

Titolo| Risk Management – La norma ISO 31000:2018. La metodologia per applicare efficacemente il risk management in tutti i contesti.

Ioannis Tsioras

# Risk Management

## La norma ISO 31000:2018

La metodologia per applicare efficacemente  
il risk management in tutti i contesti



Nuova edizione  
allineata alla versione ISO 31000: 2018

Seconda edizione allineata alla norma ISO 31000:2018

Autore| Ioannis Tsioras

Copertina a cura dell'autore

Facebook: [facebook.com/Ioannis.Tsioras](https://facebook.com/Ioannis.Tsioras)

Twitter: [twitter.com/iTsioras](https://twitter.com/iTsioras)

Ioannis Tsioras, 2018

ISBN | 9788891186201

© Tutti i diritti riservati all'Autore

Nessuna parte di questo libro può essere riprodotta senza il preventivo assenso dell'Autore e dell'Editore.



*Ioannis Tsioras* nasce in Grecia, dove compie gli studi classici e scientifici nella scuola dell'obbligo e in seguito si laurea in Ingegneria in Italia, dove vive da circa quarant'anni. Nell'ambito professionale le sue esperienze trovano consensi internazionali attraverso la pubblicazione di libri e articoli in riviste nazionali e internazionali e come membro esperto sull'eccellenza nel business e sul Risk Management in comitati italiani ed europei. È autore di articoli e dei seguenti libri:

- *Pensiero basato sul rischio - Risk-based Thinking*, ebook, Youcanprint, Self-publishing, 2016.
- *La sicurezza delle informazioni - Dal Sistema di Gestione alla sicurezza dei sistemi informatici. Le norme BS 7799-2 e ISO/IEC 15408 (Common Criteria)*, Milano, FrancoAngeli, 2004.
- *La progettazione del sistema di gestione nelle organizzazioni ad alta intensità informativa - Dalla ISO 9000 alla modellazione del business*, Milano, FrancoAngeli, 2005.
- *Guida alla certificazione ISO 9000 per le organizzazioni utenti e le aziende di informatica*, 1998.
- *Governo e Miglioramento dei Processi*, Milano, FrancoAngeli, 1998.

*A mia moglie*

Prefazione

Le organizzazioni di ogni tipo e dimensione nello svolgimento delle proprie attività si affacciano a delle incertezze, dovute, soprattutto, a fattori e influenze che risiedono sia nel contesto interno sia in quello esterno. Le incertezze, pertanto, sono fonti di rischi i quali hanno un effetto sul raggiungimento degli obiettivi e l'impatto potrebbe essere notevole per il business.

Le organizzazioni per far fronte a questa situazione cercano in una certa misura di gestire i rischi, adottando approcci più o meno conosciuti, a volte efficaci a volte no e spesso fanno affidamento solo alla tecnologia.

Per affrontare i rischi in modo sistematico, efficace ed efficiente, il normatore International Organization for Standardization (ISO) ha emesso una serie di norme per il rischio e per il risk management. La principale di queste norme è la ISO 31000.

La ISO 31000:2018 *Risk management – Guidelines* è applicabile a tutte le tipologie di organizzazioni (manifatturiere, di servizi, commerciali, organizzazioni governative, come anche alle organizzazioni senza scopo di lucro) e di qualsiasi dimensione e tipologia merceologica, ma potrebbe essere applicata anche a qualsiasi entità che ha la necessità di gestire i rischi. La ISO 31000 essendo una linea guida propone un framework per il risk management che è un modo sistematico e logico per la gestione efficace dei rischi dando solo indicazioni di massima senza approfondire in dettaglio i concetti e senza fornire un supporto operativo per l'applicazione efficace della metodologia che propone.

Forte di una vasta e significativa esperienza sul campo, l'autore propone ai manager, ai security manager e a tutti quelli che vogliono o che sono costretti a prendere decisioni in presenza di incertezze, una completa descrizione circa le ragioni e le modalità dell'applicazione delle prescrizioni della norma per la gestione dei rischi, esplicate anche attraverso esempi figurativi.

Il libro fornisce un metodo pratico e modulare per la gestione dei rischi approfondendo i concetti e gli approcci della norma. L'autore non si limita a interpretazioni generiche delle prescrizioni, ma sviluppa gli approcci in dettaglio attraverso matrici e calcoli dei rischi reali e fa riferimento a casi di studio portando esempi

per guidare gli interessati a gestire qualsiasi forma di rischio in modo sistematico, trasparente e credibile e in qualsiasi ambito e contesto.

Il libro presenta un'introduzione sul risk management, la Risk Governance che dà l'impostazione del framework e del processo di risk management, un approfondimento sul concetto del rischio, sui fattori di rischio, sull'entità di rischio e sulla correlazione tra gli elementi coinvolti nell'analisi dei rischi. Si illustra inoltre l'importanza del risk management nel processo decisionale, la consapevolezza verso il rischio e i benefici che possono derivare dal risk management. La partenza del framework e del processo di gestione dei rischi si fonda sui principi che guidano il risk management.

Il framework per il risk management si ispira dai principi ed è impostato secondo l'approccio Plan-Do-Check-Act, si basa sulla leadership e l'impegno della direzione e si sviluppa attraverso l'integrazione, la progettazione, l'implementazione, la valutazione e il miglioramento.

L'autore ha prestato particolare attenzione al processo del risk management sviluppando il flusso e descrivendo dettagliatamente tutte le attività: definizione del contesto, campo di applicazione, risk assessment (identificazione, analisi e valutazione dei rischi), piano di trattamento dei rischi con i controlli necessari da implementare per diminuire i rischi, calcolo dei rischi residui, accettazione dei rischi proposti, implementazione dei controlli e monitoraggio e il riesame.

Il processo di risk management sviluppato è supportato da due esempi pratici utili per apprendere e applicare la metodologia in tutti i contesti della vita delle organizzazioni, ma anche alle attività della vita privata.

## INDICE

- [1 Introduzione](#)
- [2 Risk governance](#)
- [3 Il rischio](#)
  - [3.1 Il concetto del rischio](#)
  - [3.2 Un approccio ingegneristico](#)
  - [3.3 Gli elementi coinvolti nel rischio](#)
  - [3.4 \*Risk-based thinking\*](#)
  - [3.4 Il \*Risk-based thinking\* e l'approccio per processi](#)
  - [4 Il risk management nel processo decisionale](#)
  - [4.1 La consapevolezza e il processo decisionale](#)
  - [4.2 Benefici dal risk management](#)
  - [5 I principi che guidano il risk management](#)
  - [6 Il framework per il risk management](#)
    - [6.1 Il framework basato sull'approccio PDCA](#)
    - [6.2 Leadership e impegno](#)
    - [6.3 Integrazione \(Plan\)](#)
    - [6.4 Progettazione \(Plan\)
      - \[6.4.1 Capire l'organizzazione e il suo contesto\]\(#\)
      - \[6.4.2 Articolazione dell'impegno per il risk management\]\(#\)
      - \[6.4.3 Assegnazione dei ruoli, responsabilità e autorità\]\(#\)
      - \[6.4.4 Allocazione delle risorse\]\(#\)
      - \[6.4.5 Stabilire la comunicazione e la consultazione\]\(#\)](#)
    - [6.5 Implementazione \(Do\)
      - \[6.5.1 Implementazione del framework\]\(#\)
      - \[6.5.2 Implementazione del processo di risk management\]\(#\)](#)
    - [6.6 Valutazione \(Check\)
      - \[6.6.1 Monitoraggio, misurazioni, analisi e valutazione\]\(#\)
      - \[6.6.2 Audit interno\]\(#\)
      - \[6.6.3 Riesame dell'alta direzione\]\(#\)](#)
  - [6.7 Miglioramento \(Act\)](#)
    - [6.7.1 Adattabilità](#)
    - [6.7.2 Miglioramento continuo](#)
  - [7 Il processo del risk management](#)
    - [7.1 Considerazioni generali](#)
    - [7.2 Comunicazione e consultazione](#)
    - [7.3 Campo di applicazione, Contesto e Criteri per il Risk Management
      - \[7.3.1 Considerazioni generali\]\(#\)
      - \[7.3.2 Contesto esterno\]\(#\)
      - \[7.3.3 Contesto interno\]\(#\)
      - \[7.3.4 Campo di applicazione del processo di risk management\]\(#\)
      - \[7.3.5 Criteri per la gestione dei rischi\]\(#\)](#)
    - [7.4 Risk Assessment
      - \[7.4.1 Considerazioni generali\]\(#\)
      - \[7.4.2 Identificazione dei rischi\]\(#\)
      - \[7.4.3 Analisi dei rischi\]\(#\)
      - \[7.4.4 Valutazione dei rischi\]\(#\)](#)
    - [7.5 Trattamento dei rischi
      - \[7.5.1 Considerazioni generali\]\(#\)
      - \[7.5.2 Selezione delle opzioni per il trattamento dei rischi\]\(#\)
      - \[7.5.3 Identificazione delle Misure da implementare\]\(#\)
      - \[7.5.4 Identificazione delle Misure esistenti\]\(#\)
      - \[7.5.5 Calcolo dei Rischi Residui\]\(#\)
      - \[7.5.6 Preparazione del Piano di Trattamento dei rischi\]\(#\)](#)
    - [7.6 Accettazione dei rischi](#)
    - [7.7 Implementazione delle Misure](#)
    - [7.8 Monitoraggio e riesame](#)
    - [7.9 Registrazione e reporting](#)
  - [8 Caso di studio: Il tesoretto](#)
  - [8.1 Considerazioni generali](#)

8.2 Campo di applicazione

8.3 Contesto

  8.3.1 *Contesto esterno*

  8.3.2 *Contesto interno*

8.4 Criteri per la gestione dei rischi

8.5 Risk Assessment

  8.5.1 *Identificazione dei rischi*

  8.5.2 *Analisi dei rischi*

  8.5.3 *Valutazione dei rischi*

8.6 Trattamento dei rischi

  8.6.1 *Selezione delle opzioni per il trattamento dei rischi*

  8.6.2 *Identificazione delle Misure da implementare*

  8.6.3 *Identificazione delle Misure esistenti*

  8.6.4 *Calcolo dei Rischi Residui*

  8.6.5 *Piano di Trattamento dei rischi*

8.7 Accettazione dei rischi

## [\*\*9 Caso di studio: Attraversamento del passaggio a livello\*\*](#)

9.1 Considerazioni generali

9.2 Campo di applicazione e Contesto

9.3 Criteri per la gestione dei rischi

9.4 Identificazione dei rischi

9.5 Analisi dei rischi

9.6 Valutazione dei rischi

9.7 Trattamento dei rischi

9.8 Consolidamento e miglioramento

## [\*\*10 Bibliografia\*\*](#)

## [\*\*11 Appendice A – strumenti e tecniche per il risk management\*\*](#)

## 1. introduzione

L'uomo, per la sua natura, è portato a gestire il rischio, sia in modo consapevole, stabilendo approcci strutturati e li usa tutte le volte che deve decidere, sia in modo inconsapevole. Questo avviene perché la gestione dei rischi è vitale per la sopravvivenza degli esseri viventi.

Quando si prende una decisione, si compie una valutazione dei rischi in modo istintivo; generalmente questa valutazione raramente è sistematica. Segue comunque un approccio che è quello di stabilire uno o più obiettivi, di stimare i risultati dell'azione, di confrontarli con gli obiettivi e, di conseguenza, si decide. Si compie, comunque, una valutazione durante la quale si rendono evidenti eventuali scostamenti dei risultati stimati rispetto agli obiettivi, quindi potrebbe essere necessario apportare delle modifiche alle azioni da compiere. Nella valutazione si possono ipotizzare diversi scenari e di conseguenza si dovrebbe decidere di seguire lo scenario che contiene meno incertezze e minor rischio.

La necessità di gestire i rischi è dovuta al fatto che le organizzazioni nello svolgimento delle proprie attività si affacciano a delle incertezze, dovute, soprattutto, a fattori che risiedono sia nel contesto interno sia in quello esterno. I rischi, quindi, hanno un effetto sul raggiungimento degli obiettivi e l'impatto potrebbe essere notevole per il business dell'organizzazione.

L'incertezza, dunque, è insita nelle attività umane ed è dovuta alla mancanza della "conoscenza assoluta" della situazione contingente alla quale ci si riferisce. La conoscenza assoluta è un limite invalicabile dell'uomo, poiché non riuscirà mai a possederla tutta in assoluto. Anche se si approfondisce una situazione o un aspetto, ci sarà sempre qualcosa che sfugge, con la conseguenza di avere una incertezza residua che ci porta ad avere il relativo rischio.

Per affrontare il rischio in modo sistematico e in modo efficace ed efficiente, il normatore ISO (International Organization for Standardization) ha emesso una serie di norme per il rischio e per il risk management, come la norma ISO/IEC Guide 73, la norma ISO 31000 e altre.

La ISO/IEC Guide 73 fornisce il vocabolario di base e i termini relativi al risk

management, allo scopo di sviluppare un contesto armonizzato comune per aiutare le organizzazioni a comprendere e ad aumentare la consapevolezza in materia di risk assessment.

La norma ISO 31000:2018 ha il titolo *Risk management – Guidelines* ed è applicabile a tutte le tipologie di organizzazioni (manifatturiere, di servizi, commerciali, organizzazioni governative, come anche alle organizzazioni senza scopo di lucro) e di qualsiasi dimensione e tipologia merceologica, ma potrebbe essere applicata anche a qualsiasi entità che ha la necessità di gestire i rischi.

La norma ISO 31000, essendo una linea guida, fornisce solo indicazioni senza approfondire in dettaglio i concetti. La norma potrebbe essere adottata per impostare il framework del risk management e per progettare il processo del risk management. Essendo una linea guida non può essere utilizzata per effettuare audit, tanto meno per emettere certificazioni, in quanto le sue prescrizioni non sono requisiti.

Il risk management potrebbe essere applicato su tutta l'organizzazione, ma anche in un solo processo, in una sola area, in una sola attività o progetto e in qualsiasi momento della vita dell'organizzazione, ma anche in qualsiasi momento della vita di un individuo. Potrebbe essere applicato su più livelli, come per esempio a livello strategico, a livello gestionale o tattico e a livello operativo.

Il successo della gestione dei rischi dipende dall'efficace gestione del framework per il risk management. Il framework fornisce la struttura e definisce le risorse necessarie per l'integrazione con i processi dell'organizzazione.

L'applicazione efficace del processo di risk management dipende anche da alcuni fattori chiave, come per esempio dalla "definizione del contesto" nel quale dovrebbe essere applicato il risk management e dal campo di applicazione, inteso come l'estensione dei confini del processo, dalla identificazione completa delle "parti interessate" (stakeholder) e delle loro esigenze, aspettative e requisiti, dagli obiettivi da soddisfare, nonché dai criteri di accettazione dei rischi.

I numerosi benefici che derivano dall'efficace applicazione del risk management sono elencati nella norma ISO 31000 alla quale si rimanda per avere

l'elenco completo. Si richiamano qui, a titolo di esempio, alcuni benefici chiave, come ad esempio:

- aumenta la probabilità per soddisfare gli obiettivi;
- incoraggia la gestione proattiva;
- aumenta la consapevolezza sulla necessità dell'identificazione e della gestione dei rischi;
- assicura la soddisfazione dei requisiti legali e regolamentari, come anche i requisiti delle norme sui sistemi di gestione (per esempio, ISO 9001, ISO 14001, ISO 22301, ISO 27001, e altre);
- migliora la confidenza e la fiducia degli stakeholder;
- migliora l'applicazione dei controlli;
- migliora l'allocazione e l'utilizzo efficace delle risorse;
- migliora l'efficacia e l'efficienza operativa;
- migliora la prevenzione e la gestione degli incidenti.

Il presente lavoro ha lo scopo di fornire un'introduzione sull'argomento risk management e di presentare:

- i principi che devono guidare la gestione dei rischi;
- l'infrastruttura (framework) per una efficace gestione dei rischi;
- il processo del risk management.

La governance guida il corso dell'organizzazione, le sue relazioni con il mondo esterno e il contesto interno e le regole, i processi, gli approcci e le pratiche necessari per raggiungere la sua missione. La gestione strategica traduce il governance in strategia e in relativi obiettivi per raggiungere i livelli desiderati di rendimento sostenibile e redditività a lungo termine e la soddisfazione dei propri stakeholder.

La risk governance è il modo con il quale l'organizzazione gestisce i rischi che riscontra durante le sue attività. La risk governance è, dunque, l'impostazione strategica dei processi di *risk management* e del *decision making*.

Il controllo dei fattori di rischio rende l'organizzazione robusta e affidabile.

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, e
- rendere applicabile e gestire con efficacia il processo del risk management.

La risk governance stabilisce le relazioni tra i Principi per la gestione dei rischi, il Framework nel quale si espleta il Processo del risk management e lo sviluppo e l'implementazione del Processo del risk management stesso. Queste relazioni sono rappresentate nel seguente schema (fig. 1).

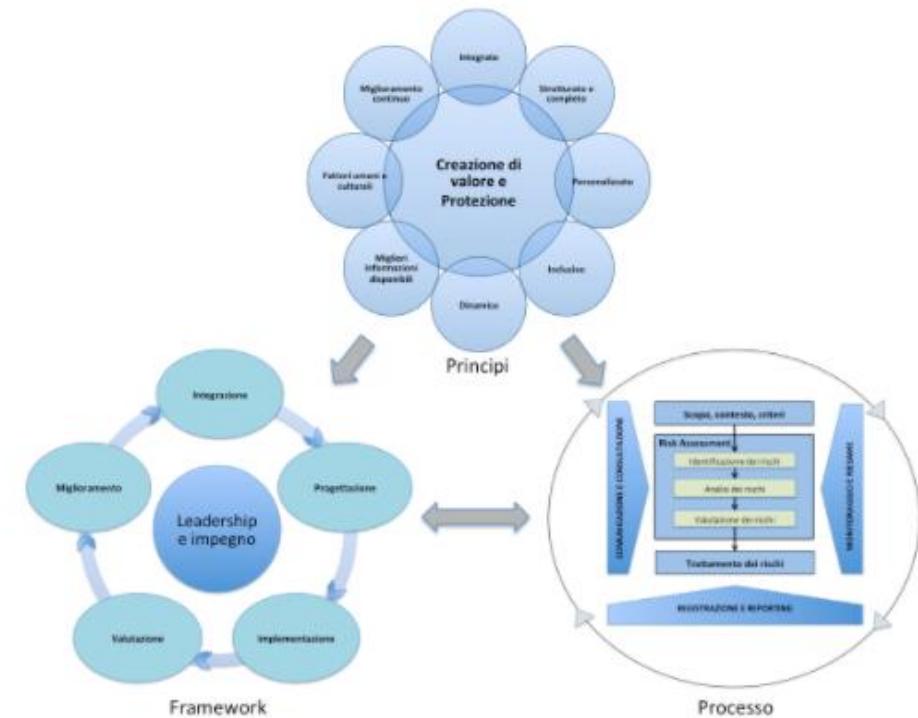


Figura 1 – Risk Governance (rif. ISO 31000: 2018)

### 3. il rischio

Come dimostrano le esperienze quotidiane di ciascuno di noi, il rischio è connaturato in tutte le attività umane. Nonostante la continua esposizione alla quale siamo soggetti, una definizione al concetto di rischio, che sia accettata da tutti, è quasi impossibile. Il rischio assume svariate accezioni in base agli ambiti sociali e culturali in cui ognuno di noi opera e in base alle diverse prospettive, attraverso le quali ognuno di noi osserva gli eventi e si espone agli eventi stessi.

Il "rischio" dal punto di vista filosofico e antropologico, in senso lato, è ineludibile, ma in ogni caso, attraverso un opportuno controllo, il rischio potrebbe essere dominabile; anche dal punto di vista ingegneristico il rischio non è del tutto eliminabile, ma sicuramente riducibile e controllabile.

Il termine "rischio", nella letteratura tecnica, si utilizza anche per indicare "la condizione o la situazione che può causare eventi sfavorevoli". Nella nuova concezione della ISO 31000, il "rischio" è espresso in termini di fonti di pericolose dipotenziali eventi sfavorevoli o favorevoli le loroconseguenze e le probabilità di accadimento. Gli eventi sfavorevoli possono portare a danni, mentre quelli favorevoli possono presentare opportunità. Pertanto, con il termine "analisi del rischio" s'intende l'individuazione delle possibili cause di un evento e le sue conseguenze.

I "rischi", dunque, possono manifestarsi nel momento in cui non si conosce la situazione contingente di un evento, i suoi stati e le condizioni di contorno. La mancanza di questa conoscenza si traduce in incertezza, in quanto, non si sa come fare per controllare l'evento stesso. Questo evento potrebbe creare una situazione di disagio e di paura e potrebbe diventare un evento sfavorevole, ma potrebbe creare anche circostanze di comodo portando a eventi favorevoli e opportunità da sfruttare.

Mentre un evento favorevole presenta delle opportunità e delle leve positive per raggiungere un obiettivo, un evento sfavorevole, invece, costituisce un ostacolo al raggiungimento dell'obiettivo, quindi, in tal senso, è un pericolo; ma non necessariamente al pericolo segue un danno; non sempre provoca effetti verso l'obiettivo. In altri termini: il pericolo è conseguente all'evento sfavorevole, mentre le

conseguenze (impatto, effetto) negative o positive, hanno una certa probabilità di seguire.

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 alla severità (magnitudo) delle sue conseguenze.

Il Rischio, quindi, è legato all'incertezza di un evento. L'incertezza aumenta con la crescita della complessità della situazione e in un contesto del genere è opportuno ridurre al minimo gli approcci empirici e intuitivi per gestire i rischi e diventa necessario adottare approcci organizzativo-ingegneristici, cioè approcci strutturati e sistematici.

In questo nostro lavoro la definizione che prendiamo in considerazione per il *Rischio* è quella data dalla norma ISO Guide 73, la quale definisce il *Rischio* come l'*effetto dell'incertezza sugli obiettivi*.

La definizione è composta dai tre termini chiave: *obiettivi, effetto e incertezza*.

Gli *obiettivi* possono:

- riguardare ambiti diversi: economico/finanziari, la salute, la sicurezza, tutela ambientale, ecc.;
- essere applicati a diversi livelli: strategico, tattivo e operativo (progetto, prodotto, processo);
- essere espressi come risultati desiderati, come uno scopo o come un criterio; possono essere espressi utilizzando parole di significato simile (obiettivo, goal o valore target da raggiungere).

L'*effetto* è una deviazione rispetto alle aspettative (positiva o negativa). L'*effetto* potrebbe essere positivo, negativo o entrambi e può portare a opportunità e minacce.

Il terzo termine della definizione è l'*incertezza*. L'incertezza è legata alla conoscenza di un processo, di un'evento, di un'entità o di una situazione.

Se si ha un obiettivo da raggiungere e non si sa nulla su come fare per soddisfarlo, se non si conosce il processo attraverso il quale l'obiettivo si può

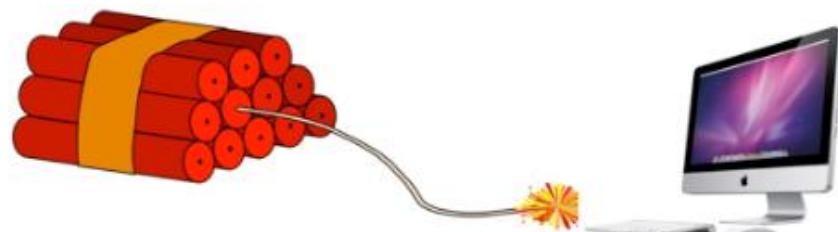
raggiungere, se non si conoscono i problemi, le fonti di pericolo, le minacce che si possono riscontrare, le varie debolezze della situazione perché mancano le informazioni sul modo di operare, allora il rischio di non soddisfare l'obiettivo è alto.

Ma anche quando si pensa di conoscere tutto, il rischio non si annulla mai, visto che la conoscenza assoluta non è possibile possederla. La sicurezza di possedere una conoscenza completa di una situazione è un'illusione. Ci sarà sempre qualcosa che sfugge alla nostra attenzione. L'esperienza, l'osservazione, l'approfondimento, il coinvolgimento delle persone esperte, aiutano ad aumentare la conoscenza della situazione.

Il Rischio dunque è legato al grado di esposizione dell'obiettivo all'incertezza della situazione contingente. Cioè, il Rischio è legato all'incertezza dell'evento o della situazione.

In riferimento all'incertezza il Rischio dipende dai seguenti due elementi (fig. 2):

- dall'incertezza, intesa come conoscenza di un evento e delle relative condizioni di contorno che si manifesta nei confronti dell'obiettivo da soddisfare;
- dall'esposizione dell'obiettivo all'incertezza, intesa come impatto, magnitudo. L'impatto potrebbe essere totale, cioè l'obiettivo non si raggiunge per niente (danno al 100%); oppure, possono esistere altre situazioni nelle quali l'obiettivo può essere soddisfatto parzialmente, cioè la perdita dell'obiettivo non è totale, ma parziale.



Fonte di pericolo

Figura 2 – Fattore di rischio: grado di esposizione all'incertezza

Il Rischio dipende dall'interazione tra la Fonte di Pericolo e l'esposizione dell'obiettivo (Bene) alla Fonte di Pericolo. La presenza contemporanea di entrambi comporta la possibilità di cagionare un impatto, cioè può compromettere la soddisfazione dell'obiettivo.

Pertanto, possiamo esprimere l'Entità di Rischio (R) con la seguente formula:

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

Ove:

- (P) è legato alla Probabilità o alla Frequenza dell'incidente in considerazione.
- (D) è legato alle conseguenze dell'evento sull'obiettivo (Impatto).
- (f) è la funzione che si sceglie per combinare (P) e (D) e dipende dal modello scelto per l'analisi.

Se l'intenzione è di salvaguardare un obiettivo, come per esempio un *Bene*, la percezione che il proprietario ha sul *Rischio* di perdere il *Bene* o di vederlo danneggiato per via delle Fonti di Pericolo presenti, che sollevano minacce, dipende dalla conoscenza che lui stesso ha sulle condizioni di contorno, cioè sulla situazione contingente.

Se si conosce il valore dell'obiettivo, cioè il valore del *Bene* nelle condizioni normali e se si conoscono le vulnerabilità della situazione reale e le minacce che incombono sul *Bene*, allora si è in grado di stimare il Rischio e di decidere opportunamente, intraprendendo Misure (controlli) adeguate per salvaguardare il *Bene*, quindi raggiungere l'obiettivo.

Gli elementi coinvolti e la dinamica che si sviluppa tra di loro lungo i processi coinvolti nella soddisfazione degli obiettivi sono illustrati nella fig. 3. Allo scopo di facilitare il ragionamento si prende in considerazione il caso in cui i rischi possono portare a effetti negativi sugli obiettivi. Un ragionamento simile si esegue nel caso

in cui l'effetto sugli obiettivi è positivo.

Quasi in tutte le situazioni ogni obiettivo ha un proprietario il quale si preoccupa per soddisfarlo. L'obiettivo potrebbe essere, per esempio, la protezione di un database o di una scatola piena di euro, il ritorno di un investimento nei tempi stabiliti, la salute di una persona, l'efficacia e l'efficienza di un processo o di un'attività, la piena riuscita di un viaggio di piacere in una crociera, l'attraversamento sicuro di una strada trafficata, il raggiungimento del budget, il lancio di un prodotto nuovo, l'obiettivo zero difetti nella produzione, ecc. È evidente che il proprietario desideri che quest'obiettivo sia raggiunto. Per assicurare la sua soddisfazione, accettando naturalmente un rischio residuo, in quanto, il rischio non può mai diventare pari a zero, è necessario analizzare il contesto in cui si opera, identificare i fattori che possono provocare ostacoli e agire di conseguenza.

La responsabilità per il raggiungimento di un obiettivo e per il controllo della situazione cade proprio sul proprietario dell'obiettivo stesso. Il ruolo del proprietario è critico, in quanto, solo lui è in grado di attribuire un valore all'obiettivo e decidere la strada per raggiungerlo.

In una situazione del genere le entità e i loro comportamenti da analizzare sono:

- l'**Obiettivo** che deve essere soddisfatto;
- il **Proprietario** dell'obiettivo;
- le **Fonti di pericolo** (agenti portatori di minacce) che possono sollevare un interesse verso l'obiettivo;
- le **Vulnerabilità** (debolezze) che sono caratteristiche della situazione reale del contesto che possono essere esplorate dalle Minacce;
- le **Minacce**, sollevate dalle Fonti di pericolo, che possono esplorare le Vulnerabilità con il conseguente effetto verso l'obiettivo;
- le **Misure** (controlli) intraprese dal proprietario per ridurre i rischi a livelli accettabili.

Osservando la fig. 3 si nota che un Proprietario ha un Obiettivo da soddisfare e

desidera mitigare o eliminare i rischi che possono incombere sulla soddisfazione dell'obiettivo.

D'altro canto, esistono sempre **Fonti di Pericolo** che attraverso **Agenti** possono sollevare **Minacce** oscacolando così la soddisfazione dell'obiettivo.

A questo punto possiamo dire che l'**Obiettivo** è un'entità soggetta a potenziali e svariate Minacce esistenti nel contesto dell'obiettivo. Il numero e la tipologia delle Minacce variano nel tempo e spesso sono note parzialmente. Il contesto nel quale ci si trova a soddisfare l'obiettivo spesso contiene anche **Vulnerabilità** (debolezze) che anch'esse variano nel tempo e anch'esse spesso sono note parzialmente. Le minacce e le vulnerabilità sono parametri probabilistici, perché si manifestano con una certa probabilità o frequenza. Le Vulnerabilità possono essere esplorate dalle Minacce creando uno o più eventi sfavorevoli (incidenti) che si manifestano nei processi attraverso i quali si arriva alla soddisfazione dell'obiettivo, arrecando così degli effetti indesiderati e quindi Rischi che incombono sull'obiettivo. Poiché un evento sfavorevole (incidente) dipende da questi due parametri probabilistici (minacce e vulnerabilità), allora anche l'evento sfavorevole o favorevole è un evento probabilistico.

L'importanza della soddisfazione dell'obiettivo spinge il suo proprietario a intervenire applicando **Misure** (controlli) appropriate contro le Minacce o contro le Vulnerabilità con lo scopo di diminuire la probabilità degli eventi associati e anche dei relativi Rischi. Spesso sono necessarie Misure adeguate per ridurre il rischio residuo a livelli accettabili. La scelta delle azioni e delle Misure da applicare deve essere compiuta in modo adeguato e in relazione ai rischi reali e può essere condizionata dalla presenza di vincoli organizzativi, tecnologici, economici e attuativi.

Lo schema nella fig. 3 è concettuale e rappresenta gli elementi coinvolti nell'analisi dei rischi e la dinamica che li correla. Lo schema è ispirato dalla norma ISO IEC 15408 (Common Criteria).

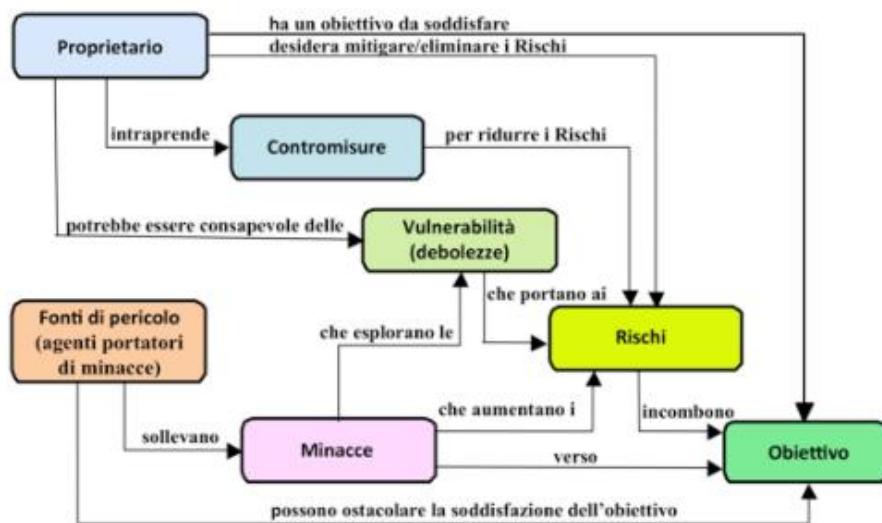


Figura 3 – Gli elementi coinvolti nell'analisi dei rischi e loro relazione (ispirato alla norma ISO/IEC 15408)

L'impostazione emergente delle norme sui sistemi di gestione, come le norme ISO 9001, ISO 14001, ISO 18001, ISO/IEC 27001, ISO 22301 e tutte le altre che si basano sull'impostazione del High Level Structure, contiene un concetto avanzato e indispensabile per garantire l'efficacia di un sistema di gestione.

Queste norme richiedono che l'organizzazione comprenda il proprio contesto e identifichi i fattori di rischio che possono portare a effetti negativi e i fattori di rischio che possono portare a effetti positivi (opportunità) come base per la pianificazione del sistema di gestione stesso. Questo rappresenta il punto di partenza dell'approccio pensiero basato sul rischio per pianificare e attuare i processi del sistema di gestione, per pianificare e per implementare le azioni da intraprendere allo scopo di affrontare i rischi e le opportunità e per misurare l'efficacia delle azioni intraprese.

Il risk-based thinking spinge l'organizzazione a stabilire un approccio sistematico e preventivo per affrontare i fattori di rischio. Si tratta di un pensiero permanente nella mente di tutti, ma soprattutto dei responsabili, quindi dovrebbe essere

interiorizzato da tutti i livelli dell'organizzazione; dovrebbe essere trasformato in un approccio che permetta di identificare i fattori di rischio il prima possibile e gestirli in modo preventivo per limitare le conseguenze negative e aumentare le conseguenze positive. I fattori di rischio portatori di minacce, vulnerabilità o punti di forza e di opportunità dovrebbero essere accertati, valutati e trattati in modo continuo durante la vita del sistema di gestione. In questo modo l'approccio diventa proattivo al fine di ridurre preventivamente gli effetti negativi e massimizzare le opportunità e decidere di conseguenza in modo consapevole.

Sebbene le norme dei sistemi di gestione specificino che l'organizzazione deve pianificare azioni per affrontare i rischi e le opportunità, non vi è alcun requisito che richieda metodi formali o un processo documentato. In questa maniera potrebbe venire a mancare la coerenza e la produzione di risultati validi a confrontabili tra loro.

Pertanto, è comprensibile il fatto che non sembra essere possibile seguire un processo strutturato come quello del risk management della ISO 31000 e sviluppato nel Cap. 7.

Qualora la situazione permettesse di dedicare del tempo per raccogliere dati reali e procedere all'analisi e alla valutazione si potrebbe seguire il processo del risk management del cap. 7, come si presenta nel Caso di Studio 1.

Qualora invece la situazione non fornisse l'opportunità di raccogliere dati, la metodologia potrebbe essere seguita con meno rigore, facendo delle valutazioni qualitative e non quantitative come nel Caso di Studio 2.

Per raggiungere e conservare un vantaggio competitivo non basta avere un buon prodotto e un buon servizio o dipendenti che si comportano da eroi o da star. Un'organizzazione popolata da eroi e da star non è un'azienda di successo. Anzi, la presenza degli eroi e delle star è sintomo di processi inefficienti e inefficienti. Il cammino verso l'eccellenza passa inevitabilmente attraverso i processi, che devono essere efficaci, efficienti e caratterizzati da un elevato grado di adattabilità. I processi progettati con cura, governati e migliorati, assicurano il successo

all'organizzazione.

I vantaggi che si ottengono con l'approccio per processi si amplificano e si moltiplicano con l'integrazione del *risk-based thinking*. La capacità di concentrare gli sforzi sui processi chiave e sulle opportunità di miglioramento, offerta dall'approccio per processi, è catalizzata dal pensiero basato sul rischio, qualora esso diventi parte integrante dei processi stessi.

Se l'approccio per processi permette la definizione degli obiettivi, delle responsabilità e delle autorità sul processo, contribuisce alla conoscenza del processo e delle sue risorse, permette di determinare le interdipendenze con altri processi e di gestire il processo con approccio sistematico per assicurare l'efficacia e l'efficienza, la gestione dei rischi aumenta la probabilità che tutto questo avvenga e che gli obiettivi stabiliti e i risultati attesi siano soddisfatti. Questo può avvenire con i controlli e i punti di controllo, che sono necessari per il monitoraggio e la misurazione delle prestazioni e sono specifici per ogni processo e variano con i rischi connessi (fig. 3.1).

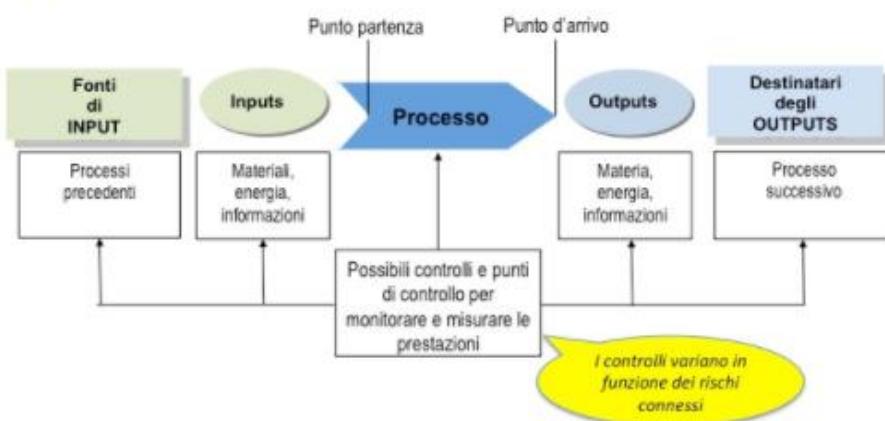


Figura 3.1 - Il *risk-based thinking* nell'approccio per processi

Il concetto del *risk-based thinking* considera il rischio parte integrante dei processi, del sistema di gestione e del modo di prendere decisioni. La gestione del rischio perciò non è indipendente e separata dai processi e dalle attività, ma diventa

un modo per gestire i processi, le attività, l'organizzazione. Con il pensiero basato sul rischio la gestione delle situazioni indesiderate diventa proattiva e non rimane reattiva.

Il *risk-based thinking* dovrebbe essere integrato nella struttura e nei processi di governance dell'organizzazione e, allo scopo di gestire ogni rischio, dovrebbe far parte del nucleo dei processi strategici, tattici e operativi. Quando il rischio è effettivamente radicato nel pensiero dei manager e integrato nei processi, allora l'organizzazione può essere veramente sicura che gli obiettivi stabiliti saranno raggiunti. L'evidenza che il rischio sia stato interiorizzato e integrato con i processi si può avere anche osservando il linguaggio dei manager nelle riunioni, nelle interviste e nei report. Se i termini "rischio", "incertezza" e "conseguenze" non sono usati, allora il concetto del rischio è poco penetrato nell'organizzazione e nei processi del sistema di gestione.

#### 4. il risk management nel processo decisionale

Ogni organizzazione di qualsiasi settore merceologico e di qualsiasi dimensione, nell'ambito del proprio business, affronta dei rischi che possono avere un impatto sulle attività, sui processi e sui progetti e quindi sugli obiettivi.

Gli obiettivi possono essere del livello strategico, tattico od operativo e possono riguardare aspetti in termini societari, ambientali, tecnologici, di sicurezza fisica e di sicurezza delle informazioni, commerciali, finanziari ed economici, come anche aspetti in termini sociali, culturali e di reputazione (fig. 4).

Tutte le attività di un'organizzazione, dunque, inevitabilmente, possono nascondere dei rischi e l'organizzazione, se è consapevole, i rischi li deve gestire. Il processo per la gestione dei rischi è il Risk Management che supporta ogni manager a prendere decisioni in presenza d'incertezze.

È pertanto raccomandabile che le organizzazioni sviluppino e implementino il processo di risk management e che questo processo venga integrato pienamente nella struttura di governo dell'organizzazione.

Le persone coinvolte nelle attività, nei processi e nei progetti, che sono critici per la soddisfazione degli obiettivi dell'organizzazione, devono interiorizzare i concetti e gli approcci del risk management; questo significa che istintivamente devono operare e prendere decisioni dopo aver analizzato e valutato i rischi che incombono sulle attività, sui processi e sui progetti critici per il business.

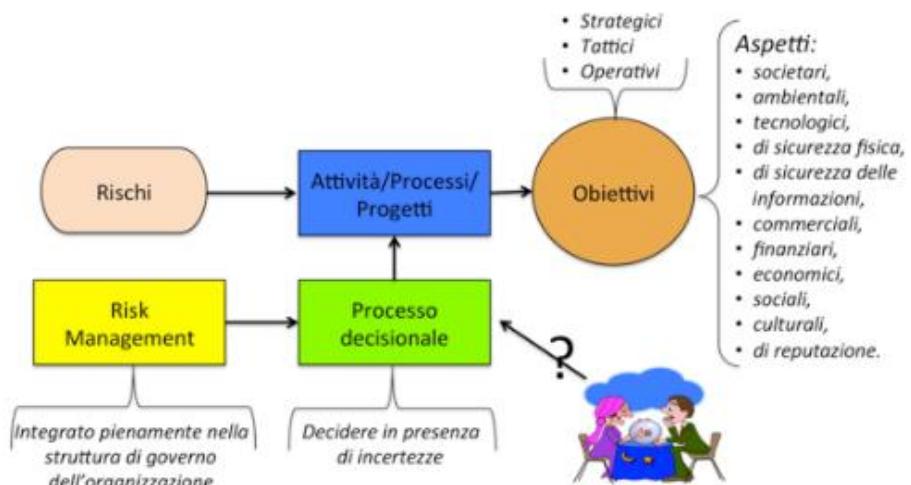


Figura 4 – Il risk management nel processo decisionale

Le decisioni prese in qualsiasi livello d'importanza e di significatività, hanno un impatto sul raggiungimento degli obiettivi e sono caratterizzate, inevitabilmente, da un qualche grado di incertezza. Questo avviene perché le decisioni si prendono sulla base delle informazioni che si hanno a disposizione, cioè sulla base della conoscenza delle condizioni della situazione e di quelle di contorno; e la conoscenza non è mai totale!

La natura e il grado d'incertezza dipendono dalla qualità, dalla quantità, dall'integrità (intesa come completezza) e dalla provenienza delle informazioni. Il metodo di raccolta e di elaborazione dei dati può variare da un'organizzazione all'altra, ma anche da un processo all'altro e questo ha un impatto enorme sulla completezza e sull'affidabilità, quindi sulla identificazione dei rischi.

Non sempre i dati disponibili sono adatti per fare previsioni e, nei casi in cui non esistono dati storici, l'identificazione dei rischi è quasi impossibile e si è costretti a prendere decisioni in assenza d'informazioni. In questa situazione l'incertezza per raggiungere gli obiettivi è molto alta.

Coloro invece che adottano il risk management, integrato nella struttura del

governo e nel processo decisionale, sono facilitati nel conoscere la tipologia e la natura dell'incertezza e riescono ad apprezzare i risultati dell'analisi e della valutazione dei rischi.

Se il risk management è radicato in modo effettivo o no nell'ambito dell'organizzazione, si nota dal linguaggio parlato e scritto dei manager, nella formulazione delle politiche, degli obiettivi e nella gestione dei processi e delle attività. Se il termine "incertezza" è usato in relazione ai rischi, significa che il concetto è entrato a fare parte del DNA dell'organizzazione.

Gli auditor, le persone preposte per valutare l'efficacia del processo di risk management, cercano evidenze sul grado d'interiorizzazione e d'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 dimostrabile attraverso azioni, dichiarazioni ed esempi reali dei manager stessi.

Le conseguenze dell'incertezza connaturata al concetto di rischio riguardano la percezione, la consapevolezza e l'accettabilità stessa del rischio. Ognuno di noi, per la nostra natura emotiva, è portato a rifiutare le situazioni di rischio; il rischio però è un elemento con cui consciamente o inconsciamente ci confrontiamo quotidianamente. In qualsiasi situazione, quando dobbiamo scegliere o decidere, in modo automatico confrontiamo le situazioni e le possibili scelte, stimando, attraverso l'intuito, i costi e i benefici che possono essere ottenuti dalla nostra decisione e scelta.

La percezione del rischio dipende da molteplici fattori non quantificabili né perfettamente identificabili quali il contesto culturale, sociale e ideologico e fattori soggettivi, psicologici ed emotivi.

La percezione e la consapevolezza sono pertanto elementi essenziali per il processo decisionale. La mancanza della consapevolezza e la scarsa applicazione di pratiche per la gestione dei rischi possono ridurre in modo significativo l'efficacia dei processi e della soddisfazione degli obiettivi.

L'accettabilità del rischio è un problema complesso e dipende almeno dalla

libertà di scelta e dalla valutazione del rapporto (\*) costi/benefici.

(\*) Costi: intesi come danni che possono essere arrecati all'uomo, all'ambiente, alla proprietà pubblica o privata e alla missione.

Il livello di accettabilità dei rischi evolve con le condizioni sociali, etiche economiche della collettività e con l'importanza che è assegnata ai valori umani, con le conoscenze scientifiche e con l'evoluzione tecnologica. Spesso l'evoluzione non è positiva, perché è proprio la stessa tecnologia a introdurre nuovi rischi, cui bisognerà in ogni caso trovare rimedio.

Il ruolo del risk management è pertanto essenziale per ottenere un quadro generale ed esauriente dell'entità dei rischi presenti, consentendo quindi l'attivazione organica della fase decisionale. La fase decisionale è riassumibile dalla definizione dei criteri di accettabilità e dalla definizione delle priorità d'intervento.

È evidente che l'introduzione del risk management dovrebbe portare all'organizzazione diversi benefici. I benefici che l'organizzazione può ottenere possono riguardare almeno i seguenti argomenti:

- il miglioramento del governo dell'organizzazione;
- il miglioramento del governo dell'organizzazione;
- l'aumento della fiducia degli stakeholder;
- l'aumento della solidità dell'organizzazione e la riduzione delle perdite;
- il miglioramento del processo decisionale;
- la soddisfazione degli obiettivi prestabiliti;
- l'introduzione della gestione proattiva;
- l'identificazione dei rischi prima possibile e la loro gestione in modo sistematico nell'organizzazione;
- il miglioramento del processo d'identificazione delle vulnerabilità (punti deboli) e delle minacce;
- la garanzia di essere conformi alle leggi.

## 5. i principi che guidano il risk management

Un'organizzazione per avere successo dovrebbe essere gestita attraverso la risk governance. La risk governance dovrebbe essere gestita in modo sistematico e trasparente. Il successo può derivare anche dall'attuazione e dall'aggiornamento del processo di risk management allo scopo di migliorare con continuità le sue prestazioni tenendo conto delle esigenze di tutte le parti interessate.

La norma ISO 31000 ha identificato otto principi per il risk management che possono essere utilizzati dall'alta direzione per guidare l'organizzazione verso il miglioramento delle prestazioni e verso l'efficacia e l'efficienza del risk management.

La creazione di valore per l'organizzazione e la sua protezione costituiscono la *vision* del risk management.

Il risk management crea valore attraverso la soddisfazione degli obiettivi e il miglioramento delle performance, per esempio: nella salute e sicurezza del personale, nella sicurezza delle informazioni, nella sicurezza stradale, nella soddisfazione dei requisiti legali e regolamentari, nella protezione ambientale, nella continuità operativa, nella prevenzione dei reati, nella gestione della qualità dei prodotti e servizi, nel miglioramento dell'efficacia e dell'efficienza dei processi, nel miglioramento della governance, nella protezione della reputazione, nel prendere decisioni, ecc. (fig. 4.1).



Figura 4.1 – Principi

Gli otto principi per il risk management possono essere interpretati liberamente come di seguito.

Il risk management non è un'attività indipendente e separata dai processi e dalle attività dell'organizzazione. Il risk management è una delle responsabilità della direzione e il processo di risk management dovrebbe essere parte integrante dei processi dell'organizzazione.

Il risk management dovrebbe far parte del nucleo di tutti i processi strategici, tattici e operativi. Questo giustifica il perché il rischio è considerato come "l'effetto delle incertezze sugli obiettivi". La struttura e i processi di governance dovrebbero contenere il risk management. Se il risk management è effettivamente radicato e attuato secondo i criteri stabiliti, allora i manager possono essere veramente sicuri che i propri obiettivi saranno raggiunti. L'evidenza che il risk management sia stato interiorizzato e integrato con i processi si può avere anche esaminando il

linguaggio dei manager nelle riunioni, nelle interviste e nei report. Se i termini "rischio" e "incertezza" non vengono usati, allora il concetto del rischio è poco penetrato nell'organizzazione.

Il management delle organizzazioni spesso si trova a gestire ambienti (situazioni e progetti) organizzativi complessi e a prendere decisioni in situazioni difficili. Il processo decisionale è uno dei fattori critici di successo nella vita dell'organizzazione ed è il risultato della sommatoria qualitativa delle singole decisioni, assunte a livello strategico, tattico e operativo; l'efficacia del processo decisionale dipende dalla qualità delle decisioni elementari assunte ai diversi livelli. A sua volta la qualità delle decisioni elementari dipende sia dalla capacità del decisore sia dalle condizioni d'incertezza in cui esse vengono assunte. Per ridurre tale incertezza è necessario ricorrere all'uso di strumenti idonei per generare conoscenze sulle condizioni esistenti al momento dell'attivazione del processo decisionale e sui possibili effetti che potrebbero derivare dalle diverse ipotesi decisionali alternative, valutati prima dell'effettiva assunzione delle decisioni. Le scelte e le decisioni, che il manager decisore compie, diventano più efficaci con l'aumento delle sue conoscenze riguardanti l'ambito e la situazione nella quale si decide. Per decidere consapevolmente è necessario, dunque, conoscere la situazione, le incertezze e la probabilità di successo della decisione che si deve prendere. Le decisioni, prese a qualsiasi livello d'importanza e di significatività, sono assunte con efficacia con l'applicazione del processo del risk management. Il risk management aiuta a fare scelte consapevoli, a dare priorità alle azioni, a distinguere gli scenari alternativi di azione e a prendere decisioni efficaci.

Il risk management prende in considerazione esplicitamente le incertezze, la loro natura e cause e come devono essere gestite.

Un approccio sistematico, strutturato e tempestivo del risk management contribuisce a ottenere risultati consistenti, comparabili e affidabili e a raggiungerli in modo efficiente.

Gli elementi in ingresso al processo di gestione dei rischi devono basarsi su sorgenti d'informazioni accertate, come a dati storici, esperienze, informazioni di ritorno dagli stakeholder, informazioni basate su osservazioni, previsioni e giudizi di esperti. Tuttavia, le persone preposte per decidere devono essere consapevoli circa le limitazioni dei dati o dei modelli usati o la possibilità di divergenza dei giudizi degli esperti.

Il risk management deve essere personalizzato per allinearla alla realtà del contesto interno ed esterno, nonché al profilo dei rischi dell'organizzazione.

Il risk management deve riconoscere le capacità, le percezioni e le intenzioni delle persone esterne e interne che possono facilitare o ostacolare il conseguimento degli obiettivi dell'organizzazione.

Un appropriato e tempestivo coinvolgimento degli stakeholder e, in particolare, dei preposti per decidere a tutti i livelli dell'organizzazione, assicura che la gestione dei rischi rimanga rilevante e aggiornata. Il coinvolgimento degli stakeholder permette, inoltre, di essere adeguatamente rappresentati e di aver i loro punti di vista nel determinare i criteri di rischio.

Il risk management sente e risponde continuamente al cambiamento. Con il verificarsi degli eventi nel contesto esterno e interno e con il monitoraggio e il riesame degli eventi stessi emergono ancora nuovi rischi, alcuni di questi cambiano nel tempo e altri scompaiono.

Le organizzazioni dovrebbero sviluppare e attuare strategie permanenti per migliorare in modo continuo la gestione dei rischi accanto a tutti gli aspetti dell'organizzazione.

Il miglioramento continuo delle prestazioni complessive del risk management dovrebbe essere un obiettivo permanente. Si dovrebbe porre l'accento sul miglioramento continuo del risk management attraverso la definizione degli obiettivi di performance dell'organizzativa, la misurazione, il riesame e la successiva modifica

dei processi, sistemi, risorse, capacità e competenze. L'organizzazione dovrebbe migliorare con continuità l'idoneità, l'adeguatezza e l'efficacia del processo di risk management. I miglioramenti ottenuti dovrebbero essere pubblicati e comunicati. L'alta direzione dovrebbe intraprendere dei riesami periodici per valutare e per assicurare la continua idoneità, adeguatezza ed efficacia del framework, nonché del processo di risk management. I risultati di questi riesami dovrebbero includere decisioni relative a opportunità per il miglioramento continuo e le possibili necessità per apportare cambiamenti al framework e al processo del risk management.

## 6. il framework per il risk management

Il framework (infrastruttura) è l'impostazione che permette di integrare efficacemente il processo del risk management nel sistema di gestione aziendale. L'integrazione dovrebbe avvenire nell'ambito dello specifico contesto e su tutti i livelli di applicazione (strategico, tattico, operativo). Per questo motivo ogni organizzazione dovrebbe adattare i vari componenti del framework alle proprie specifiche esigenze.

L'impostazione del framework dovrebbe seguire l'approccio Plan-Do-Check-Act (PDCA). La norma ISO 31000 non richiama espressamente l'approccio PDCA, ma è evidente che l'impostazione che ha dato per il framework segue questo approccio (fig. 5).

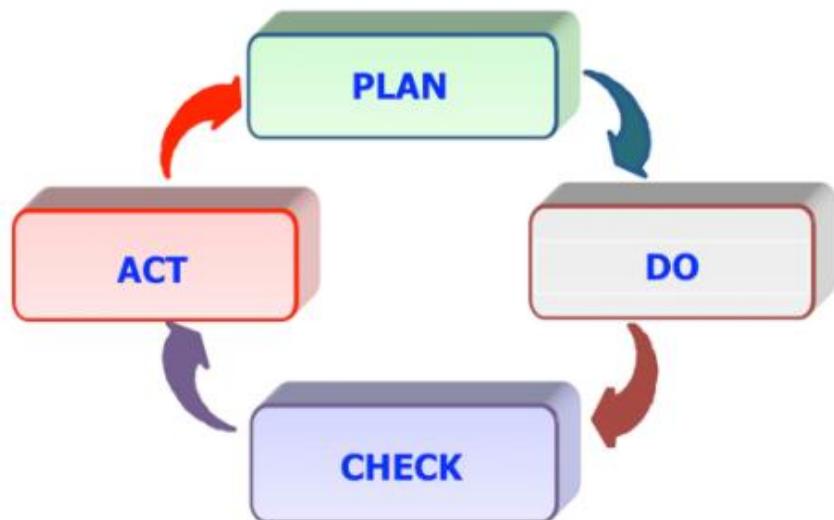


Figura 5 - L'approccio Plan-Do-Check-Act (PDCA)

<b>Plan</b> (Stabilire)	<i>Progettare il framework per il risk management</i>
<b>Do</b> (Implementare e operare)	<i>Implementare il framework e applicare il processo del risk management</i>
<b>Check</b> (Monitorare e riesaminare)	<i>Monitorare e riesaminare il framework e il processo del risk management</i>
<b>Act</b> (Mantenere e Migliorare)	<i>Mantenere e migliorare il framework</i>

Personalizzando in dettaglio il framework del risk management nell'ambito del PDCA si ha la seguente impostazione (fig. 6).



Figura 6 - Relazione tra i componenti del framework nel processo PDCA

L'alta direzione e tutti i ruoli rilevanti dell'organizzazione, dovrebbero essere caratterizzati da una forte leadership riguardo al risk management e dovrebbero essere in grado di dimostrarla.

La leadership può essere dimostrata con la motivazione e con la crescita delle persone e dei gruppi nell'ambito del risk management.

La leadership e l'impegno sono necessari per assicurare l'efficacia e l'efficienza del processo di risk management. L'impegno dovrebbe essere dimostrato attraverso una rigorosa pianificazione strategica, tattica e operativa. A questo proposito

l'alta direzione dovrebbe:

- stabilire e approvare la policy per il risk management;
- assicurare che la policy per il risk management sia compatibile con la direzione strategica dell'organizzazione;
- assicurare che la policy per il risk management sia allineata alla cultura dell'organizzazione;
- assegnare ruoli, responsabilità e autorità ai livelli appropriati dell'organizzazione relativi al risk management;
- assicurare l'integrazione del processo di risk management con i processi strategici, tattici e operativi dell'organizzazione;
- mettere a disposizione risorse adeguate per il risk management;
- stabilire indicatori per misurare le prestazioni del risk management e per assicurare la loro integrazione con le misurazioni delle prestazioni dell'organizzazione;
- assicurare la soddisfazione dei requisiti legali e regolamentari;
- comunicare i benefici ottenuti dal risk management a tutti gli stakeholder;
- assicurare la continua adeguatezza del framework per il risk management;
- promuovere il continuo miglioramento del framework e del processo di risk management;
- dare supporto ai rilevanti ruoli di responsabilità allo scopo di dimostrare la loro leadership e il loro impegno nelle proprie aree di responsabilità, secondo le necessità.

Inoltre, l'altra direzione dovrebbe:

- definire i criteri e i livelli di accettazione dei rischi;
- condurre i riesami periodici per valutare l'idoneità, l'adeguatezza, l'efficacia e l'efficienza del framework e del processo di risk management;
- dimostrare il suo impegno verso il miglioramento continuo.

La risk governance (Cap. 2) determina la responsabilità di gestione dei rischi e

dei ruoli di supervisione all'interno di un'organizzazione, in quanto essi sono parti integranti della governance dell'organizzazione.

Ogni organizzazione modella la propria struttura in funzione dei propri scopi, obiettivi e complessità dei processi.

Allo scopo di assicurare la completa integrazione e penetrazione del risk management con i processi è necessario conoscere molto bene la struttura dell'organizzazione e i suoi contesti.

I rischi esistono ovunque nell'organizzazione, in qualsiasi punto dei processi e della struttura e ogni persona dovrebbe essere sensibilizzata e responsabilizzata per identificare e segnalare ogni fattore di rischio prima possibile.

È evidente, dunque, che l'integrazione del risk management con la struttura dell'organizzazione e i processi è legata al grado d'interiorizzazione del concetto del rischio da parte delle persone e in modo particolare dai manager. Si tratta di un processo dinamico e iterativo e dovrebbe essere personalizzato, ritagliato su misura in funzione delle esigenze, della cultura, della complessità dei processi, del livello tecnologico e del contesto.

Il processo del risk management dovrebbe essere integrato e vincolato in tutti i processi (strategici, tattici e operativi) e in tutte le attività dell'organizzazione in modo tale da essere pertinente, efficace ed efficiente. La gestione dei rischi, dunque, dovrebbe essere fatta dentro i processi.

Prima ancora di iniziare con qualsiasi attività di risk management è opportuno determinare il contesto esterno e interno dell'organizzazione. Determinare il contesto significa definire i parametri di base per gestire i rischi.

Il contesto (esterno e interno) di un'organizzazione, a prescindere dalla sua dimensione (grande o piccola), dalle sue attività e dai suoi prodotti o dalla sua tipologia (a scopo di lucro o non a scopo di lucro), è soggetto a cambiamenti in modo continuo; di conseguenza, il contesto esterno e quello interno dovrebbero essere monitorati costantemente. Tale monitoraggio dovrebbe permettere all'organizzazione di identificare, valutare e gestire i rischi che possono incomberne sulle

parti interessate e sulle loro mutevoli esigenze ed aspettative.

L'alta direzione dovrebbe assumere decisioni che si riferiscono al cambiamento organizzativo e all'innovazione in modo tempestivo, al fine di mantenere e migliorare le prestazioni dell'organizzazione.

Per l'identificazione del contesto è necessario approfondire:

<b>Il contesto esterno nel quale l'organizzazione opera e affronta le sfide</b>	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.
---	--

<b>Il contesto interno dell'organizzazione</b>	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.
--	--

<b>Capire le esigenze e le aspettative degli Stakeholder</b>	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 con i responsabili dovrebbero dimostrare e articolare il loro impegno per il risk management attraverso una politica o altra dichiarazione.

L'impegno per il risk management espresso attraverso la politica dovrebbe:

- essere appropriato agli scopi dell'organizzazione;
- assicurare il collegamento tra gli obiettivi, le politiche operative e la politica per la gestione dei rischi;
- dichiarare la necessità dell'integrazione del risk management nella cultura dell'organizzazione;
- guidare l'integrazione del risk management con i processi di business e con il processo decisionale;
- stabilire le responsabilità e le autorità per la gestione dei rischi;
- mettere a disposizione le risorse necessarie;
- essere comunicato all'interno dell'organizzazione;
- essere disponibile agli stakeholder, per quanto necessario, in funzione della loro importanza;
- definire il modo per gestire i conflitti d'interesse;
- contenere l'impegno per mettere a disposizione le risorse necessarie a

supporto dei responsabili per la gestione dei rischi;

- contenere le modalità per misurare le prestazioni della gestione dei rischi e le modalità di reporting;
- essere riesaminata a intervalli prestabiliti allo scopo di valutare la sua idoneità nel tempo e quando si apportano significanti cambiamenti all'organizzazione;
- includere l'impegno per il miglioramento continuo.

L'alta direzione con i vari responsabili dovrebbe assicurare le responsabilità, le autorità e le competenze necessarie dei ruoli rilevanti per la gestione dei rischi. Le responsabilità e le autorità dovrebbero estendersi anche nell'implementazione e nel mantenimento del processo di risk management. Tutto questo potrebbe essere fatto attraverso:

- l'identificazione dei proprietari dei rischi ai quali è stata attribuita adeguata responsabilità e autorità;
- l'identificazione dei responsabili per sviluppare, implementare e mantenere aggiornato il framework del risk management;
- l'identificazione delle persone responsabili situate nei vari livelli dell'organizzazione per il processo di risk management;
- stabilendo le responsabilità per le misurazioni delle prestazioni e per il reporting interno ed esterno e la gestione delle eventuali escalation;
- garantendo adeguati livelli di riconoscimento.

L'alta direzione con i responsabili dovrebbe:

- enfatizzare che il risk management è una responsabilità primaria;
- identificare le persone che hanno la responsabilità e l'autorità per la gestione dei rischi (proprietari dei rischi).

L'organizzazione dovrebbe determinare e fornire le risorse necessarie (finanziarie, umane, competenze, metodologie, approcci, strumenti, tecnologia, ecc.) per stabilire, implementare, mantenere e migliorare il framework del risk management.

L'organizzazione dovrebbe riesaminare periodicamente la disponibilità e l'adeguatezza delle risorse identificate e le azioni da intraprendere. I risultati di questi riesami dovrebbero essere utilizzati anche come elementi in ingresso nei riesami da parte dell'alta direzione.

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 nelle attività di risk management dovrebbe possedere la competenza necessaria. Tale competenza dovrebbe essere acquisita sulla base di un adeguato grado di istruzione, addestramento, abilità ed esperienza.

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 comprendere una continua comunicazione con gli stakeholder interni ed esterni, offrendo una gamma completa e frequente di rapporti sulle prestazioni della gestione dei rischi, come parte di una buona governance. Allo scopo di decidere in modo coerente e di trattare i rischi in

conformità ai criteri dei rischi, la comunicazione dovrebbe essere impostata come un processo a due vie. Per un'efficace gestione della comunicazione dovrebbe essere preparato a intervalli prefissati un'esauriente reporting sulla gestione dei rischi.

L'organizzazione dovrebbe determinare i canali di comunicazione e di reporting verso gli stakeholder interni.

Per assicurare che la comunicazione sia efficace ed efficiente sarebbe opportuno sviluppare e implementare un piano. La comunicazione, in ogni caso, dovrebbe rispettare i requisiti legali e regolamentari.

Il piano dovrebbe stabilire:

- cosa comunicare: obiettivi, informazioni, risultati, ecc.;
- quando comunicare: quando preparare i report;
- con chi comunicare: ruoli, alta direzione, dipendenti;
- chi dovrebbe comunicare;
- le modalità di consultazione con gli stakeholder interni.

I canali di comunicazione e di reporting dovrebbero essere adeguati alla politica per il risk management dell'organizzazione e dovrebbero essere efficaci ed efficienti.

L'organizzazione dovrebbe determinare i canali della comunicazione e di reporting con gli stakeholder esterni. Come stakeholder esterni si possono prendere in considerazione per comunicare, in funzione della situazione, i clienti, eventuali partner, la comunità locale, i media, ecc. La comunicazione con gli stakeholder esterni diventa necessaria soprattutto quando si tratta della gestione dei rischi in caso di crisi o in caso di eventi che possono mettere in difficoltà l'organizzazione.

Per assicurare una comunicazione efficace ed efficiente sarebbe opportuno sviluppare e implementare un piano. Il piano dovrebbe stabilire quello che deve essere comunicato agli stakeholder esterni e in quale occasione. La comunicazione, in ogni caso, dovrebbe rispettare i requisiti legali e regolamentari.

La comunicazione con l'esterno dovrebbe essere tale da rinforzare la fiducia degli stakeholder verso l'organizzazione.

Per l'implementazione del framework l'organizzazione 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.

L'organizzazione dovrebbe stabilire e documentare il processo del risk management, compresi i criteri dei rischi che dovrebbero includere:

- i criteri per l'accettazione dei rischi,
- i criteri per l'esecuzione della valutazione dei rischi.

Ogni implementazione del processo è un'istanza. Tutte le volte che viene applicato il processo dovrebbe essere implementato in modo strutturato seguendo l'approccio stabilito.

Il processo di risk management dovrebbe produrre risultati consistenti, validi, ripetibili e comparabili.

Il processo di risk management dovrebbe essere implementato a tutti i livelli dell'organizzazione e a tutte le funzioni.

Il processo del risk management è descritto in dettaglio nel **Capitolo 7**.

## **7. il processo del Risk Management**

Il processo di Risk Management coinvolge in modo sistematico l'applicazione delle politiche, delle procedure e delle best practices nella comunicazione e nella consultazione, nella definizione del contesto, nella valutazione, nel trattamento, nel monitoraggio e riesame, nella registrazione e nelle attività di reporting dei rischi.

Il processo di Risk Management è composto dalle seguenti fasi (fig. 7):

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

Il processo di Risk Management viene espletato attraverso le istanze. Ogni istanza è un'applicazione particolare del processo, per trattare un determinato evento o fattore di rischio sfavorevole o favorevole. Ogni istanza dovrebbe essere coerente con il processo di management delineato nel framework e dovrebbe essere applicato in modo sistematico, efficace ed efficiente.

La sequenza delle attività del processo di risk management, la prima volta che viene implementato, generalmente, è la seguente: Campo di applicazione, Contesto

e Criteri, Risk Assessment, Trattamento dei rischi, Accettazione dei rischi e Implementazione delle Misure. Le attività di Comunicazione e Consultazione e il Monitoraggio e Riesame devono essere espletate in modo continuo lungo tutto il processo del Risk Assessment.

In seguito le attività dovrebbero continuare in modo che i rischi siano rivalutati e il loro trattamento sia rivisto in momenti opportuni. Questo è necessario in quanto la conoscenza del contesto, quindi anche dei rischi, potrebbe arricchirsi con nuove informazioni, nuovi intuizioni e nuove idee.

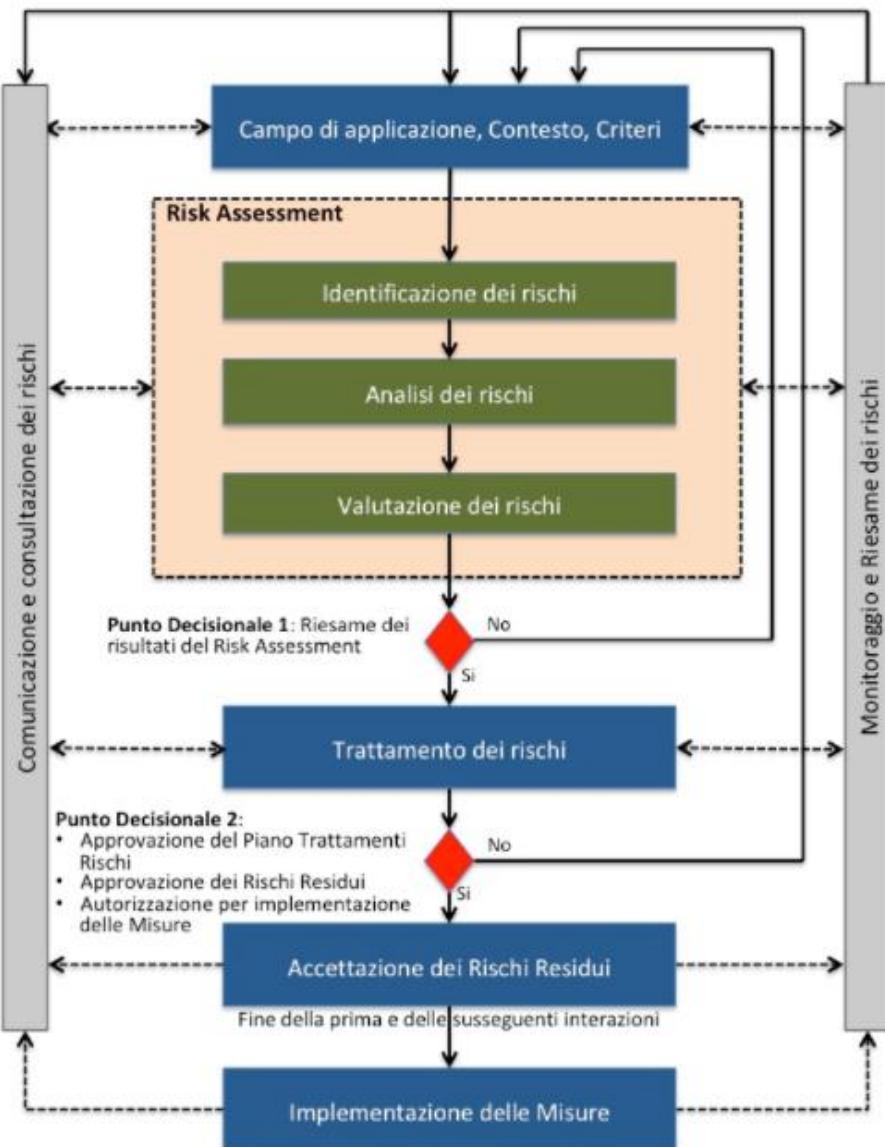


Figura 7 - Il processo di Risk Management

Comunicazione e la Consultazione dovrebbe avvenire in modo continuo durante tutto il processo di Risk Management.

Sarebbe pertanto necessario stabilire i canali e i mezzi da usare per garantire un processo di Comunicazione e Consultazione efficace ma anche efficiente. Per questo dovrebbero essere sviluppati piani e/o procedure per stabilire i canali e i mezzi che devono essere utilizzati e chi deve comunicare e con chi, quando e cosa dovrebbe essere comunicato.

La persona che deve soddisfare uno o più obiettivi, inevitabilmente, riscontra delle difficoltà, dovute alle vulnerabilità e alle minacce che incombono sui processi attraverso i quali intende soddisfare gli obiettivi.

La persona interessata dovrebbe sollecitare e gestire la Comunicazione e la Consultazione con gli stakeholder; egli dovrebbe gestire il rischio in modo da soddisfare gli obiettivi e coinvolgere tutti gli stakeholder esterni ed interni all'organizzazione che possono essere interessate al soddisfacimento degli obiettivi.

Tenendo presente che i rischi possono manifestarsi in ogni momento, la Comunicazione e la Consultazione dovrebbero estendersi in modo efficace ed efficiente lungo tutto il processo del Risk Management (fig. 8).

Come si nota nello schema della fig. 7, la Comunicazione e la Consultazione non è una fase in serie al processo di Risk Assessment e del Risk Treatment. La

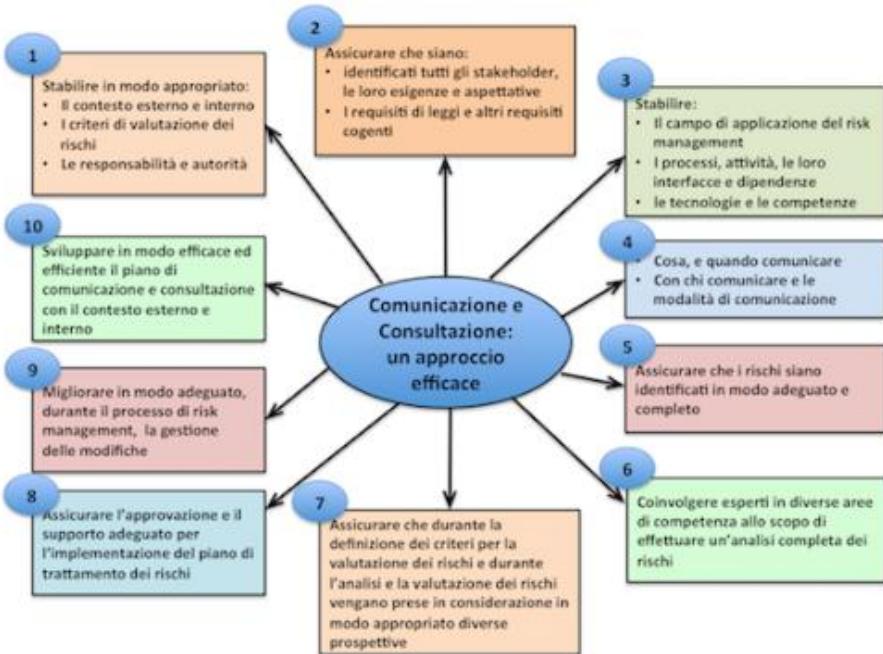


Figura. 8 – Approccio efficace della Comunicazione e Consultazione nel Risk Management

Lo scopo di queste attività è quello di personalizzare il processo di Risk Management rendendo efficace il Risk Assessment e il risk Treatment (trattamento).

Pertanto, è necessario stabilire:

- il campo di applicazione (confini ed estensione del processo del Risk Management);
- il contesto esterno;
- il contesto interno;
- i criteri per la gestione dei rischi (i criteri per la valutazione dei rischi, i criteri per la valutazione delle conseguenze e i criteri per l'accettazione dei rischi).

Stabilire il contesto significa definire i confini entro i quali dovrà essere applicato il processo di Risk Management. In questo contesto l'organizzazione

stabilisce e articola i suoi obiettivi, definisce i parametri interni ed esterni da prendere in considerazione durante la gestione dei rischi e stabilisce i criteri per i rischi.

È possibile che diversi di questi parametri siano identici a quelli che sono stati identificati durante la progettazione del framework del Risk Management, ma durante la presente attività essi dovrebbero essere presi in considerazione e sviluppati dettagliatamente e in particolare dovrebbero essere personalizzati al campo di applicazione e agli obiettivi per il quale si applica il processo di Risk Management.

Supponiamo, per esempio, che un manager abbia bisogno di soddisfare gli obiettivi relativi a un progetto; il processo del Risk Management viene attuato per gestire i rischi che incombono sulle attività di quel progetto. In tal caso il contesto interno è composto dalle attività del progetto stesso, mentre il contesto esterno riguarda tutto quello con il quale si interfaccia il progetto. Perciò è necessario familiarizzare con tutti gli aspetti e con i parametri interni ed esterni coinvolti, nonché con i requisiti applicabili.

È necessario perciò stabilire l'estensione e i confini di azione e di responsabilità e tutti i fattori che possono sollevare rischi rilevanti per la soddisfazione degli obiettivi del progetto in questione.

Il contesto esterno è l'ambiente esterno nel quale l'organizzazione deve soddisfare i suoi obiettivi.

La comprensione del contesto esterno è importante allo scopo di assicurare che gli obiettivi e le aspettative degli stakeholder siano stati considerati in modo completo. In realtà tutto questo dovrebbe essere sviluppato nel momento dell'analisi per la definizione del contesto del framework, ma qui tutto deve essere analizzato in dettaglio compreso i requisiti cogenti, le percezioni degli stakeholder e altri aspetti che possono sollevare rischi verso gli obiettivi.

Il contesto esterno potrebbe includere, almeno, quanto segue:

- la situazione economica e finanziaria;
- la posizione di mercato;
- i clienti e i requisiti contrattuali;

- il comportamento della concorrente a livello internazionale, nazionale e regionale;
- gli impegni e i rapporti con il mondo esterno;
- l'ambiente fisico;
- la tecnologia, la connettività e la trasmissione dati;
- l'ambiente culturale e sociale;
- la gestione delle alleanze/joint venture;
- le leggi e i regolamenti delle associazioni di categoria;
- i fattori guida e le tendenze;
- le relazioni con gli stakeholder, le loro percezioni e i loro valori;
- la comunicazione con le autorità locali;
- i subappaltatori;
- i vicini.

Il contesto interno è l'ambiente interno nel quale l'organizzazione opera per soddisfare i suoi obiettivi.

È necessaria per tanto la definizione e l'analisi di questo ambiente diventa necessaria in quanto potrebbe nascondere delle situazioni di pericolo che possono influenzare i processi attraverso l'organizzazione soddisfa gli obiettivi.

Il contesto interno dovrebbe essere stabilito, in quanto le organizzazioni, senza un ambiente ben definito, non riescono a operare in modo concreto e applicare il processo del Risk Management.

Pertanto è necessario stabilire il contesto interno di applicazione del processo di Risk Management.

Il contesto interno potrebbe includere, almeno, quanto segue:

- la governance, la struttura organizzativa, i ruoli, le responsabilità e i rapporti reciproci;
- le politiche, gli obiettivi e le strategie messe in atto per raggiungerli;
- le capacità delle risorse, le conoscenze e le competenze (per esempio, capitale, tempo, processi, sistemi, approcci e tecnologia);

- i rapporti con gli stakeholder, la loro percezione e i loro valori;
- la cultura dell'organizzazione;
- i sistemi informativi, i flussi delle informazioni e il processo decisionale formale e informale;
- le norme, le linee guida e i modelli a disposizione dell'organizzazione;
- la forma e l'estensione delle relazioni contrattuali.

Il campo di applicazione del processo di Risk Management potrebbe riguardare tutta l'organizzazione o una sua parte; è pertanto necessario stabilire l'estensione e i confini del dominio entro il quale si ha intenzione di applicare il processo di Risk Management. Naturalmente il campo di applicazione e i confini dipendono dalla particolarità degli obiettivi, dalla tipologia dei processi e dalla organizzazione stessa.

Il campo di applicazione deve prendere in considerazione i fattori identificati nell'analisi del contesto esterno ed interno, i requisiti degli stakeholder, nonché le leggi e i regolamenti applicabili; gli obiettivi e i target da soddisfare, le strategie e tutte le informazioni inerenti agli obiettivi.

Dall'analizzare il contesto interno ed esterno così come è stato descritto nei paragrafi precedenti (7.3.2 e 7.3.3), si procede con l'analisi per stabilire il campo di applicazione del processo di Risk Management.

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.

Com'è stato specificato al par. 3.2, l'Entità di Rischio si può esprimere con la seguente formula:

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

Un evento sfavorevole o favorevole possiede la potenzialità di causare un impatto, nel senso che potrebbe ostacolare o facilitare il raggiungimento degli obiettivi. Come abbiamo visto il rischio è legato alla probabilità (o frequenza) (P) del verificarsi dell'evento e alla severità (magnitudo) delle sue conseguenze (D).

L'esperienza ha messo in atto due approcci per il risk assessment:

- l'approccio analitico, e
- l'approccio empirico che usa la *Matrice di Rischio* o *Matrice di Probabilità*.

L'approccio analitico sviluppa in modo dettagliato la funzione  $R = f(P, D)$ . L'entità di Rischio (R) è associata a un determinato fattore di rischio, cioè a una determinata minaccia che esplora e sfrutta una determinata vulnerabilità.

Minaccia e vulnerabilità sono due cause di un evento sfavorevole (incidente), nel caso in cui il rischio porta a conseguenze negative, cioè associato a un danno. Nel caso in cui il rischio porta a conseguenze positive (opportunità da sfruttare con effetti positivi sugli obiettivi), allora le cause sono dei fattori di forza e o situazioni favorevoli.

L'utilizzo dell'approccio analitico richiede conoscenze particolari sull'analisi

delle probabilità degli eventi, perché richiede l'analisi e la stima delle probabilità delle cause (per esempio, delle minacce e delle vulnerabilità) e la loro combinazione e l'applicazione risulta essere più difficile.

L'approccio empirico che utilizza la *Matrice di Rischio* o *Matrice di Probabilità* risulta più facile da utilizzare. Per questo motivo e per evitare i calcoli complicati, la valutazione dei rischi, in seguito, si baserà su questo approccio empirico.

Pertanto, i criteri per la gestione dei rischi sono:

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 magnitudo dell'impatto derivanti dal verificarsi dell'evento sfavorevole/favorevole collegato a uno specifico fattore di rischio, il quale, se si manifesta, può ostacolare/facilitare il raggiungimento di un obiettivo stabilito.

Pertanto occorre creare una scala con i diversi valori delle conseguenze. Questa scala è un riferimento per la metodologia che viene adottata dall'organizzazione.

La granularità della scala dipende dal livello di dettaglio che si vuole avere nella scala dell'entità dei rischi.

A titolo di esempio viene riportata qui una scala qualitativa per le conseguenze, che si userà in seguito per il calcolo dell'entità dei rischi:

- Molto Basso: 1
- Basso: 2
- Medio: 3
- Alto: 4
- Molto Alto: 5

I livelli delle conseguenze possono essere strutturati utilizzando una scala da 1 a 10, oppure in valore percentuale. Tutto dipende da come si decide di lavorare.

La probabilità di avvenimento dell'evento sfavorevole/favorevole collegato a uno specifico fattore di rischio che può ostacolare/facilitare il raggiungimento di un obiettivo stabilito esprime la frequenza con la quale si manifesta l'evento stesso.

La granularità della scala può variare in funzione del livello di dettaglio della scala dell'entità dei rischi che si decide da adottare.

A titolo di esempio è riportata una scala qualitativa della Probabilità, che si userà in seguito per il calcolo dell'entità del rischio:

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

I livelli di probabilità possono essere strutturati utilizzando una scala da 1 a 10, oppure in valore percentuale. Tutto dipende da come si decide di lavorare.

Uno degli strumenti largamente usato per la rappresentazione grafica del rischio è la *Matrice dei Rischi* o *Matrice di Probabilità*.

Partendo dalla formula  $R = f(P, D)$  si crea la matrice bidimensionale con i due parametri Probabilità (P) e Conseguenza (D).

La combinazione dei valori dei due parametri (P) e (D) crea, nel nostro esempio presentato nella fig. 9, all'interno della matrice, i livelli da 1 a 25 che sono i livelli dei Rischi ( $R$ ). Il numero dei livelli dipende dai livelli di (P) e (D). Per esempio, nel caso in cui il livello di Probabilità è  $P=3$  e quello delle Conseguenze è  $D=4$ , allora il livello di Rischio è pari a  $R=12$ , ecc..

Inoltre, in funzione delle esigenze, ad ogni livello potrebbe essere associato un valore economico.

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>B</b>	4	6	8
Medio (3)	3	6	<b>M</b>	12	15
Alto (4)	4	8	12	<b>A</b>	20
Molto Alto (5)	5	10	15	20	25

Figura 9 – Matrice dei Rischi, Criteri di valutazione dei Rischi.

Facendo riferimento alla Matrice dei Rischi del paragrafo precedente, le tre aree: Area bianca (B), Area arancione (M) e Area rossa (A), rappresentano i tre macro-livelli di accettazione dei Rischi ( $R$ ) (fig. 10).

Pertanto i livelli, la tipologia e la priorità dell'intervento, secondo il nostro esempio, sono:

Area	Macro-livelli	Entità di rischio	Priorità di intervento
B	1-4 (rischio accettabile)	Bassa (B)	Bassa
M	5-14 (rischio da ridurre)	Media (M)	Media
A	15-25 (rischio da ridurre immediatamente)	Alta (A)	Alta

Figura 10 – Criteri di accettazione dei rischi

I livelli quindi da 1 a 4 possono essere considerati come Rischio Residuo Accettabile ( $RR_{ac}$ ) al di sopra del quale qualsiasi rischio dovrebbe essere ridotto. Questo significa che il livello di rischio Alto (A) deve essere ridotto immediatamente e con priorità alta, mentre il livello di rischio Medio (M) deve essere ridotto con priorità media.

Risk Assessment si svolge attraverso le attività d'Identificazione, Analisi e Valutazione dei rischi (fig. 11).

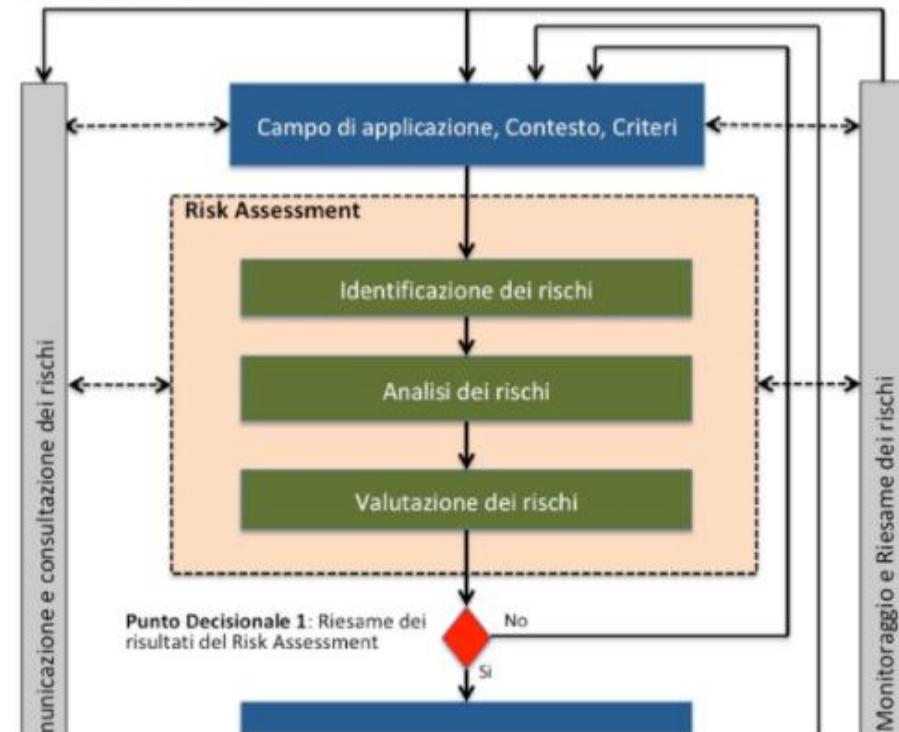


Figura 11 – Le attività del Risk Assessment

Durante l'attività d'identificazione dei rischi l'organizzazione dovrebbe individuare le fonti degli eventi (sfavorevoli o favorevoli), gli eventi stessi (incluso i cambiamenti delle circostanze), gli agenti portatori delle cause, le cause stesse (minacce, vulnerabilità, opportunità e punti di forza) le aree d'impatto, gli scenari di concatenamento delle cause e le loro conseguenze.

Lo scopo dell'attività d'identificazione dei rischi è quello di generare una lista di tutti i fattori di rischio basati su quegli eventi che potrebbero compromettere o facilitare la soddisfazione degli obiettivi.

È necessaria, pertanto, una comprensione completa ed esaustiva della

situazione, in quanto i rischi devono essere identificati al più presto possibile. Quanto più tardi si scoprono i rischi, tanto più critica diventa la situazione e l'impatto sugli obiettivi diventa maggiore.

L'identificazione dei rischi dovrebbe prendere in considerazione anche eventuali fonti, fattori e agenti esterni, che non sono sotto il diretto controllo dell'organizzazione, compresi quei fattori che sono apparenti e non sono evidenti e i loro impatti sugli obiettivi devono essere analizzati durante questa attività.

L'identificazione dei fattori e delle fonti, che possono sollevare delle cause come minacce, vulnerabilità, opportunità e punti di forza, dovrebbero essere eseguita in modo continuo attraverso il coinvolgimento di persone esperte e creando appositi gruppi di lavoro che sono capaci di immaginare possibili cause e scenari e possono stimare le loro conseguenze.

È pertanto necessario che l'organizzazione metta in atto strumenti e tecniche adeguate, idonei e coerenti con la realtà per l'identificazione dei rischi. Nell'Appendice A sono riportate indicazioni utili per gli strumenti che sono sviluppati nella norma ISO 31010, da utilizzare durante l'identificazione dei 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.

Nella fig. 11.1 è rappresentata la correlazione tra causa-evento-impatto (conseguenza). La spinta provocata dalla mano è la causa minaccia, l'instabilità delle pedine è la causa vulnerabilità, l'evento sfavorevole è il movimento delle pedine e l'impatto è la caduta delle pedine.

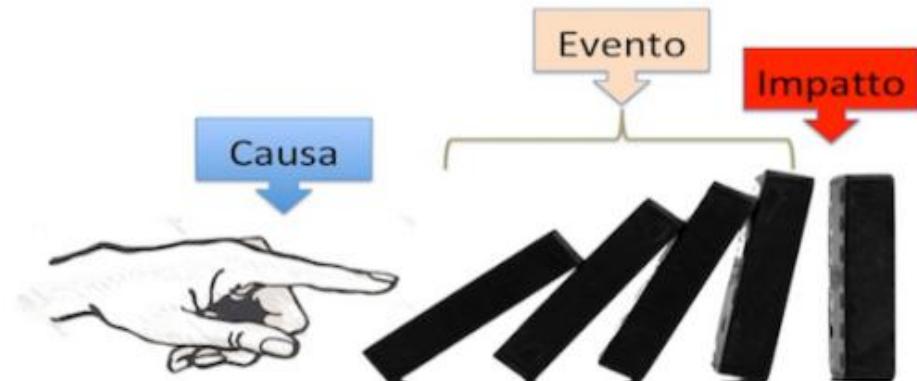


Figura 11.1 – La catena Causa-Evento-Impatto (Conseguenze)

Una tecnica veloce e facile da usare nell'identificazione e nell'analisi dei rischi è l'Analisi Bow-tie (farfallino, papillon) (fig. 11.2) (v. ISO 31010).

#### Bow tie Analysis (ISO 31010: 2009)

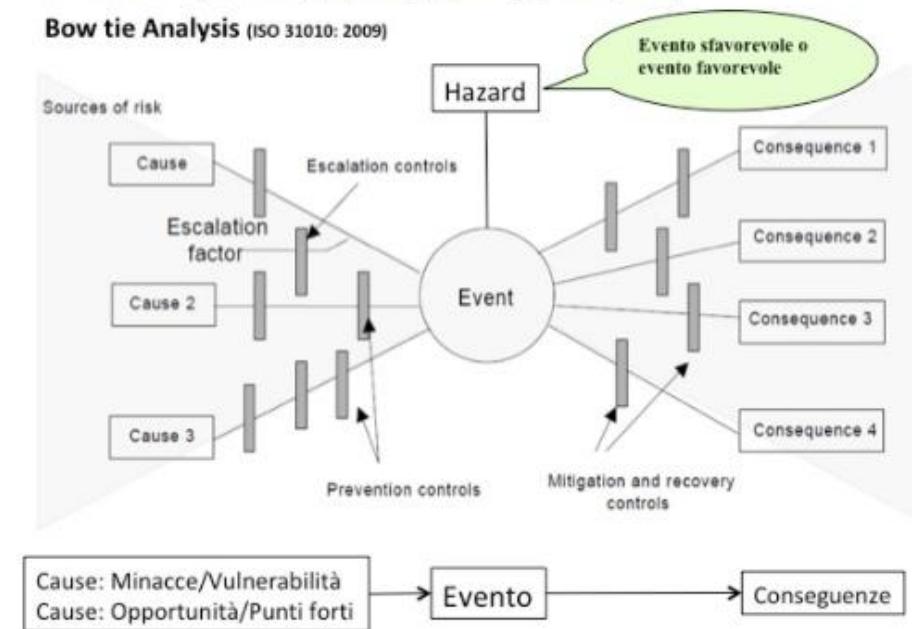


Figura 11.2 – Bow-tie analysis

L'analisi Bow-tie si svolge disegnando un diagramma che ha la forma del

farfallino.

Si costruisce identificando prima di tutto l'evento sfavorevole o favorevole. Al centro abbiamo l'evento, a sinistra le varie cause, a destra le conseguenze collegate. Le cause possono essere, in funzione della tipologia dell'evento, minacce e vulnerabilità oppure opportunità e punti di forza. Si possono collegare più Bow-tie (una causa può essere una conseguenza di un altro evento) per vedere le interdipendenze tra i vari elementi.

Nella fig. 12 è rappresentato un fumatore che si gode la sua sigaretta.

Per identificare e analizzare i rischi che incombono su questa persona, è necessario prima di tutto identificare il suo obiettivo in termini di salute. Naturalmente, come tutti, l'obiettivo del fumatore è di vivere bene senza problemi per la salute. Si analizza, pertanto, la situazione per identificare l'evento che in questo caso è un sfavorevole. S'identificano gli agenti portatori delle cause e le cause stesse (minaccia e vulnerabilità) e, infine, le eventuali conseguenze (impatto).



- Obiettivo:.....
- Evento sfavorevole:.....
- Vulnerabilità:.....
- Agente portatore di minaccia:.....
- Impatto/conseguenza:.....
- Misure preventive:.....
- Misure di mitigazione:.....

Figura 12 – Esempio di analisi dei rischi di un fumatore

Nella fig. 12.1 è riportata una soluzione dell'analisi dei rischi di un fumatore

utilizzando il metodo Bow-tie.

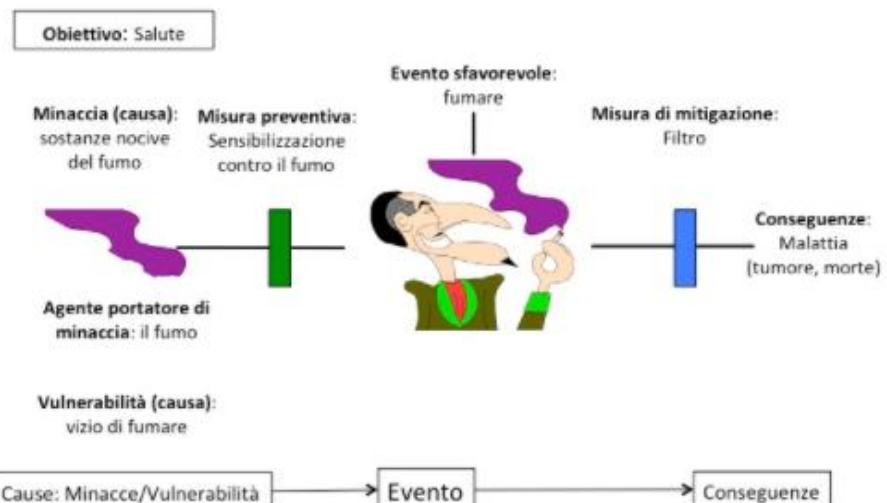


Figura 12.1 – Un esempio di soluzione dell'analisi dei rischi di un fumatore con il metodo Bow-tie.

Durante questa attività si analizzano i rischi in modo approfondito allo scopo di aumentare la conoscenza sul contesto interno ed esterno e di aumentare la consapevolezza sui rischi che incombono su di essi.

L'approfondimento delle fonti di pericolo dovute a fattori fisico-ambientali, organizzativi e tecnologici (cioè, gli agenti, le minacce, le vulnerabilità, le opportunità e i punti di forza), che sono state identificate durante la precedente attività, è materia dell'attività di Analisi dei rischi.

Una minaccia quando esplora una vulnerabilità può creare un evento sfavorevole il quale potrebbe ostacolare la soddisfazione degli obiettivi. Analogamente, un punto di forza potrebbe favorire una situazione accelerando la soddisfazione di un obiettivo.

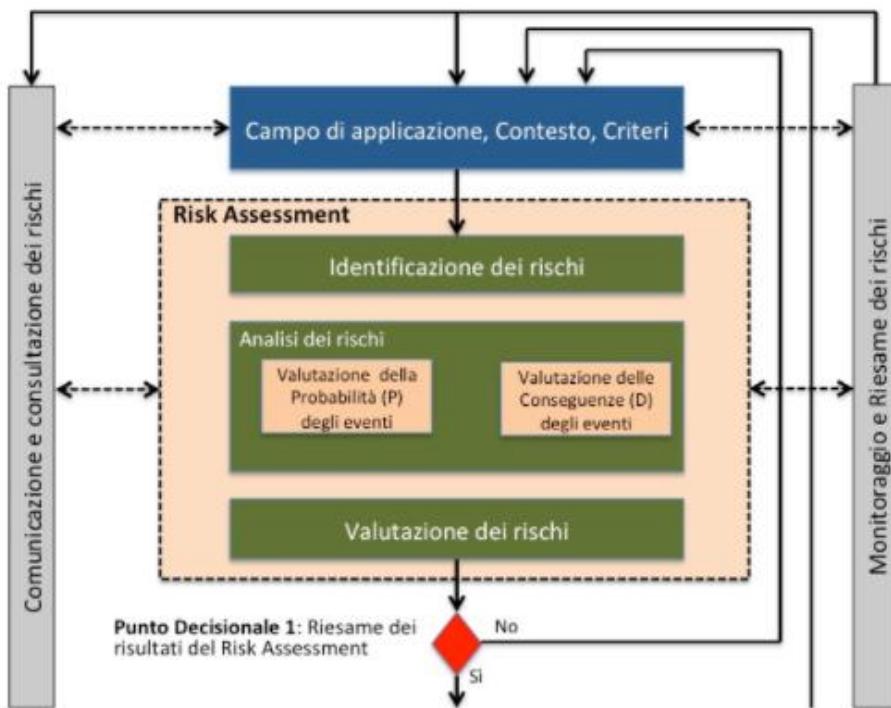


Figura 13 – Le attività di Analisi dei rischi

L'analisi dei rischi, dunque, è l'attività attraverso la quale, sulla base della situazione reale rilevata durante l'attività d'identificazione dei rischi, si valuta (fig. 13):

- le potenziali **Conseguenze (D)** sugli obiettivi;
- la **Probabilità (P)** di accadimento dell'evento sfavorevole considerato che può impedire la soddisfazione dell'obiettivo o degli obiettivi.

Nel paragrafo 7.3.5 *Definizione dei criteri per la gestione dei rischi*, si è stabilita la scala dei livelli delle **Conseguenze (D)** che sono: *Molto Basso, Basso, Medio, Alto, Molto Alto* e la scala dei livelli della **Probabilità (P)**: *Molto Basso, Basso, Medio, Alto, Molto Alto*.

La **Probabilità (Pi)** di un evento sfavorevole, è la combinazione delle due

probabilità, cioè, della **probabilità della Minaccia ( $P_m$ )** con la **probabilità della Vulnerabilità ( $P_v$ )**. Quindi, possiamo la probabilità dell'evento sfavorevole è:  $P_i = f(P_v, P_m)$ . La probabilità di una vulnerabilità esprime la facilità con la quale una determinata minaccia esplora e sfrutta una determinata vulnerabilità.

È, pertanto, necessario stimare la **probabilità della Minaccia ( $P_m$ )** (nel senso della frequenza con la quale una minaccia si manifesta) e la **probabilità o la facilità** con la quale una minaccia può esplorare e sfruttare una o più **Vulnerabilità ( $P_v$ )** e creare un evento sfavorevole provocando un incidente con impatto negativo sulla soddisfazione degli obiettivi.

A questo punto s'identificano tutte le potenziali **Minacce (M)** e tutte le potenziali **Vulnerabilità (V)**. Esse possono essere del tipo fisico-ambientale, organizzativo e logico (per le tecniche informatiche).

In ogni caso, per facilitare il compito, conviene analizzare separatamente ogni vulnerabilità e di studiare la probabilità con la quale essa può essere esplorata o sfruttata da una minaccia e che possa creare un incidente, quindi un rischio per gli obiettivi. È possibile che la stessa vulnerabilità possa essere sfruttata da una seconda minaccia creando così un secondo incidente che porta a un secondo rischio e così via. Ogni rischio così identificato è un **Rischio Parziale  $R_i = f(P_v, P_m, D) = f(P_i, D)$** .

Nello stesso modo una minaccia potrebbe sfruttare più vulnerabilità, creando così altri **Rischi Parziali ( $R_i$ )**.

Le conseguenze di una vulnerabilità potrebbero essere multiple come anche la presenza di una minaccia che potrebbe sfruttare più vulnerabilità.

È pertanto necessario che l'organizzazione metta in atto strumenti e tecniche adeguati, idonei e coerenti con la situazione reale per effettuare l'Analisi dei rischi. Indicazioni molto utili per gli strumenti sono riportati nell'Appendice A e sono sviluppati nella norma ISO 31010.

Partendo dai risultati dell'analisi si procede con la valutazione dei rischi. Lo scopo è quello di calcolare i rischi e di effettuare la comparazione tra i livelli dei

rischi riscontrati con i criteri di accettazione dei rischi.

Le decisioni dovrebbero tener conto il contesto del rischio più ampio e includere le considerazioni della tolleranza dei rischi a carico di soggetti diversi dall'organizzazione che beneficia del rischio. Le decisioni devono essere effettuate in conformità con i requisiti legali, normativi, regolamentari e altri requisiti.

In alcune circostanze, la valutazione dei rischi può portare a decidere di effettuare ulteriori analisi. La valutazione dei rischi può anche portare a decidere di non intraprendere ulteriori misure per ridurre i rischi o sfruttare le opportunità, mantenendo solo i controlli esistenti e accettando i rischi senza modificarne la situazione. Questa decisione sarà influenzata dall'atteggiamento dell'organizzazione verso i rischi e dai criteri di rischio che sono stati stabiliti.

Ogni potenziale evento sfavorevole può creare un rischio parziale per gli obiettivi da soddisfare e, come si è detto, la combinazione tra minacce e vulnerabilità possono provocare diversi incidenti che possono essere indipendenti tra di loro. Lo stesso ragionamento vale anche per gli eventi favorevoli.

Ogni Rischio Parziale viene calcolato utilizzando la *Matrice del Rischio* (fig. 9). Sulla base del risultato che viene ottenuto per ogni Rischio Parziale ( $R_i$ ), incrociando le **Conseguenze (D)** con la **Probabilità ( $P_i$ )** di ogni incidente si ha il corrispettivo valore:  $R_i = f(P_i, D)$ .

Ogni Rischio Parziale ( $R_i$ ) dovrebbe essere calcolato separatamente e dovrebbe essere trattato indipendentemente dagli altri.

Questo approccio può essere usato per identificare le situazioni che potrebbero avere il maggiore impatto sul raggiungimento degli obiettivi. L'approccio serve per prendere decisioni e per individuare gli impatti più gravi per i quali ci si dovrebbe preoccupare di affrontare con urgenza.

La decisione viene presa sulla base dei criteri di accettazione dei rischi (fig. 10).

I Rischi Parziali ( $R_i$ ) che sono stati valutati di Entità Bassa (di livello da 1 a 4), e sono cioè tollerabili, hanno un impatto minimo sugli obiettivi e nella gerarchia della gestione degli aspetti possono non essere trattati a meno che il proprietario degli obiettivi riconosce qualche beneficio.

Il ragionamento che si è fatto finora si riferisce ai singoli Rischi Parziali ( $R_i$ ). Così facendo si ha una visione parziale dei rischi e manca la visione del rischio complessivo che incombe sugli obiettivi. La ponderazione di tutti i Rischi Parziali ( $R_i$ ) forma il cosiddetto **Rischio Aggregato ( $R_{Agg}$ )**; la combinazione per ottenere il valore ponderato del Rischio Aggregato ( $R_{Agg}$ ) dovrebbe essere in funzione del contesto e della tipologia degli incidenti. Il valore che si ottiene dà un'indicazione di massima del rischio complessivo che incombe sugli obiettivi. Il Rischio Aggregato ( $R_{Agg}$ ) potrebbe essere la media aritmetica ponderata (o media pesata) che viene calcolata sommando i valori dei Rischi parziali ( $R_i$ ), ognuno moltiplicato per un coefficiente (detto anche peso) che ne definisce l'"importanza" di ogni  $R_i$ , e dividendo tutto per la somma dei pesi (quindi è una combinazione lineare convessa dei dati in analisi).

In questo caso la formula per il calcolo del Rischio Aggregato ( $R_{Agg}$ ) per  $n$  Rischi Parziali ( $R_i$ ) è:

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

dove  $f_i$  è il peso del termine  $i$ -esimo Rischio parziale ( $R_i$ ). Questo significa che è necessario conoscere il peso con il quale ogni Rischio parziale ( $R_i$ ) contribuisce al Rischio Aggregato ( $R_{Agg}$ ).

Nel caso in cui tutti i pesi  $f_i$  hanno valore unitario, la media aritmetica ponderata si riduce in media aritmetica semplice:

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

Il Rischio Aggregato ( $R_{\text{Agg}}$ ) potrebbe essere calcolato utilizzando anche altre formule che possono essere in funzione del contesto e della tipologia degli eventi.

Il livello di confidenza con il quale si arriva a calcolare il Rischio Aggregato ( $R_{\text{Agg}}$ ) dipende dall'approfondimento e dalla conoscenza che si ha sulla situazione reale. Non si deve dimenticare in questo caso l'incertezza con la quale si arriva alla conclusione. Il coinvolgimento di esperti e di persone che conoscono il contesto può aiutare ad avere un risultato attendibile, in quanto, l'analisi dei rischi viene svolta attraverso la conoscenza approfondita delle fonti di pericolo che minano le condizioni di contorno delle attività/processi e possono impedire la soddisfazione degli obiettivi.

In ogni caso il Rischio Aggregato ( $R_{\text{Agg}}$ ) dà solo un'indicazione su tutti i rischi che incombono su un obiettivo e aiuta a decidere sulle opzioni da seguire (v. par. 7.5.2); non aiuta, invece, a lavorare sulla loro riduzione o eliminazione. La riduzione o eliminazione deve avvenire agendo su ogni Rischio Parziale ( $R_i$ ) implementando Misure idonee.

L'attività di Valutazione dei rischi termina elencando i Rischi parziali ( $R_i$ ) con i rispettivi livelli stimati e con la priorità con la quale occorre intervenire per ridurre o per eliminare i rischi. La valutazione dello scenario dei risultati dell'entità di rischio dovrà stabilire le priorità di intervento per tutti i rischi. Naturalmente la priorità maggiore va assegnata a quei rischi di entità tale da rendere l'azione di riduzione o eliminazione urgente (Area rossa nella Matrice dei Rischi). I rischi per i quali gli interventi di riduzione, pur urgenti, possono essere programmati sul medio o lungo periodo sono quelli che sono posizionati nell'Area arancione.

È pertanto necessario che l'organizzazione metta in atto strumenti e tecniche adeguati, idonei e coerenti con la situazione reale per effettuare la Valutazione dei rischi. Indicazioni utili per gli strumenti sono riportati nell'Appendice A e sono sviluppati nella norma ISO 31010.

Il trattamento dei rischi parte dall'elenco dei Rischi Parziali ( $R_i$ ) con i rispettivi livelli stimati e con la priorità con la quale occorre intervenire per ridurre o per

eliminare i rischi.

Prima di iniziare le attività del trattamento dei rischi è opportuno procedere con un riesame dei risultati che provengono dalla fase precedente. Questo riesame costituisce il **Punto Decisionale 1** ed è una valutazione dei risultati del Risk Assessment. Si tratta di una valutazione critica costruttiva e nel caso in cui si riscontrano scostamenti rispetto ai risultati attesi è necessario tornare indietro e confrontarsi con quello che è stato stabilito durante l'identificazione del contesto di applicazione del processo di risk management. Durante la valutazione è necessario coinvolgere tutti gli stakeholder interessati, i quali, nel caso di esito positivo dei risultati, dovranno dare l'approvazione per procedere con l'attività di trattamento dei rischi.

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

- selezione delle opzioni per il trattamento dei rischi;
- identificazione delle Misure da implementare;
- identificazione delle Misure esistenti;
- calcolo dei Rischii Residui;
- preparazione del Piano di Trattamento dei Rischii;

La fig. 14 illustra in dettaglio l'attività relative al Trattamento dei rischi nell'ambito del processo risk management presentato nella fig. 7.

Il trattamento dei rischi si sviluppa con la scelta di una o più delle seguenti opzioni:

- modificare i rischi;
- accettare i rischi;
- evitare i rischi;
- condividere o trasferire i rischi.

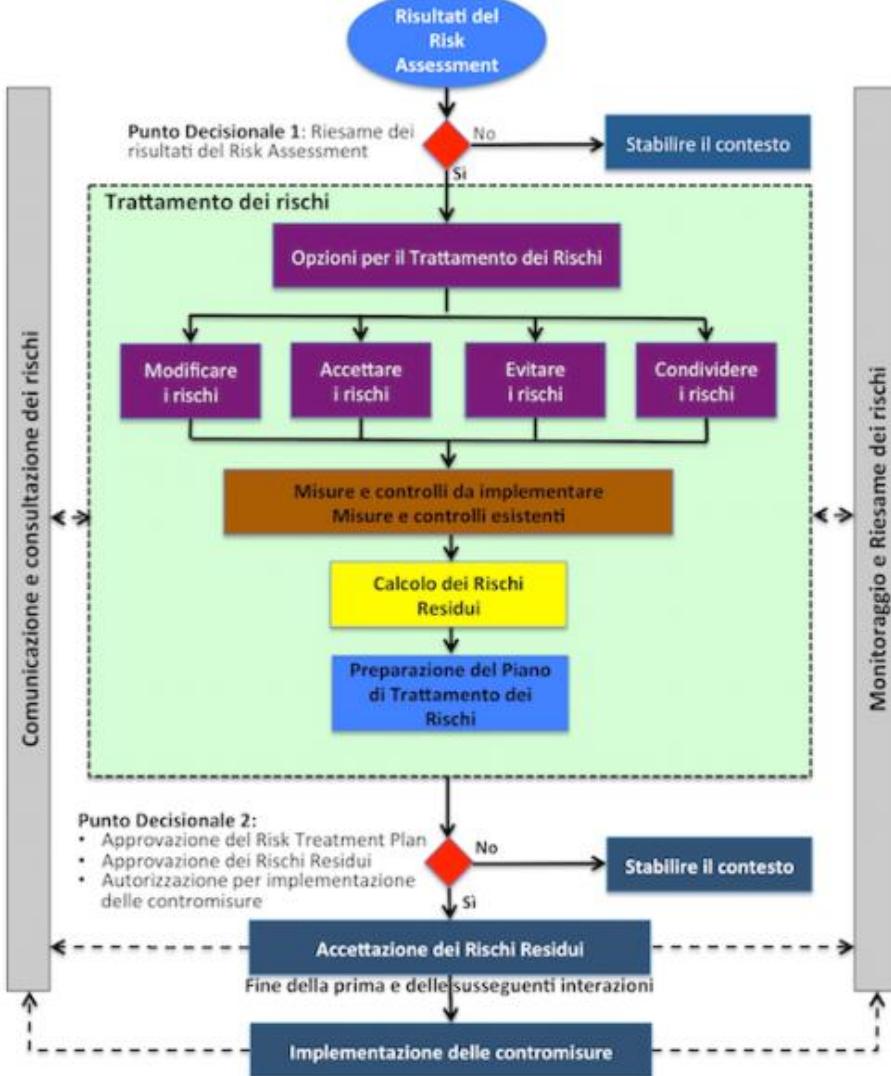


Figura 14 – Le attività del Trattamento dei Rischi

Le opzioni per il trattamento dei rischi dovrebbero essere scelte sulla base del valore del rischio Aggregato ottenuto con il risk assessment e sulla base dei costi che devono essere stimati per l'implementazione delle opzioni scelte e dei benefici stimati, dei costi stimati per l'implementazione delle opzioni scelte e dei benefici.

In linea generale si devono preferire le opzioni con le quali si stima che con il minimo sforzo si ottiene il massimo dei benefici.

Le quattro opzioni non si escludono mutualmente. Esse possono essere applicate singolarmente o in combinazione. Spesso una loro combinazione è la migliore soluzione che porta ad avere alti benefici. A titolo di esempio si cita la combinazione tra l'opzione per la modifica dei rischi con la condivisione o il trasferimento dei rischi e l'accettazione dei rischi residui. Alcuni trattamenti possono essere indirizzati a più rischi contemporaneamente (per esempio, addestramento e consapevolezza).

Selezionando l'opzione più appropriata porta a bilanciare i costi e gli sforzi di attuazione in relazione ai benefici derivanti, per quanto riguarda i requisiti legali, normativi e altri, come la responsabilità sociale e la protezione dell'ambiente naturale.

Quando si selezionano le opzioni di trattamento, l'organizzazione dovrebbe considerare i valori e le percezioni degli stakeholder e dei modi più appropriati per comunicare con loro. A volte le opzioni scelte impattano anche altre parti interessate al di fuori del campo di applicazione; in ogni caso questi dovrebbero essere coinvolti nelle decisioni.

È evidente che alcune Misure possono introdurre nuove vulnerabilità le quali possono portare a nuovi rischi. Un tale rischio può essere il fallimento o l'inefficacia totale o parziale della contromisura introdotta. È pertanto necessario monitorare e riesaminare continuamente il trattamento dei rischi allo scopo di dare la garanzia che le Misure rimangano efficaci.

I paragrafi che seguono approfondiscono le quattro opzioni.

I rischi devono essere trattati con l'introduzione o con la modifica delle Misure

in modo che il rischio residuo sia accettabile.

Le Misure da selezionare devono essere adeguate e giustificabili per soddisfare le esigenze per il trattamento dei rischi. Tale selezione dovrebbe tener conto i criteri di gestione dei rischi, nonché i requisiti legali, regolamentari e contrattuali. La selezione dovrebbe tener conto anche i costi e i tempi per l'attuazione delle Misure e gli aspetti tecnici, ambientali e culturali.

In generale le misure possono essere del tipo preventivo e di mitigazione (fig. 14.1).

Le misure preventive vengono intraprese per impedire/sollecitare il verificarsi dell'evento sfavorevole/favorevole e agiscono sulle cause dell'evento riducendo/aumentando la probabilità di accadimento e si agisce sul grado di esposizione dell'obiettivo all'incertezza. Le misure di mitigazione, invece, vengono intraprese per ridurre/aumentare le conseguenze al verificarsi dell'evento sfavorevole/favorevole.

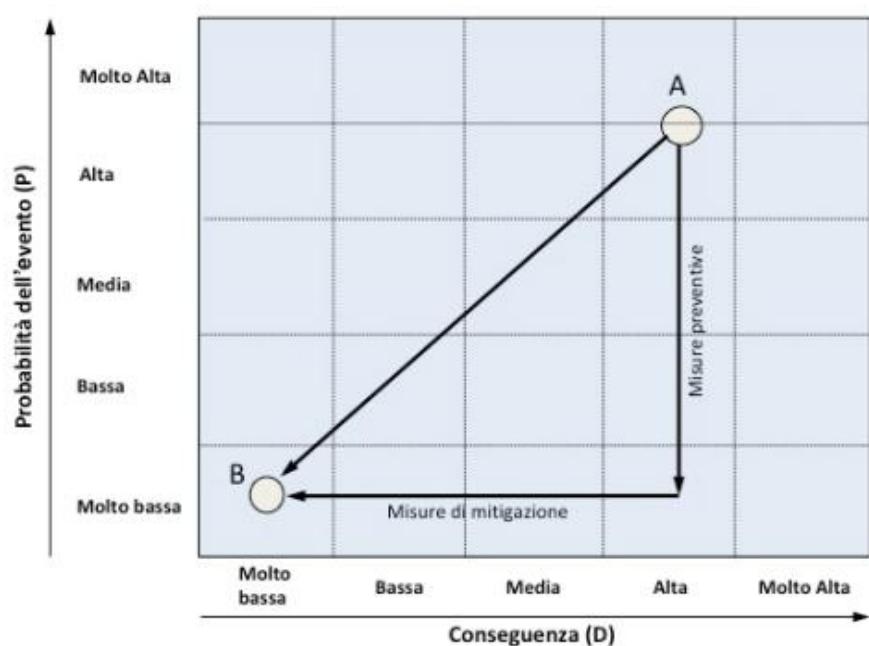


Figura 14.1 – Misure preventive e di mitigazione

Durante la selezione delle Misure è importante valutare il costo di acquisto delle risorse necessarie, l'implementazione, la gestione, il monitoraggio e la manutenzione. È importante non dimenticare la valutazione del ritorno degli investimenti. Occorre, anche, tenere in considerazione le competenze specialistiche che possono essere necessarie per definire e implementare nuove misure o modificare quelle esistenti.

Esistono molti vincoli che possono influenzare la scelta delle misure. Essi possono essere del tipo tecnico, come anche i requisiti di prestazioni, di gestione (requisiti di supporto operativo) e problemi di compatibilità; essi possono ostacolare l'uso di alcune misure o potrebbero indurre a errori umani annullando così la misura, dando, in questo caso, un falso senso di sicurezza o addirittura aumentare il rischio oltre il non avere il controllo (ad esempio richiesta di una password complessa senza un'adeguata formazione che porta agli utenti a scrivere le password in foglietti lasciandoli in evidenza). Inoltre, potrebbe essere il caso che un controllo potrebbe influire sulle prestazioni. I responsabili dovrebbero cercare di individuare una soluzione che soddisfi i requisiti di prestazioni pur garantendo la soddisfazione degli obiettivi. Il risultato di questa fase è un elenco di possibili misure, con i loro costi, benefici e la priorità d'implementazione.

Per quanto che è stato detto, quando si scelgono, dunque, le Misure e, durante la loro implementazione, si dovrebbero prendere in considerazione diversi vincoli, ad esempio: temporali, finanziari, tecnici, operativi, culturali, etici, ambientali, legali, vincoli relativi al personale e vincoli di integrazione, ma anche le misure esistenti.

La decisione sull'accettazione dei rischi senza ulteriori azioni e rinunciando a qualsiasi intervento, dovrebbe essere presa qualora i rischi risultano tollerabili, assumendo in questo caso l'onere delle conseguenze del verificarsi dell'evento. Tale scelta dovrebbe essere coerente con la politica del risk management, giustificabile secondo i casi, ed è, generalmente, limitata ai rischi con bassa probabilità e magnitudo.

A volte tale scelta scaturisce dalla non conoscenza o sottovalutazione dei rischi presenti, dalla inconsapevolezza del management e da una carenza metodologica dell'analisi dei rischi.

Quando i rischi sono considerati troppo alti, o i costi di attuazione delle Misure per il trattamento dei rischi superano i benefici, si potrebbe decidere di evitare i rischi del tutto, cancellando le relative attività sulle quali incombono tali rischi o apportando modifiche alle condizioni alle quali l'attività è gestita (per esempio, i rischi causati da minacce del tipo fisico ambientali, si potrebbe decidere di spostare le relative attività in una località diversa, nella quale tali minacce non esistono, o se esistono la loro probabilità di manifestarsi potrebbe essere minore e facilmente controllabile o inesistente).

La condivisione dei rischi implica una decisione di condividere (trasferire) determinati rischi con soggetti esterni. Ciò potrebbe essere ottenuto da assicurazioni convenzionali, da accordi contrattuali, altri accordi con società in joint venture in cui le esposizioni e le passività sono condivise, così come il guadagno.

È importante riconoscere i limiti di trasferimento del rischio. La condivisione dei rischi può introdurre anche nuovi rischi o modificare rischi esistenti già identificati e gestiti. Pertanto, un ulteriore risk assessment e trattamento potrebbe essere necessario.

La condivisione può essere fatta anche da assicurazioni che supporteranno le conseguenze, o con il subappalto a un partner il cui ruolo sarà il monitoraggio della situazione e l'intraprendere azioni immediate per fermare un attacco prima che subisca un danno.

Pertanto è importante prendere in considerazione il fatto che è possibile condividere la responsabilità di gestire dei rischi, ma non è normalmente possibile condividere la responsabilità di un impatto.

In pratica, il trasferimento dei rischi è tipicamente usato in combinazione con una o più opzioni di risposta al rischio.

La scelta della opzione o delle opzioni decise permette di procedere con la pianificazione delle Misure per il trattamento. Nel caso in cui l'opzione decisa è quella di eliminare o mitigare i rischi, allora si procede con l'elenco delle Misure da implementare. Quando la situazione porta a scegliere altre opzioni, allora si decide opportunamente come proseguire.

Le Misure si possono scegliere da diverse fonti, in funzione del contesto e in funzione delle vulnerabilità e delle minacce da eliminare.

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.

Poiché la tecnologia evolve, le minacce cambiano come anche le vulnerabilità è opportuno pensare che l'Annex A non sia esaustivo e si può avere la necessità di cercare ancora altri controlli aggiuntivi.

Nel caso in cui il contesto non è coperto da nessuna fonte normativa, allora, si crea un gruppo di persone coinvolte nelle attività e si decide insieme le Misure da implementare.

L'uomo per la sua natura è portato a difendere i propri averi e fa in modo che ogni situazione che si trova sotto il suo controllo sia dotata di un minimo di misure di protezione. Nell'ambito dei sistemi e in particolar modo nei sistemi informatici, gli amministratori introducono, sia per esperienza sia per cultura o per istruzione, procedure e meccanismi protettivi. Spesso si tratta di misure superate, inefficaci, non adeguate ai livelli di protezione richiesti, ma comunque possono

gestire un certo quantitativo di rischio, perciò lo possiamo chiamare Rischio Gestito ( $R_G$ ). Il Rischio Gestito dovrebbe essere preso in considerazione per calcolare i Rischi Residui (RR).

In questa fase l'identificazione delle misure in atto viene effettuata al fine di completare il quadro della situazione esistente. Conviene comunque, per ragioni economiche, tenerne conto, nell'ambito del possibile, integrandole nell'elenco complessivo in corso di realizzazione. In ogni caso è necessario valutare la loro effettiva adeguatezza, efficacia e coerenza con le altre Misure che saranno implementate.

I rischi naturalmente, come si è detto in precedenza, non possono essere eliminati del tutto, ma possono essere mitigati attraverso le Misure che si decide di implementare.

Maggiore è la riduzione del livello dei rischi, maggiore è il numero delle misure da applicare, quindi, maggiori sono i costi. Questo significa che per ridurre al massimo i rischi i costi possono crescere notevolmente (fig. 15).

Si può ad ogni modo accettare un livello di rischio, definito come livello dei Rischio Residuo Accettabile ( $RR_{ac}$ ). La quantità, invece, di rischio ridotto con l'introduzione delle Misure porta ad avere un Rischio Residuo (RR). Se il Rischio Residuo è maggiore del Rischio Residuo Accettabile ( $RR_{ac}$ ), allora è necessario applicare ancora altre Misure per ridurre ancora i rischi in modo da soddisfare l'aspettativa del proprietario dei rischi.

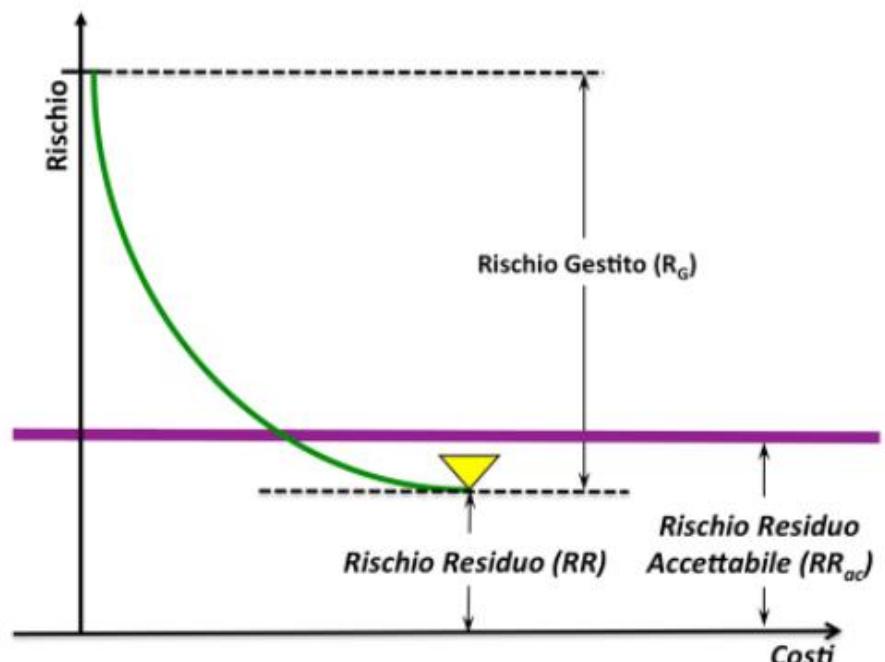


Figura 15 – Andamento dei costi in funzione della riduzione dei rischi

Naturalmente il Rischio Residuo Accettabile ( $RR_{ac}$ ) non è da considerarsi in senso statico. Gli scenari mutano e così anche le minacce, le vulnerabilità, ma anche le esigenze degli stakeholder. Lo dimostra la statistica degli incidenti. L'analisi, la riflessione e i riesami dei risultati costituisce la retroazione necessaria per correggere l'azione tesa a restringere sempre più l'area del caso fortuito.

Il Rischio Residuo Accettabile ( $RR_{ac}$ ) costituisce la soglia minima al di sopra della quale il rischio deve essere ridotto. La valutazione dello scenario dei risultati dell'entità di rischio dovrà stabilire le priorità d'intervento per tutti i rischi che non ricadono nell'area di accettabilità. Naturalmente la priorità alta va assegnata a quei rischi di entità tale da rendere l'azione di riduzione indilazionabile (area rossa della matrice di rischio della fig. 16). I rischi per i quali gli interventi di riduzione, pur urgenti (priorità media), possono essere programmati sul medio o lungo periodo,

sono quelli che sono posizionati nell'area arancione.

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	6	8	10
Medio (3)	3	6	M	12	15
Alto (4)	4	8	12	A	20
Molto Alto (5)	5	10	15	20	25

Figura 16 – Livello di accettabilità dell'entità dei rischi: definizione delle priorità

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 decisori e altri soggetti interessati devono essere consapevoli della natura e dei livelli dei Rischi Residui dopo il trattamento dei rischi. I Rischi Residui devono essere documentati e sottoposti a monitoraggio, riesame e, ove del caso, devono essere ulteriormente tratti.

Il proprietario dei rischi, che in generale coincide con il proprietario degli obiettivi da soddisfare, dovrebbe essere la persona preposta per gestire il Punto Decisionale 2 (fig. 14).

Il Piano di Trattamento dei rischi descrive come i rischi valutati devono essere trattati per soddisfare i criteri di accettazione dei rischi (par. 7.3.5). È importante per il proprietario dei rischi rivedere e approvare le Misure proposte per il trattamento dei rischi e i conseguenti Rischi Residui e registrare qualsiasi condizione associata a tale approvazione.

L'accettazione dei rischi può essere più complessa di un semplice determinare se un Rischio Residuo scende al di sopra o al di sotto di una soglia unica. Questo non significa che si deve inventare dei criteri complessi là dove non servono. Tutto dipende dal contesto e dalla situazione contingente da affrontare.

In alcuni casi il livello di Rischio Residuo può non soddisfare i criteri di accettazione dei rischi, perché i criteri applicati non tengono conto delle prevalenti circostanze. Ad esempio, si potrebbe sostenere che è necessario accettare alcuni rischi, in quanto i vantaggi che si possono avere senza nessun trattamento, sono molto convenienti per causa dell'alto costo d'implementazione delle Misure in relazione ai benefici che si possono ottenere. In ogni caso, questa decisione dovrebbe essere giustificata. Tali circostanze potrebbero indicare che i Criteri di accettazione dei rischi sono insufficienti e devono essere rivisti, se è possibile. Tuttavia, non è sempre possibile rivedere i criteri di accettazione dei rischi in modo tempestivo. In questi casi, il proprietario dei rischi può accettare i rischi che non soddisfano i criteri di accettazione normali. Se comunque la strada da intraprendere è questa, il proprietario dei rischi dovrebbe esplicitamente commentare la

situazione e giustificare, come è stato detto, la decisione intrapresa di ignorare i normali criteri di accettazione dei rischi.

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.

I risultati dovrebbero essere formalizzati in un documento. Nel caso in cui alcuni elementi non vengono approvati, questo risultato dovrebbe essere giustificato e la decisione deve essere documentata.

A completamento del Punto Decisionale 2 si procede con l'implementazione delle Misure stabiliti nel Piano di Trattamento dei Rischi allo scopo di raggiungere gli obiettivi stabiliti.

Si potrebbe definire, nel caso in cui è praticabile, le modalità di misurazione dell'efficacia delle Misure e specificare come queste misure devono essere utilizzate per la valutazione dell'efficacia allo scopo di produrre risultati comparabili e riproducibili.

Nel caso in cui l'implementazione e la gestione delle Misure richiedono competenze specifiche è necessario fornire l'addestramento e la formazione necessaria. L'addestramento e la formazione dovrebbe essere indirizzata soprattutto sulla crescita della consapevolezza in merito alla gestione dei rischi.

Il processo di risk management dovrebbe essere monitorato, riesaminato e migliorato con continuità secondo le esigenze.

Il monitoraggio e il riesame continuo è necessario al fine di garantire che il contesto, il risultato del risk assessment, il trattamento dei rischi e i piani di trattamento dei rischi rimangano pertinenti e adeguati alle circostanze, in quanto i rischi non sono statici. Le minacce, le vulnerabilità o le conseguenze possono cambiare bruscamente senza avere alcuna indicazione. I fattori che influenzano le loro probabilità e le conseguenze potrebbero cambiare, come potrebbero cambiare i

fattori che influenzano l'idoneità o il costo delle varie opzioni di trattamento. Importanti cambiamenti che interessano la situazione dovrebbero essere motivo per una revisione più specifica. Pertanto è necessario eseguire il monitoraggio costantemente per rilevare questi cambiamenti. Il monitoraggio potrebbe essere supportato anche da altri servizi esterni che possono fornire informazioni riguardo le nuove minacce o 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 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.

Inoltre, l'organizzazione dovrebbe regolarmente riesaminare che i criteri utilizzati per la misurazione dei rischio e dei suoi elementi siano ancora validi e coerenti con gli obiettivi di business, le strategie e la politica, e i cambiamenti al contesto di business devono essere presi in considerazione in modo adeguato durante il processo di risk management.

Le attività di monitoraggio e di riesame dovrebbero affrontare (ma non limitarsi a) 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 si dovrebbe garantire che le risorse per il risk management e il trattamento dei rischi siano sempre a disposizione.

I risultati del monitoraggio e del riesame dovrebbero essere registrati e dovrebbero essere utilizzati come elementi in ingresso all'attività di riesame del framework del risk management (par. 6.5).

Le attività del risk management dovrebbero essere tracciabili attraverso le registrazioni e costituiscono le fondamenta per l'efficacia, l'efficienza e per il miglioramento continuo del processo di risk management e del framework.

Le registrazioni possono essere in qualsiasi formato (per esempio, cartaceo, elettronico) e potrebbero essere su qualsiasi supporto: cartaceo, elettronico, fotografico, magnetico, ottico, disegni, diagrammi, diagrammi di flusso, grafici, ecc.

Le registrazioni devono essere controllate e conservate dal proprietario degli obiettivi.

Le decisioni riguardanti la creazione delle registrazioni dovrebbero tenere conto:

- le esigenze per l'apprendimento continuo;
- i benefici del riutilizzo delle informazioni a fini di gestione;
- i costi e gli sforzi spesi nella creazione e nel mantenimento delle registrazioni;
- i requisiti legali, normativi e operativi;

- il metodo di accesso, la facilità di recupero e i supporti di memorizzazione;
- il periodo di conservazione; e
- 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.

## 8. CASO DI STUDIO 1: IL TESORETTO

Il presente Caso di Studio è stato sviluppato per l'applicazione del processo di risk management è un caso di studio didattico reso appositamente semplice per rendere comprensibili i concetti allo scopo di apprendere la metodologia. Nella realtà le situazioni sono notevolmente più complesse. Pertanto una volta seguito e appreso il processo con l'esempio che segue, diventa più facile applicare la metodologia nelle situazioni reali.

I confini entro i quali dobbiamo applicare il processo del risk management si estendono ai confini dell'appartamento.

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.

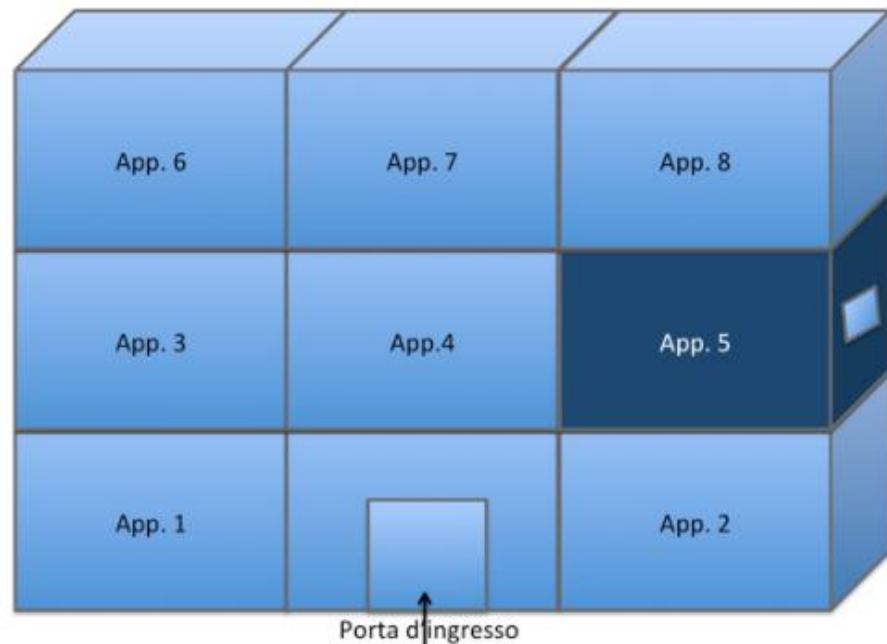


Figura 17 – Configurazione della palazzina

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).

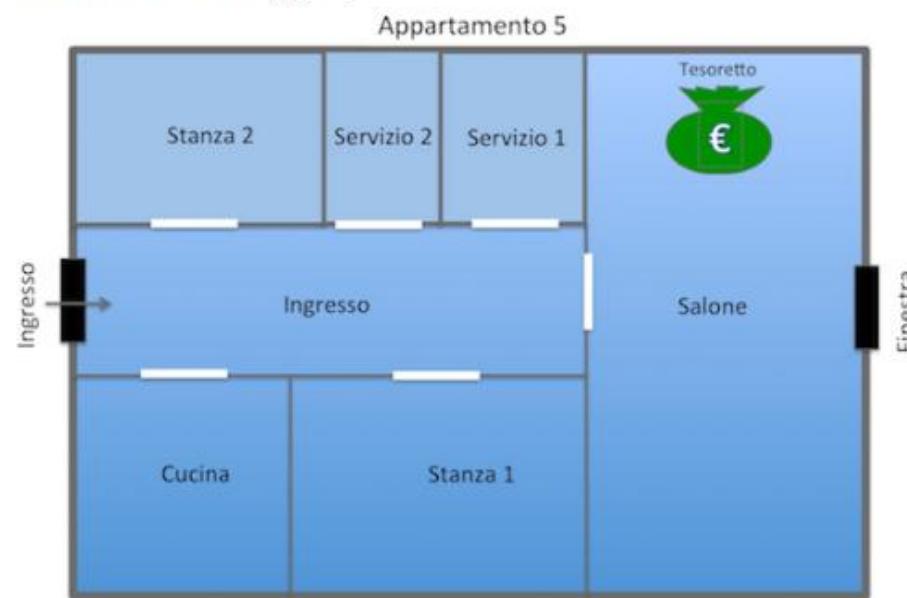


Figura 18 – Configurazione dell'appartamento

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.



Figura 19 – Identificazione delle Minacce e delle Vulnerabilità

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 incomberre 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 hanno 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.

La Vulnerabilità  $V_3$  è la finestra del salone che si affaccia verso l'esterno.

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 sottrarre un importo pari a  $D_3 = 30.000,00 \text{ €}$ . Questa è una delle ipotesi, in quanto 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  $D_2 = 40.000,00 \text{ €}$ . 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:

- $D_3 = € 30.000,00$ , individuato, nella scala delle Conseguenze, come Medio ( $M=3$ );
- $D_4 = € 40.000,00$ , 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):

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

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 Bassa (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

Figura 20 – Valutazione dei Rischi Parziali ( $R_i$ )

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

Figura 21 – Rischi Parziali ( $R_i$ ) e priorità d'intervento

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

$$R(Aggr) = \frac{1}{n} \sum_{i=1}^n R_i \\ = 43/3 = 14,33 \approx 14$$

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 lasciarlo 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 soluzione 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 ( $R_{\text{Agg}}$ ) è del livello Medio. Questa situazione non è accettabile, perché il Rischio Residuo Accettabile ( $RR_{\text{ac}}$ ) 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	X		
$C_2$ - Inserire il tesoretto in una cassaforte, posizionandola nel salone e gestire la chiave in modo sicuro.	X	X	X
$C_3$ - Chiudere la porta del salone a chiave e gestire la chiave.	X		
$C_4$ - Sensibilizzare il figlio per aumentare la consapevolezza sul comportamento etico.	X		
$C_5$ - Installare la porta blindata all'ingresso dell'appartamento. (esistente)			X
$C_6$ - Inserire le inferriate alla finestra.			X

Figura 22 – Elenco delle Contromisure da applicare

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 ( $R_{GjCj}$ ).

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 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:  $RR_1 = R_1 \cdot R_{G1} = 15 \cdot 14 = 1$ .

#### 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:  $RR_2 = R_2 \cdot R_{G2} = 16 \cdot 15 = 1$ .
- 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:  $RR_3 = R_3 \cdot R_{G3} = 12 \cdot 11 = 1$ .

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

Il Piano di Trattamento dei Rischi (fig. 23) nel nostro caso è molto semplice ed è composto dalla seguente tabella:

Contromisura	Priorità	Implementazione		Risorse	Incaricato	Stato
		Data inizio	Data fine			
$C_1$ - Cercare al più presto un lavoro per il figlio	Alta	Gennaio 20XX	Feb. 20XX	• Agenzie interinali • Società ricerca e selezione personale	Proprietario	Da implementare
$C_2$ - Inserire il termometro in una cassaforte, posizionandola nel salone e gestire la chiave in modo sicuro.	Alta	Gennaio 20XX	Feb. 20XX	Acquistare e installare la cassaforte	Proprietario	Da implementare
$C_3$ - Chiudere la porta del salone a chiavi e gestire la chiave.	Alta	Gennaio 20XX	Feb. 20XX	Acquistare e installare serratura e tenere chiuso a chiavi	Proprietario	Da implementare
$C_4$ - Sensibilizzare il figlio per aumentare la consapevolezza sul comportamento elico.	Alta	Gennaio 20XX	Feb. 20XX	---	Proprietario	Da implementare
$C_5$ - Installare la porta blindata all'ingresso dell'appartamento. (esistente)	Alta	N.A.	N.A.	N.A.	N.A.	Esistente
$C_6$ - Inserire le infierite alla finestra.	Media	Gennaio 20XX	Feb. 20XX	Fabbro e installatore	Proprietario	Da implementare

Figura 23 – Piano Trattamento dei Rischi

Dopo aver fatto una valutazione, il proprietario dei rischi ha deciso di approvare il Piano di Trattamento dei Rischi e di approvare i Rischio 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.

## 9. 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. Sfortunatamente per lui, questa mattina il tempo è brutto e piovigginia. 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 indispensabile, 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 diverse linee ferroviarie. A volte capita di aspettare anche 20 minuti davanti alle sbarre prima che esse si alzino per consentire 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 livello 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 attraversare il passaggio a livello per arrivare:

- in ufficio all'ora pianificata per partecipare alla riunione, e naturalmente,

- senza essere investito.

La valutazione per decidere sull'azione da seguire, dovrebbe 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 valutata secondo la seguente scala: 1-Molto Basso, 2-Basso, 3-Medio, 4-Alto, 5- Molto Alto. c)
- **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 valore del Rischio più basso, naturalmente, dovrebbe avere la priorità più alta e dovrebbe essere la soluzione preferibile. 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 potrebbe migliorare la situazione: prendere il ponte sopraelevato 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 costituiscono 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 vulnerabilità) 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 ragionando 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 percorso. 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 arrivesse 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 essere investito è Molto Alta ( $P=5$ ), in quanto non è possibile 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 salute. Perciò, il rischio è pari a  $R=20$ .

3. Decidere di cambiare completamente strada allungando 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 arrivare 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 preferibile, 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 percorso 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 mettersi 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 atmosferiche non sono favorevoli, tutte le volte che ci sono appuntamenti 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 pianificata durante le prime ore del mattino.

## **10. bibliografia**

- ISO/IEC Guide 73, Risk management – Vocabulary.
- ISO 31000: 2018, Risk management – Guidelines.
- ISO/IEC 31010: 2009, Risk management – Risk assessment techniques.
- ISO/IEC 27001: 2013, Information technology - Security techniques-Information security management systems–Requirements.
- ISO/IEC 27002: 2013, Information technology - Security techniques - Code of practice for information security controls.
- ISO/IEC 27005: 2011, Information technology - Security techniques - Information security risk management.
- Ioannis Tsiouras, *Pensiero basato sul rischio, Risk-based thinking*, ebook, Youcanprint Self-publishing, 2016.
- Ioannis Tsiouras, *La sicurezza dell'informazione. Dal sistema di gestione alla sicurezza dei sistemi informatici*, FrancoAngeli, Milano, 2004.
- INAIL, Commentario alla sicurezza del lavoro - i decreti legislativi 626/94 e 242/96, Il Sole 24 Ore Pirola S.p.A., Milano, 1996.

## **11. Appendice A – strumenti e tecniche per il risk management**

Gli strumenti e le tecniche sono indispensabili nella gestione del processo del risk management e in modo particolare nella gestione efficace ed efficiente dei rischi. Generalmente sono usati nella raccolta delle informazioni, nell'analisi del contesto per identificare le minacce e le vulnerabilità, nel risk assessment (causa-effetto, analisi degli impatti, la stima delle probabilità e delle frequenze, la stima dei livelli dei rischi, nella valutazione dei rischi, ecc.), nella comunicazione interna e con gli stakeholder e in altre situazioni.

Ci sono molti strumenti e tecniche; ciascuno è adatto per particolari compiti e situazioni. Alcune volte la scelta degli strumenti e delle tecniche può risultare facile, mentre altre volte sono più difficili; la facilità di utilizzo dipende dalle caratteristiche della persona che deve usare gli strumenti e le tecniche (per esempio: la competenza e l'esperienza con lo strumento, la capacità di comprendere i vantaggi di utilizzare lo strumento).

La scelta di uno strumento o di una tecnica dipende, inoltre, dalle caratteristiche del lavoro da svolgere, dalle caratteristiche dello strumento/tecnica stessa, dalla disponibilità delle informazioni, dalla facilità di utilizzo, dalla complessità delle istanze, dal costo, ecc.

Gli strumenti e le tecniche, in funzione del lavoro qualitativo o quantitativo che permettono di svolgere, possono essere classificati in strumenti/tecniche per dati non numerici e strumenti/tecniche per dati numerici.

Le decisioni nelle attività di risk management possono essere basate su dati non numerici. Questi dati giocano un ruolo importante nell'identificazione, nell'analisi e nella valutazione dei rischi.

Appropriati strumenti sono utilizzati per elaborare correttamente questi dati e trasformarli in informazioni utili su cui basare le decisioni da prendere.

Spesso le decisioni nelle attività di risk management sono basate su dati numerici. Le decisioni circa differenze, andamenti e cambiamenti nei dati numerici sono basate su appropriate interpretazioni statistiche.

Gli strumenti e le tecniche, inoltre, possono essere classificati anche in funzione del tipo di utilizzo. Si possono distinguere perciò le seguenti categorie: di consultazione, di supporto, per le analisi degli scenari, per le analisi funzionali, per i controlli delle valutazioni, per le statistiche.

La Tabelle A.1 (ispirata dalla norma ISO 31010) presenta l'applicabilità degli strumenti e delle tecniche per il risk assessment.

**Tabella A.1 – Applicabilità degli strumenti e delle tecniche nel risk management**  
*(ispirato alla norma ISO 31010: 2009)*

Strumenti e tecniche	Processo di Risk Assessment				
	Identificazione dei rischi	Analisi dei rischi			Valutazione dei rischi
		Conseguenze	Probabilità	Livelli dei rischi	
<b>Metodi di consultazione</b>					
Check-lists	✓				
Primary hazard analysis	✓				
<b>Metodi di collaborazione</b>					
Brainstorming	✓				
Structured or semi-structured interviews	✓				
Delphi	✓				
Structure « What if? » (SWIFT)	✓	✓	✓	✓	✓
Human reliability analysis	✓	✓	✓	✓	✓
<b>Analisi degli scenari</b>					
Root cause analysis		✓	✓	✓	✓
Scenario analysis	✓	✓	✓	✓	✓
Business impact analysis	✓	✓	✓	✓	✓
Fault tree analysis	✓		✓	✓	✓
Event tree analysis	✓	✓	✓	✓	✓
Cause and consequence analysis	✓	✓	✓	✓	✓
Decision tree		✓	✓	✓	✓
Environmental risk assessment	✓	✓	✓	✓	✓
Cause-and-effect analysis	✓	✓			

Strumenti e tecniche	Processo di Risk Assessment				
	Identificazione dei rischi	Analisi dei rischi			Valutazione dei rischi
		Conseguenze	Probabilità	Livelli dei rischi	
<b>Analisi Funzionali</b>					
Failure mode effect analysis (FMEA)	✓	✓	✓	✓	✓
Multi-criteria decision analysis (MCDA)	✓	✓	✓	✓	✓
Reliability centred maintenance	✓	✓	✓	✓	✓
Sneak circuit analysis	✓				
Cost/benefit analysis	✓	✓	✓	✓	✓
Hazard and operability studies (HAZOP)	✓	✓	✓	✓	✓
Hazard Analysis and Critical Control Points (HACCP)	✓	✓			✓
<b>Controllo delle valutazioni</b>					
Layer protection analysis (LOPA)	✓	✓	✓	✓	
Bow tie analysis		✓	✓	✓	✓
<b>Metodi statistici</b>					
Markov analysis	✓	✓			
Monte Carlo simulation					✓
Bayesian statistics and Bayes Nets		✓			
Risk indices	✓	✓	✓	✓	✓
<b>Metodi grafici</b>					
FN curves	✓	✓	✓	✓	✓
<b>Metod/a matrice</b>					
Consequence/probability matrix	✓	✓	✓	✓	✓

## **Indice**

[Copertina](#)

[Titolo e diritti](#)

[L'autore](#)

[Dedica](#)

[Prefazione](#)

[Indice completo](#)

[1. Introduzione](#)

[2. Risk governance](#)

[3. Il rischio](#)

[4. Il risk management nel processo decisionale](#)

[5. I principi che guidano il risk management](#)

[6. Il framework per il risk management](#)

[7. Il processo del risk management](#)

[8. Caso di Studio 1: Il tesoretto](#)

[9. Caso di Studio 2: Attraversamento del passaggio a livello](#)

[10. Bibliografia](#)

[11. Appendice A - Strumenti e tecniche per il risk management](#)

[Tab. A.1 - Applicabilità degli strumenti e delle tecniche nel risk management](#)