguenze (D)	Probabilità (P)				
	Molto bassa (1)	Bassa (2)	Media (3)	Alta (4)	Molto Alta (5)
Molto Basso (1)	1	2	3	4	5
Basso (2)	2	4	6	8	10
Medio (3)	3	6	9	12	15
Alto (4)	4	8	12	16	20
Molto Alto (5)	5	10	15	20	25

La tabella che segue identifica i valori dei Rischi Parziali (R_i) e la priorità con la quale occorre intervenire per ridurre o per eliminare i rischi. L'introduzione di contromisure richiede un investimento e i costi per l'implementazione e per la gestione sono proporzionali al salto di diminuzione dell'entità del rischio.

Rischio (R_i)	Livello	Entità di rischio	Priorità di intervento
R_1	15	Alta	2
R_2	16	Alta	1
R_3	12	Media	3

Rischio Aggregato (R_{Agg}): allo socpo di semplificare il calcolo del Rischio Aggregato (R_{Agg}), si è deciso la media aritmetica semplice dei Rischi Parziali (R_i):

$$R(Aggr) = \frac{1}{n}\sum_{i=1}^{n} Ri$$

$= 43/3 = 14{,}33 \simeq 14$

Facendo riferimento ai Criteri di Accettazione dei Rischi della fig. 10, il Rischio Aggregato assume un valore pari a $R_{Agg}=14$ ed è un rischio del livello Medio. Come è stato detto precedentemente, il valore del Rischio Aggregato (R_{Agg}) dà il livello indicativo del rischio complessivo. Questo valore potrebbe spingere il capofamiglia a decidere se il tesoretto deve rimanere nascosto nell'appartamento, oppure spostarlo in un altro posto più sicuro. Nel caso in cui si decidesse di lascialro nell'appartamento, il Rischio Aggregato (R_{Agg}) si riduce solo intervenendo in modo mirato sui Rischi Parziali (R_i) che lo compongono e con la priorità stabilita nella tabella precedente.

Le opzioni che abbiamo a disposizione sono:

- Modificare i rischi.
- Accettare i rischi.
- Evitare i rischi.
- Condividere o trasferire i rischi.

La soluzioni migliore, nel nostro caso, è quella da evitare i rischi e di trasferirli a un'entità esterna. In questo caso si potrebbe portare il tesoretto in una banca o in una cassetta di sicurezza. Questo però non è possibile, in quanto, come è stato detto precedentemente, per varie ragioni, il capofamiglia è costretto a tenere il tesoretto nel suo appartamento per un po' di tempo.

A questo punto rimangono le altre due opzioni: modificare introducendo misure adeguate o accettare i rischi così come sono. Accettare i rischi così come

sono, non è la strategia percorribile, perché i Rischi Parziali sono di livello Medio e Alto e il Rischio Aggregato (R_{Agg}) è del livello Medio. Questa situazione non è accettabile, perchè il Rischio Residuo Accettabile (RR_{ac}) è Basso (livelli da 1 a 4) (par. 8.4).

Pertanto si può solo modificare la situazione introducendo misure idonee e adeguate per ridurre i rischi ai livelli accettabili.

Per ridurre i Rischi Parziali è necessario applicare delle Contromisure adeguate. Esse possono essere scelte ad hoc per la situazione.

Per ridurre il Rischio Parziale R_1 (= 15 - Alto) che è dovuto al probabile furto da parte del figlio, si potrebbe agire in due modi: si potrebbe fare in modo di ridurre o eliminare del tutto il rischio rimuovendo la vulnerabilità, o allontanando la minaccia (intraprendendo misure preventive). La rimozione della vulnerabilità potrebbe avvenire proteggendo, cioè, in modo sicuro il tesoretto. Questo potrebbe avvenire attraverso l'inserimento di una serratura nella porta del salone, oppure con l'adozione di una cassaforte da posizionare nel salone.

L'allontanamento della minaccia potrebbe avvenire sistemando la posizione occupazionale del figlio, cercandogli, per esempio, un lavoro e rendendolo economicamente indipendente.

Pertanto, per affrontare questa situazione e ridurre la probabilità del furto da parte del figlio e le conseguenze, sono state identificate le seguenti Misure (C_i) (per ridurre il Rischio R_1 dal livello 15 al livello 1):

- C_1 - Cercare al più presto un lavoro per il figlio.
- C_2 - Inserire il tesoretto in una cassaforte, posizionandola nel salone e gestire la chiave.
- C_3 - Chiudere la porta del salone a chiave e gestire la chiave.
- C_4 - Sensibilizzare il figlio per aumentare la consapevolezza sul comportamento etico.

Si procede nella stessa maniera per ridurre il Rischio Parziale R_2 dal livello 16 al livello 1 (rischio dovuto al probabile furto da parte di malviventi attraverso la porta d'ingresso).

Le Contromisure che sono state individuate sono:

- C_2 - Inserire il tesoretto in una cassaforte, posizionandola nel salone e gestire la chiave in modo sicuro.
- C_5 - Installare la porta blindata all'ingresso dell'appartamento.

Le Contromisure che sono state individuate per ridurre i rischio R_3 dal livello 12 al livello 1 (rischio dovuto al furto da parte di malviventi attraverso la finestra), sono:

- C_2 - Inserire il tesoretto in una cassaforte, posizionandola nel salone e gestire la chiave in modo sicuro.
- C_6 - Inserire le inferriate alla finestra.

Queste sono tutte le Contromisure (fig. 22) che possiamo applicare per ridurre i Rischi Parziali dai livelli: R_1 =15 - Alto, R_2 =16 – Alto, R_3 =12 - Medio al livello 1 - Basso.

La tabella che segue illustra la corrispondenza tra Rischi e Contromisure.

Contromisure	R_1	R_2	R_3
C_1 - Cercare al più presto un lavoro per il figlio	×		
C_2 - Inserire il tesoretto in una cassaforte, posizionandola nel salone e gestire la chiave in modo sicuro.	×	×	×
C_3 - Chiudere la porta del salone a chiave e gestire la chiave.	×		
C_4 - Sensibilizzare il figlio per aumentare la consapevolezza sul comportamento etico.	×		
C_5 - Installare la porta blindata all'ingresso dell'appartamento. (esistente)		×	
C_6 - Inserire le inferriate alla finestra.			×

Durante questa attività, dobbiamo analizzare la situazione reale, al fine di individuare eventuali Contromisure esistenti. Ogni Contromisura (C_j) esistente riduce il rischio di una determinata quantità. Questo rischio è il Rischio Gestito (R_{GiCj}).

Dalla tabella sopra si nota che la Contromisura C_5 - *porta blindata nella porta d'ingresso dell'appartamento* è già implementata.

Tenendo presente che la misura C_5 è già esistente, questo significa che questa contromisura gestisce già una certa quantità di rischio e, quindi, riduce il valore del R_2 di una quantità pari a R_{G2C5}. Questo è il Rischio Gestito della C_5. Quindi è necessario quantificare questo Rischio Gestito (R_{G2C5}).

Nel par. 8.4 è stato impostato come **Rischio Residuo Accettabile (RR_{ac})** pari al livello Basso (da 1 a 4). Quindi, ogni Rischio parziale deve essere ridotto al livello Basso.

Ipotizzando che ogni Contromisura ha un peso equivalente unitario, cioè, tutte riducono i rischi nella stessa quantità, il loro coefficiente nella formula per il calcolo del Rischio Aggregato (R_{Agg}), quindi, è pari a 1.

Rischio Residuo Parziale R_1 proposto:

- Rischio Parziale: $R_1 = 15$
- Nel momento in cui saranno applicate tutte le Misure identificate (C_1, C_2, C_3, C_4), il livello del del rischio R_1 dovrebbe ridursi al livello 1. Si ha, perciò, un Rischio gestito R_{G1} pari a 14 livelli. Ognuna di queste Misure riduce il rischio di una quantità pari a 3,5 (14/4=3,5). Questo in quanto abbiamo ipotizzato che nel momento in cui vengono implementate le 4 Misure, esse possono portare il rischio Parziale R_1 da 15 a 1.
- Quindi, Rischio Residuo Parziale proposto: $RR_1 = R_1 - R_{G1} = 15 - 14 = 1$.

Rischio Residuo Parziale R_2 proposto:

- Rischio Parziale: $R_2 = 16$
- Nel momento in cui saranno applicate tutte le misure identificate (C_2, C_5), il livello del R_2 dovrebbe ridursi al livello 1. Si ha, perciò, un Rischio gestito

R_{G2} pari a 15 livelli.

- Quindi, Rischio Residuo Parziale proposto: $RR_2 = R_2 - R_{G2} = 16 - 15 = 1$.

- **Rischio Residuo Parziale R_3 proposto:**
- Rischio Parziale: $R_3 = 12$
- Nel momento in cui saranno applicate tutte le misure identificate (C_2, C_6), il livello del R_3 dovrebbe ridursi al livello 1. Si ha, perciò, un Rischio gestito R_{G3} pari a 11 livelli.
- Quindi, Rischio Residuo Parziale proposto: $RR_3 = R_3 - R_{G3} = 12 - 11 = 1$.

A questo punto si può calcolare il Rischio Residuo Aggregato proposto: $RR_{Aggr} = 1$.

Dopo aver fatto una valutazione, il proprietario dei rischi ha deciso di approvare il Piano di Trattamento dei Rischi e di approvare i Rischi Parziali Residui (RR_i) proposti:

- $RR_1 = 1$

- $RR_2 = 1$
- $RR_3 = 1$
- $RR_{Aggr} = 1$

È evidente che tutti i Rischi Parziali Residui (RR_i) risultano sotto il livello di accettazione.

In seguito il proprietario deve approvare i Rischi Parziali Residui (RR_i) proposti e di procedere con l'implementazione delle Contromisure stabilite nel Piano di Trattamento dei Rischi provvedendo all'investimento alle competenze necessarie e alle risorse interne ed esterne (fornitori) e ogni altro supporto.

CASO DI STUDIO 2-ATTRAVERSAMENTO DEL PASSAGGIO A LIVELLO

Il presente Caso di Studio tratta una situazione la quale, per la natura della situazione, non è possibile seguire in modo rigoroso il processo strutturato del risk management. In questa situazione è difficile raccogliere i dati, compiere l'analisi con strumenti e tecniche e decidere opportunamente sulla base dei risultati dell'analisi strutturata. L'analisi e la valutazione che viene eseguita in questi casi sono qualitative e si basano su ragionamenti mentali del momento. Naturalmente la qualità delle decisioni dipende dalla capacità della persona nel percepire la realtà della situazione e dei fattori presenti, dalle informazioni che riesce a raccogliere e dalla sua capacità di analizzare e di valutare i rischi.

Un amico, dipendente di una azienda di servizi, si sposta al mattino per andare in ufficio a piedi con la borsa in mano che contiene documenti e il computer portatile. Sfortu-natamente per lui, questa mattina il tempo è brutto e piovig-gina. Non ha voglia di utilizzare l'automobile per problemi di parcheggio. Deve arrivare puntuale per partecipare a una riunione importante. La sua presenza alla riunione è indi-spensabile, quindi deve arrivare almeno 15 minuti prima per la necessaria preparazione. La strada che porta all'azienda incrocia un passaggio a livello lungo il quale transitano di-verse linee ferroviarie. A volte capita di aspettare anche 20 minuti davanti alle sbarre prima che esse si alzino per con-sentire il passaggio ai pedoni.

A distanza di alcune centinaia di metri, per i pedoni che non vogliono aspettare l'apertura del passaggio a livello, e voglio passare dall'altra parte, esiste un ponte sopraelevato con gli scalini in ferro.

Quando il nostro amico arriva al passaggio a livello, le sbarre sono abbassate. I treni attraversano il passaggio a li-vello e sono diretti in entrambe le direzioni. Naturalmente le sbarre rimangono abbassate durante il passaggio dei treni.

L'obiettivo del nostro amico in quel momento è di attra-versare il passaggio a livello per arrivare:

- in ufficio all'ora pianificata per partecipare alla riu-nione, e naturalmente,
- senza essere investito.

La valutazione per decidere sull'azione da seguire, do-vrebbe essere fatta in modo molto veloce.

È necessario pertanto stabilire i criteri per la gestione dei rischi, come segue:

- **Probabilità (P)**, con la quale si manifesta la causa; è valutata secondo la seguente scala: 1-Molto Bassa, 2-Bassa, 3-Media, 4-Alta, 5-Molto Alta.
- **Conseguenze (D)**, impatto verso la persona; è valuta-to secondo la seguente scala: 1-Molto Basso, 2-Basso, 3-Medio, 4-Alto, 5- Molto Alto. c)

ù

- **Rischio (R)**, calcolato come funzione della probabilità (P) e delle Conseguenze (D): R=f(PxD).
- **Priorità** con la quale occorre agire. In questo caso il va-lore del Rischio più basso, naturalmente, dovrebbe avere la priorità più alta e dovrebbe essere la soluzione prefe-ribile. Il valore più alto del Rischio dovrebbe avere la priorità più bassa e dovrebbe essere la soluzione da evitare.

Come è stato detto, lo scopo dell'attività d'identificazione dei rischi è quello di generare una lista di tutti i fattori di rischio basati su quei eventi che potrebbero compromettere o facilitare la soddisfazione degli obiettivi.

Il fattore di rischio della situazione contingente, come si nota, è il passaggio a livello chiuso e potrebbe creare il seguente risultato sfavorevole: arrivare in ritardo per la riunione.

La sbarra abbassata del passaggio a livello è il fattore di rischio; ma c'è anche un'opportunità a disposizione che po-trebbe migliorare la situazione: prendere il ponte sopraele-vato con gli scalini in ferro.

A questo punto il nostro amico analizza velocemente la situazione allo scopo di individuare la(e) causa(e). Una volta conosciuta la(e) causa(e) si potrebbe stimare il rischio che incombe sul suo obiettivo: una prima causa è dovuta ai treni che passano uno dietro l'altro senza preavviso. Anche il brutto tempo, la pioggia, la visibilità, l'agilità della persona e la borsa con i documenti e il computer portatile costituisco-no ostacoli.

Si ipotizza, pertanto, che tutte le cause pesino in ugual misura e tutte concorrono al rischio di arrivare in ritardo in riunione.

Il contesto offre le seguenti opzioni:

1. attraversare i binari.
2. Usufruire del ponte sopraelevato per i pedoni che dista alcune centinaia di metri.
3. Cambiare completamente strada allungando il percorso.
4. Aspettare che passino tutti i treni e si alzino le sbarre liberando il passaggio pedonale.

Per ogni azione dovrebbero essere identificate e valutate le potenziali minacce, ma anche i punti di debolezza (le vul-nerabilità) della situazione. La pioggia e la visibilità bassa, per esempio, sono potenziali minacce per l'attraversamento del ponte di ferro; la mancanza dell'agilità della persona, perché non è addestrata ad affrontare situazioni del genere, potrebbe costituire un punto di debolezza per l'attraversamento del ponte di ferro.

Si procede, dunque, con l'analisi delle opzioni ragionan-do sulle cause nel modo seguente:

1. attraversare i binari passando sotto le sbarre potrebbe essere una delle soluzioni. Nel momento in cui le sbarre sono abbassate tra il passaggio di un treno e l'altro. I treni, però, passano uno dietro l'altro senza preavviso. Questa scelta aumenta il rischio di essere investito.
2. Usufruire del ponte per attraversare i binari non è una scelta felice. Il ponte si trova a circa 400 metri lontano. Si deve salire e scendere le scale di ferro e per di più con la borsa in mano e non ha tanta voglia di fare queste acrobazie, anche perché pioviggina e la visibilità non è buona; si rischia così di farsi male. Nel caso decidesse per questa soluzione, alla fine, riuscirà ad arrivare in tempo per la riunione? Potrebbe avvisare il collega che ha

organizzato la riunione chiedendogli di posticiparla di almeno 15-30 minuti. Possono bastare i 30 minuti di posticipo? E poi c'è il rischio di scivolare e farsi male!

3. Cambiare completamente strada, allungando il percor-so. Anche con questa soluzione c'è il rischio di arrivare in ritardo alla riunione. Potrebbe avvisare il collega che ha organizzato la riunione, chiedendogli di posticiparla di almeno 15-30 minuti.
4. Potrebbe aspettare l'apertura del passaggio a livello, avvisando il collega che ha organizzato la riunione, chiedendogli di posticiparla di almeno 15-30 minuti. In questo caso quanto tempo deve ancora aspettare prima che si liberi il passaggio a livello? Possono bastare i 30 minuti di posticipo?

Ogni decisione sull'azione da seguire dovrebbe essere presa sulla base della valutazione dei rischi che in questo caso viene eseguita mentalmente dalla persona interessata.

Come si fa a evitare o a eliminare le cause che possono provocare il rischio del ritardo.

Come si fa a mitigare questi rischi?

Si dovrebbe pensare di agire in modo tale da ridurre la probabilità del ritardo o di ridurre l'impatto qualora si arri-vasse in ritardo. L'obiettivo è di arrivare alla riunione in tempo senza danni, agendo in fretta.

Occorre eseguire una rapida valutazione mentale dei rischi e assegnare, in seguito, un ordine di priorità alle azioni (per i criteri per la gestione dei rischi vedere il par. 7.3.5):

1. Nel caso dell'attraversamento del passaggio a livello mentre le sbarre sono abbassate la probabilità di esse-re investito è Molto Alta (P=5), in quanto non è possibi-le controllare il passaggio dei treni. Anche l'impatto è Molto Alto (D=5). Perciò, il rischio risulterebbe pari a R=25. Questa scelta, dunque, è da escludere.
2. Anche l'attraversamento del ponte di ferro predisposto per i pedoni è da escludere per le minacce sopra citate: la probabilità di farsi male potrebbe essere Alta (P=4) e l'impatto Molto Alto (D=5), poiché si tratta della salu-te. Perciò, il rischio è pari a R=20.
3. Decidere di cambiare completamente strada allun-gando il percorso la probabilità di arrivare in ritardo è Media (P=3), con un impatto sulla salute è Molto Basso (D=1). Perciò, il rischio è pari a R= 3.
4. Aspettare che passino tutti i treni e si alzino le sbarre liberando il passaggio pedonale: la probabilità di arri-vare molto in ritardo è Molto Alta (P=5) e l'impatto sulla salute è Molto Basso (D=1). Perciò il rischio è pari a R=5.

Pertanto, sulla base dei risultati della valutazione le azioni che si dovrebbe prendere in considerazione sono le terza e la quarta. Tra queste due la terza è quella preferibi-le, in quanto, la quarta azione è molto incerta sulla durata dell'apertura del passaggio a livello.

L'attività di attuazione dell'azione decisa in questo caso non richiede nessuna formalizzazione. Nel momento in cui si è deciso cosa fare si procede con le seguenti azioni:

- chiamare il collega per posticipare la riunione di almeno 30 minuti;
- far mente locale per tracciare mentalmente la strada alternativa da percorrere;
- avviarsi verso la direzione tracciata.

Durante il percorso conviene sempre controllare il tempo e il precorso allo scopo di arrivare in ufficio senza superare il tempo concordato di 30 minuti. La valutazione dell'efficacia dell'azione intrapresa dovrebbe essere continua lungo il percorso. Nel caso di nuovi impedimenti sarebbe necessario met-tersi ancora in comunicazione con il collega per concordare come procedere allo scopo di evitare di essere assente alla riunione.

Una volta appresa la lezione, per migliorare la situazione sarebbe necessario agire come segue:

- partire prima, soprattutto quando le condizioni atmosfe-riche non sono favorevoli, tutte le volte che ci sono ap-puntamenti importanti pianificati durante le prime ore del mattino;
- informarsi sugli orari di chiusura del passaggio a livello (tenendo presente che i treni non sempre sono puntuali);
- chiedere di non pianificare le riunioni importanti nelle prime ore di mattino;
- prendere in considerazione l'opportunità di presenziare alla riunione con un collegamento remoto (videoconferenza), qualora la riunione dovesse essere per forza pia-nificata durante le prime ore del mattino.

Appendice A-strumenti e tecniche per il risk management

Gli strumenti e le tecniche sono fondamentali per il processo di risk management e soprattutto per la sua efficacia ed efficienza.

Sono usati nella raccolta delle informazioni, nell'analisi del contesto (individuazione minacce e vulnerabilità, nel risk assessment, nella comunicazione interna e con gli stakeholder e in altre situazioni.

La scelta di uno strumento o di una tecnica dipende dalla situazione (dalle caratteristiche del lavoro da svolgere, dalle caratteristiche dello strumento in questione, dalla disponibilità delle informazioni, dalla facilità di utilizzo, dalla complessità delle istanze e dal costo).

Gli strumenti e tecniche possono essere classificati in s/t per dati numerici o s/t per dati non numerici in base al tipo di lavoro qualitativo o quantitativo da svolgere.

Quando le decisioni nel processo di risk management si basano su dati non numerici questi dati vengono trasformati in informazioni utili per capire quali decisioni prendere.

Spesso le decisioni sono applicate su dati numerici e le decisioni sono basate su appropriate interpretazioni statistiche.

Gli strumenti e le tecniche possono essere classificati anche in funzione del tipo di uso che se ne fa (consultazione, supporto, per analisi degli scenari, per analisi funzionali, per i controlli delle valutazioni, per le statistiche).

Vedi tabella se hai tempo.