SAPIENZA
UNIVERSITÀ DI ROMA

Il processo di Risk Identification con l'Intelligenza Artificiale: il caso Italferr

Facoltà di Ingegneria dell'Informazione, Informatica e Statistica
Dipartimento di Ingegneria Informatica, Automatica e Gestionale
Corso di laurea Magistrale in Ingegneria Gestionale

Michele Cardone
Matricola 1755212

Relatore
Fabio Nonino

Correlatore
Guido Mastrobuono

A.A. 2022-2023

Indice

Abstract

Questo elaborato affronta i temi del rischio, del Project Risk Management e dell'identificazione dei rischi per raggiungere un obiettivo ben specifico.

Infatti, l'obiettivo di questo elaborato è di dimostrare come il processo di Identificazione Automatizzata di Italferr sia adatto ad essere il riferimento per creare uno strumento di Identificazione servendosi dell'Intelligenza Artificiale. Per raggiungere l'obiettivo dell'elaborato, coincidente con l'obiettivo di implementazione dell'IA nei processi di Project Risk Management di Italferr sono stati creati degli indici di valutazione di qualità ed efficienza dell'identificazione automatizza di Italferr. Questi hanno lo scopo ultimo di essere applicati alle identificazioni dell'Intelligenza Artificiale per valutarne la qualità. Sono stati fatti dei test sulla capacità dell'Intelligenza Artificiale di comprendere relazioni e associazioni tra rischi e vulnerabilità (concetto centrale dello studio) e sulla base dei risultati si dimostra come l'obiettivo di implementazione dell'IA nei processi di identificazione sia effettivamente raggiungibile. Questo elaborato vuole essere un passo in avanti verso l'espansione della gestione del rischio di Italferr in nuovi settori, ad oggi, ancora ignoti.

Indice delle figure e delle tabelle

Introduzione

L'elaborato nasce con un duplice obiettivo. Il primo riguarda l'espansione della cultura del rischio in ambito accademico e il secondo di valutare l'efficienza di un processo di identificazione dei rischi tramite analisi svolte direttamente sul processo e analisi svolte grazie all'utilizzo dell'Intelligenza Artificiale. Lo studio è stato possibile grazie alla collaborazione con Italferr, azienda di ingegneria italiana che si occupa principalmente di progetti infrastrutturali e ferroviari. Nel primo capitolo viene esposto il concetto di rischio dapprima con un approccio storico, passando per l'analisi del fondamentale concetto di Risk Appetite terminando con un leggero focus sui rischi in ambito infrastrutturale. Il secondo capitolo serve a contestualizzare il Risk Management all'interno del Project Management, analizzando come il Project Risk Management (PRM) sia presente all'interno di tutte le fasi del ciclo di vita di un progetto e come il PRM sia un processo ciclico e iterativo a sé stante utile all'accertamento del raggiungimento degli obiettivi di progetto e della creazione di valore. Il discorso entra sempre di più nel dettaglio nel terzo capitolo, all'interno del quale ci si sofferma sul processo di Identificazione dei Rischi. Viene descritto il processo presentando una serie di tecniche presenti in letteratura e utilizzate oggigiorno in moltissime imprese produttrici, sia di beni che di servizi. Il capitolo si conclude con la dettagliata spiegazione del processo di Identificazione in Italferr. Una parte del processo, è l'identificazione automatizzata. Questa snellisce e velocizza fortemente tutto il processo più esteso di PRM. Negli anni di utilizzo, però, non era mai stata valutata da un punto di vista esterno. Nell'ultimo capitolo, partendo dal concetto di vulnerabilità, centrale per l'identificazione

automatizzata, vengono presentati degli indici per la valutazione dell'efficienza e i test atti a comprendere l'implementabilità dell'Intelligenza Artificiale nel processo con risultati e commenti.

1 Il Rischio

I rischi sono intorno a noi e appaiono in diverse forme. Ci interfacciamo quotidianamente con i rischi più disparati: nelle nuove tecnologie, nella medicina, nelle relazioni personali, nelle scelte finanziarie ecc...

Oltre che nella forma, questi variano anche nella conseguenza: abbiamo rischi il cui effetto è immediato, altri in cui è sul lungo periodo; rischi materiali o immateriali. Ma se la loro natura è così variegata e mutevole, è possibile definire precisamente il loro significato? Partiamo dal concetto più semplice: il rischio è correlato a ciò che ha valore (Fischhoff B. e Kadvany J., 2011).

L'obiettivo di ogni azienda è quello di creare valore condiviso e cioè valore economico e sociale per l'organizzazione stessa, per tutti gli stakeholders e l'ambiente in cui opera, avendo una visione tridimensionale degli obiettivi nel tempo e nello spazio (Porter M.E. e Kramer M.R., 2011). Con l'aumentare della complessità del contesto sociale e dell'area di influenza delle aziende, si intensifica la difficoltà nella definizione e nel raggiungimento degli obiettivi prefissati, e ciò è conseguenza della presenza naturale di fonti di incertezza.

Come espresso nell' articolo "Prospect Theory: An Analysis of Decision under Risk" (Kahneman D. e Tversky A., 1979), il rischio è presente nella quotidianità delle persone, ma il significato reale della parola è molto più complesso e profondo di quanto si percepisca. Il concetto di rischio è collegato inevitabilmente a una tendenza verso un obiettivo significativo. Infatti, in assenza di quest'ultimo verrebbe a mancare il significato vero e proprio del rischio. Questo ragionamento assume un valore molto forte in

ambito aziendale, ma può essere interpretato anche nella vita quotidiana: essere investiti da un'automobile è un rischio solo se ci interessa della nostra salute o del nostro stato attuale, e quindi l'obiettivo è quello della nostra integrità. Nel momento in cui venisse a mancare questo obiettivo, non esisterebbe più il concetto del "rischio di essere investito" ma avremmo, al massimo, "l'evento essere investito". Questo esempio seppur banale ed estremizzato può aiutare a comprendere il punto di partenza dell'analisi.

La significatività dell'obiettivo è fondamentale, ma bisogna ricordarsi sempre della soggettività presente nella valutazione della stessa e, quindi, nella valutazione del rischio. Il rischio legato alla sconfitta di una squadra di calcio può essere nullo per alcuni, ma può assumere un valore per un individuo che avesse scommesso dei soldi sulla vittoria o semplicemente molto tifoso. In modo analogo anche l'impatto del rischio può assumere valori diversi indipendentemente dalla quantificazione effettiva. Ad esempio, la perdita di 10 euro può avere pesi differenti per individui con diverse capacità economiche. La presenza di soggettività nelle analisi e nelle valutazioni non preclude la possibilità di arrivare a conclusioni oggettive e fondate, ma è una condizione che bisogna sempre tenere in considerazione. Vedremo sulla base delle varie definizioni presenti in letteratura che esistono molti concetti satelliti del rischio:

- **Contesto:** ambiente in cui si origina il rischio; i rischi influenzano e sono influenzati dal contesto. È definito da caratteristiche temporali, spaziali e materiali.
- **Vulnerabilità**: caratteristica di un componente, o di un sistema nella sua interezza, per cui risulta suscettibile a particolari situazioni. Le Nazioni Unite/International Strategy for Disaster Reduction (UN/ISDR) (Living with Risk. A Global Review of

Disaster Reduction Initiatives, 2004), ad esempio, definiscono le vulnerabilità come le ''condizioni determinate da fattori o processi fisici, sociali, economici e ambientali che aumentano la suscettibilità di una comunità all'impatto dei pericoli''.

- **Fonte di rischio:** causa, sorgente del rischio. In altre parole, la fonte di rischio è ciò che potrebbe causare un evento negativo, mentre il rischio rappresenta la possibilità che l'evento si verifichi.
- **Evento**: occorrenza o modifiche di un insieme di circostanze. (International Standards Organization (ISO), 2018)
- **Incertezza**: mancanza di sicurezza riguardo a un dato elemento, può essere causata da una mancanza di informazioni, dalla presenza di informazioni sbagliate o capite male, o dall'impredicibilità.
- **Impatto**: è la quantificazione della deviazione dall'obiettivo a causa dell'avverarsi del rischio.
- **Probabilità:** rappresenta la probabilità di accadimento di un determinato rischio.

La differenza tra questi concetti non è assolutamente banale. Poiché il rischio è generalmente definito come il prodotto della probabilità dell'accadimento di un evento e delle sue conseguenze, il rischio può essere visto come una funzione dell'evento di pericolo e della vulnerabilità degli elementi esposti. La vulnerabilità è spesso vista come una caratteristica intrinseca di un sistema o di un elemento. La maggior parte degli analisti riconosce che la vulnerabilità è condizionata da un pericolo, ad esempio rispetto alla sua frequenza e gravità, o che è

inutile discutere la vulnerabilità indipendentemente dal suo contesto di pericolo (Birkmann J., 2007).

1.1 Una prima definizione

Il rischio è la deviazione positiva o negativa dagli obiettivi per effetto dell'incertezza. Per quanto la parola rischio possa trarre in inganno, questa indica anche una deviazione positiva nel raggiungimento dell'obiettivo, quindi un'opportunità. Inizialmente questo termine veniva considerato come sinonimo di minaccia, ma negli anni si è capito che la minaccia è solamente il lato più facilmente visibile della medaglia; l'altro lato, quello spesso ignorato, nasconde la possibilità di opportunità (Hillson D., 2002). Il rischio è generato da fonti di rischio, cioè elementi endogeni o esogeni al sistema che possono provocarlo, da soli o combinandosi tra di loro. Il rischio è, inoltre, legato ad eventi, cioè occorrenze o modifiche di circostanze. Affinché ci sia rischio, devono essere presenti soggetti esposti ad esso. Gli eventi possono essere previsti e non accaduti, oppure essere imprevisti ed accaduti. Il verificarsi del rischio genera sempre delle conseguenze sugli obiettivi.

Il più recente degli standard che include sia l'opportunità che la minaccia nella sua definizione di "rischio" è l'ultima edizione della Guida al Project Management Body of Knowledge (PMI, 2017), in cui si afferma che "Il rischio di progetto è un evento o condizione incerta che, se si verifica, ha un effetto positivo o negativo su un obiettivo di progetto. Il rischio di progetto include sia le minacce agli obiettivi del progetto sia le opportunità per migliorare tali obiettivi". La decisione di racchiudere sia le opportunità che le minacce all'interno di un'unica definizione di rischio è una chiara dichiarazione di intenti, riconoscendo che entrambe hanno influenze

ugualmente importanti sul successo del progetto ed entrambe devono essere gestite in modo proattivo. Si sostiene che le opportunità e le minacce non siano di natura qualitativamente diversa, poiché entrambe implicano incertezza, la quale ha il potenziale di influenzare gli obiettivi del progetto. Di conseguenza, entrambi possono essere gestiti dallo stesso processo, anche se potrebbero essere necessarie alcune modifiche all'approccio standard di gestione del rischio per gestire efficacemente le opportunità (Hillson D., 2002).

Nella norma ISO (2018) si evidenziano altri concetti importanti come quello di incertezza, di probabilità e di conseguenze (entità del danno). L'incertezza è la mancanza, totale o parziale, di informazioni riguardo a situazioni, stati di un sistema o eventi futuri, ed è alla base del concetto di rischio. Spesso, erroneamente, i termini 'pericolo', 'incertezza' e 'rischio' vengono considerati come sinonimi, ma la distinzione tra questi termini, seppur sottile, è indispensabile. Il pericolo rappresenta la proprietà intrinseca di un fattore di essere una potenziale fonte di danno. L'incertezza è definita dall'economista Knight (Knight F. H., 1921) come una situazione con probabilità sconosciuta, infine il rischio è definito dalle differenti probabilità di raggiungere stati o risultati diversi e può essere considerato come un'incertezza misurabile.

In letteratura esistono diverse definizioni di rischio. L' IRM (Institute of Risk Management (IRM), 2003) lo definisce come la combinazione della probabilità del verificarsi del danno e delle conseguenze che questo può avere, sia positive che negative. Si è visto che Il PMI (2017) lo definisce come un insieme di condizioni o eventi incerti che, se accadono, hanno conseguenze negative o positive su uno o più obiettivi di progetto, invece, secondo la norma ISO 31000 (International Standards Organization (ISO),

2018)il rischio è l'effetto dell'incertezza sugli obiettivi e pone un'attenzione maggiore sulle lacune informative piuttosto che sugli eventi. Ciò che accomuna queste e altre definizioni presenti è la rappresentazione della natura del rischio attraverso la combinazione di differenti eventi possibili ma non noti, non capiti oppure incerti, che causano degli scostamenti da obiettivi prefissati e pianificati sfruttando delle vulnerabilità dell'azienda.

L'entità del rischio, come già visto, è legata alla deviazione generata dall'obiettivo. La probabilità è una misura numerica della possibilità di accadimento di un evento che a sua volta genera un rischio. La probabilità varia tra 0, cioè l'evento con probabilità nulla, e 1 associabile ad un evento con probabilità di accadimento certa. Il rischio non è un'entità a sé stante ma è originata in un determinato contesto, sfruttando specifiche vulnerabilità. Nonostante il rischio sembri un concetto molto astratto, è indispensabile che a esso siano associati valori quantificabili. Non avrebbe senso costruire un processo di gestione, e provare a controllare, qualcosa che non è misurabile. La concezione del rischio può essere interpretata in diversi modi, a seconda del contesto in cui viene utilizzata.

Una possibile concezione del rischio è quella di energia potenziale del contesto, ovvero la capacità di un ambiente di generare eventi sfavorevoli. Questa concezione mette in evidenza il fatto che i rischi non sono solo il risultato di singoli eventi, ma sono anche influenzati dal contesto in cui si verificano. Ad esempio, nella gestione del rischio ambientale, l'energia potenziale del contesto può essere vista come la capacità di un ambiente di generare eventi che possono causare danni all'ecosistema. In questo caso, la gestione del rischio si concentra sulla valutazione e sulla mitigazione delle fonti di energia potenziale, come ad esempio l'inquinamento atmosferico o la contaminazione del suolo.

Un altro esempio di come la concezione del rischio come energia potenziale del contesto possa essere applicata è nella gestione del rischio finanziario. Qui, l'energia potenziale del contesto può essere vista come la capacità dei mercati finanziari di generare eventi che possono causare perdite economiche. In questo caso, la gestione del rischio si concentra sulla valutazione e sulla mitigazione delle fonti come, ad esempio, le fluttuazioni dei tassi di cambio o delle quote azionarie. In sintesi, il concetto di rischio come energia potenziale del contesto offre una nuova prospettiva sulla gestione del rischio, che può aiutare a comprendere meglio i rischi come parte integrante del mondo che ci circonda e a sviluppare strategie di gestione del rischio più efficaci e sostenibili. I rischi sono così elementi latenti nel sistema, per questo motivo non sono facilmente visibili o analizzabili. È indispensabile, perciò, la conoscenza profonda delle caratteristiche e proprietà del contesto per poter indagare al meglio tutti i rischi che da esso possono essere generati.

1.2 Rischio come incertezza

Un concetto importante definito sia nell'ISO che nel PMBoK (PMI, 2017) ed affrontato da molti esperti in materia di rischio è l'incertezza. L'incertezza è la causa principale della realizzazione dei rischi. Per poter parlare di rischio è necessario riuscire a quantificare l'incertezza in relazione all'obiettivo; nel caso in cui una quantificazione numerica non sia possibile è indispensabile, comunque, una descrizione qualitativa che ne definisca il peso. L'incertezza rappresenta l'inquantificabile e ciò che non si può misurare. A Knight (Risk, uncertainty and profit, 1921) si deve la prima definizione economica di rischio e la distinzione tra rischio e incertezza. "Quello che noi viviamo è un mondo di mutamenti ed un mondo di incertezza. Noi viviamo solo perché conosciamo qualcosa del futuro; mentre i problemi della vita o almeno della condotta derivano dal fatto che noi ne conosciamo troppo poco. Questo è altrettanto vero negli affari come nelle altre sfere di attività. L'essenza della situazione sta nell'azione derivante dall'opinione, più o meno fondata e valida, che non vi è né ignoranza assoluta, né completa e perfetta informazione, ma conoscenza parziale". Secondo Knight si può parlare di rischio soltanto quando è possibile calcolare oggettivamente la probabilità dell'evento futuro. In tal caso vi è la possibilità obiettiva di tradurre il rischio in fattore di costo e quindi di assicurarlo. Quando l'evento non è prevedibile, ossia la probabilità che si verifichi non è calcolabile in modo oggettivo, o in maniera analoga l'impatto, è impossibile parlare di rischio. A dimostrazione della fondatezza della distinzione tra rischio e incertezza Knight afferma che "se tutto ciò che fosse incerto fosse anche rischioso (e misurabile) saremmo in una situazione nella quale l'avversione al rischio annullerebbe qualsiasi opportunità di profitto". La definizione di Knight - adottata anche dalla

teoria economica degli anni '30-'50 - limita l'analisi delle scelte in condizioni di incertezza soltanto ai casi in cui l'operatore è in grado stimare una probabilità oggettiva sugli eventi futuri. Il rischio è quindi definito come un'incertezza misurabile.

Il PMBOK (2017) distingue i rischi in due categorie:

- Rischi associati ad eventi
- Rischi non associati ad eventi

Analizzando bene il concetto di evento è possibile ricondurre la natura dei rischi all'incertezza stessa, poiché l'accadimento di un evento di per sé non causa danni, ma è l'incertezza legata all'evento stesso che genera il rischio: se nel momento in cui devo prendere una coincidenza di due treni so già che accadrà un ritardo e so la sua quantificazione, allora posso organizzarmi per prendere i biglietti dei treni con la giusta coincidenza, ma se è presente l'incertezza sull'evento ritardo, o sulla quantificazione dello stesso, allora l'acquisto dei biglietti diventa un rischio. Il rischio è più di un evento incerto, ma è legato a diversi tipi di incertezza:

- Incertezza aleatoria: legata a variabilità intrinseca dei fenomeni;
- Incertezza epistemica: legata a mancanza di conoscenza e che può essere ridotta acquisendo più informazioni;
- Incertezza linguistica;
- Incertezza delle decisioni: legata a giudizi professionali, alle norme della società, ai valori condivisi;
- Incertezza legata ai limiti umani;
- Impredicibilità;
- Mancanza di conoscenza che deriva dalla non comprensione dell'incertezza;

- Incertezza sugli eventi;
- Incertezza nei modelli;

L'incertezza a volte può essere diminuita o addirittura eliminata, ad esempio cercando di acquisire più dati o informazioni. In altri casi non è possibile modificarla, allora sarà ancora più importante cercare di capirla. Sapere di non sapere dà la possibilità di riconoscere il potenziale rischio e quindi di eliminarlo, mitigarlo, accettarlo e così via.Il PMBoK si concentra sulla definizione e sulla gestione del rischio in relazione ai progetti, mentre la norma ISO 31000 definisce un approccio integrato e sistematico al rischio per l'intera organizzazione, ricordando che il framework deve essere adattato alla specificità dell'azienda, del settore in cui opera ma anche al livello operativo in cui viene adottato. In entrambi i casi il concetto del rischio deve far parte della cultura aziendale, definendo così il grado di maturità dell'azienda sul rischio.

1.3 Rischio e soggettività

La differenza tra rischio e incertezza viene in qualche modo affiancata da quell'insieme di teorie che prendono in considerazione non solo le probabilità oggettive, ma anche l'elemento soggettivo. Secondo le teorie delle scelte oggettive gli operatori economici sono in grado di costruire delle stime sul verificarsi o meno di eventi futuri e quindi possono prendere le proprie decisioni/scelte anche in assenza di valutazioni probabilistiche oggettive e in assenza di esperienza (dati storici). La natura soggettiva delle stime non consentirebbe di parlare di rischio, essendo il rischio definito da Knight determinato esclusivamente tramite le probabilità oggettive degli eventi. Le teorie economiche delle scelte soggettive hanno consentito di

studiare situazioni precedentemente considerate al di fuori del campo di studio dell'economia politica e hanno fortemente indebolito la differenza economica tra incertezza e rischio.

Per quanto siamo abituati a considerare la probabilità come un qualcosa di oggettivo, anche essa in realtà è influenzata in parte da soggettività (si pensi solo alla scelta della teoria della probabilità a cui si fa affidamento). Sia se parliamo di entità del rischio sia se parliamo di probabilità risulta molto forte la presenza di valutazioni soggettive intorno al rischio, un richiamo interessante può essere fatto alla Teoria del Prospetto che analizza la valutazione del possibile impatto del danno dipende dal valutatore e dalla percezione soggettiva del danno. Negli anni 70 (Kahneman D. e Tversky A., 1979) si interrogano su come si modificano i processi decisionali in situazioni di rischio avanzando la loro teoria in contrapposizione alla teoria dell'utilità attesa di Bernoulli. Nel caso in cui i soggetti sono in condizioni di rischio, la teoria classica dell'utilità attesa non funziona. Le persone, infatti, non riflettono razionalmente sulle reali probabilità di un evento, ma selezionano le informazioni sulla base di schemi soggettivi differenti. Un risultato affascinante nei loro studi delinea il fatto che di fronte a uno stesso problema, formulato in maniera differente, lo stesso individuo può compiere scelte diverse.

Negli ultimi decenni, come visto precedentemente, l'attenzione per il tema del rischio è aumentata esponenzialmente. Le motivazioni sono spiegate in modo molto approfondito attraverso le analisi sociologiche di Giddens (1990).In questo proposito, anche Slovic (2000) precisa che ciò che è aumentato, rispetto ad altri momenti storici, non è in realtà il numero degli eventi rischiosi, ma la "coscienza del rischio" nelle persone, la quale impone

misure di sicurezza sempre maggiori per tutti. In effetti, oggi le persone sono meno disposte ad accettare rischi che un tempo erano tollerati.

Le persone costruiscono la propria realtà e valutano i rischi secondo le loro percezioni soggettive. Questo tipo di percezione intuitiva del rischio si basa sul modo in cui vengono comunicate le informazioni sulla fonte di un rischio, sui meccanismi psicologici per l'elaborazione dell'incertezza e sull'esperienza precedente del pericolo. Questo processo mentale si traduce in un rischio percepito: una raccolta di nozioni che le persone acquisiscono sulle fonti di rischio relative alle informazioni a loro disposizione e al loro buon senso di base. (Jaeger C., Renn O., Rosa E. e Webler, T., 2002)

La percezione del rischio è influenzata da differenti fattori: geografici, sociologici, politici, psicologici e antropologici. Ciò che si qualifica come rischio è quindi soggetto a cambiamenti sociali dinamici. La ricerca sulla percezione del rischio ha identificato una serie di modelli di percezione utilizzati dalla società per percepire e valutare il rischio. Guardando in particolare ai pericoli tecnologici e naturali, si possono identificare i seguenti modelli di percezione (Renn O. , 2004):

- **Rischio come minaccia mortale**: il valore della probabilità non ha alcun effetto sul valore percepito del rischio, è la natura casuale dell'evento che pone la sensazione di minaccia. Le persone sono più a loro agio con le minacce che possono prevedere e pianificare piuttosto che con le minacce che potrebbero materializzarsi in qualsiasi momento. Le fonti di rischio in questa categoria includono le principali strutture come le centrali nucleari, gli impianti di stoccaggio di gas naturale liquido (GNL), i siti di produzione chimica e altre fonti di potenziale pericolo che

potrebbero avere effetti catastrofici sull'uomo e sull'ambiente in caso di grave incidente;

- **Rischio come destino:** rischi su cui si sa di non avere il controllo. I disastri naturali sono generalmente visti come eventi inevitabili con effetti catastrofici. La relativa rarità dell'evento fornisce un rinforzo psicologico per la negazione del rischio;
- **Il rischio come prova di forza:** le persone corrono dei rischi per mettere alla prova la propria forza e sperimentare il trionfo sulle forze naturali o su altri fattori di rischio;
- **Rischio come gioco d'azzardo**: il rischio come brivido, in cui le proprie capacità di far fronte al rischio sono strumentali per entrare nell'attività. Le aspettative statistiche non forniscono alcuno standard su cui basare un comportamento di gioco razionale;
- **Il rischio come indicatore di preallarme:** in questo modello di percezione del rischio, gli studi scientifici aiutano a individuare tempestivamente il pericolo in agguato e la scoperta di relazioni causali tra attività o eventi e i loro effetti latenti.

La probabilità e la gravità degli effetti avversi non sono gli unici componenti che la maggior parte delle persone utilizza come parametri di riferimento per percepire e valutare i rischi. È piuttosto il contesto in cui tali rischi vengono vissuti che determina il loro destino nella percezione del rischio. Questa dipendenza dalle circostanze di supporto non è casuale, ma segue alcuni principi che possono essere identificati da un'indagine psicologica sistematica. La ricerca ha fornito un lungo elenco di circostanze di supporto o fattori qualitativi.

L'analisi fattoriale di solito riduce questi elenchi a pochi importanti fattori composti. Diversi studi hanno individuato come particolarmente rilevanti i seguenti fattori:

- familiarità con la fonte di rischio;
- accettazione volontaria del rischio;
- capacità di controllare personalmente il grado di rischio;
- se la fonte di rischio è in grado di provocare un disastro (potenziale catastrofico);
- certezza dell'impatto fatale in caso di rischio (terrore);
- impatto indesiderato sulle generazioni future;
- percezione sensoriale del pericolo;
- impressione di un'equa distribuzione di benefici e rischi;
- impressione di reversibilità dell'impatto del rischio;
- congruenza tra benefattori e portatori di rischio;
- fiducia nel controllo del rischio e nella gestione del rischio operati dallo Stato;
- esperienza (collettiva e individuale) con la tecnologia e la natura;
- affidabilità delle fonti informative;
- chiarezza delle informazioni sul rischio.
- L'importanza di questi fattori qualitativi offre una spiegazione plausibile che le fonti di rischio classificate a bassa rischiosità dalla valutazione tecnica siano, in realtà, fonte di maggiore preoccupazione tra il pubblico generale. Le fonti di rischio ritenute controverse, come l'energia nucleare, sono molto spesso gravate da attributi negativi mentre le attività del tempo libero sono associate a quelle più positive.

- Se assumiamo che i meccanismi intuitivi di percezione e valutazione del rischio abbiano caratteristiche praticamente universali che possono essere più o meno rimodellate da influenze socioculturali, è possibile fornire una base fondamentale per la comunicazione di cui ci si può avvalere indipendentemente dalle differenze tra i vari punti di vista.

1.4 Evoluzione del concetto di rischio

Il concetto di rischio come elemento funzionale dell'azienda è relativamente moderno. Eventi storici chiave aiuteranno a capire la sua evoluzione nel tempo. Il tema del rischio è presente da sempre nella quotidianità degli individui. Essendo la gestione del rischio un'estensione della natura umana è ovvio che il suo mutare è un riflesso degli eventi storici, economici, sociali e ambientali. Di seguito si analizza l'evoluzione del concetto di rischio seguendo la suddivisione convenzionale della storia dell'umanità in periodi di tempo, cioè le quattro età storiche:

- Storia antica: dall'invenzione della scrittura (3500 a.C.) alla caduta dell'Impero Romano d'Occidente (476 d.C.).
- Storia medievale: dalla caduta dell'Impero Romano d'Occidente (476 d.C.) alla scoperta dell'America (1492).
- Storia moderna: dalla scoperta dell'America (1492) alla Rivoluzione francese (1789) o alla Rivoluzione industriale (1760).
- Storia contemporanea: dalla Rivoluzione francese (1789) o dalla Rivoluzione industriale (1760) al presente.

La storia contemporanea verrà suddivisa ulteriormente in base ai principali eventi scatenanti che hanno portato sviluppi importanti nello studio e nella concezione del rischio.

1.4.1 Età antica

Covello e Mumpower (1985) hanno ripercorso la storia del rischio tornando indietro a quattromila anni prima dell'anno 0, osservando l'area tra il Tigri e l'Eufrate, in cui erano presenti dei sacerdoti sumeri – la casta degli asipu – cui il popolo si rivolgeva per ottenere indicazioni circa l'opportunità di iniziative dall'esito incerto. La comprensione del rischio nella storia antica era spesso legata alla divinazione e alla religione. Ad esempio, l'oroscopo e la lettura delle viscere degli animali sacrificate erano usati come metodi per prevedere il futuro e mitigare i rischi.

Tuttavia, l'antichità ha anche visto la nascita di alcune pratiche che possono essere considerate precorritrici del Risk Management moderno. Ad esempio, gli antichi babilonesi utilizzavano la tecnica del contratto a premio per coprire i rischi legati alla navigazione fluviale e commerciale. In base a questi contratti, i commercianti pagavano una somma iniziale (il premio) per coprire il rischio di perdere la merce a causa di eventi imprevisti come il naufragio o il furto.

Inoltre, già in questi anni si sono sviluppati alcuni concetti fondamentali che sono ancora utilizzati nella gestione del rischio. Ad esempio, la legge delle conseguenze impreviste, nota anche come effetto farfalla, che sostiene che una piccola azione può avere conseguenze imprevedibili e di grande portata, è stata formulata già dall'antico filosofo greco Eraclito. Anche il concetto di diversificazione del rischio, ovvero la pratica di ridurre il rischio

attraverso l'investimento in diverse attività, è stato proposto da antichi filosofi come Aristotele e Plinio il Vecchio. Nell'antica Roma esistevano forme di assicurazione marittima che coprivano il rischio di perdita delle merci durante il trasporto. In generale, l'antichità ha visto la nascita di alcune pratiche e concetti fondamentali che sono stati alla base dello sviluppo del Risk Management moderno. Tuttavia, la comprensione del rischio e la sua gestione sono evolute notevolmente nel corso dei secoli successivi, grazie a importanti studi e innovazioni tecnologiche.

1.4.2 Età medievale

Durante l'età medievale il concetto di rischio si è sviluppato intorno ad un altro elemento importante: le assicurazioni. Le prime documentazioni del fenomeno assicurativo si collocano intorno al secolo XII ed alla rivoluzione commerciale che vede l'affermazione di fenomeni politici ed economici originali che fecero delle città italiane, in termini di sviluppo e di organizzazione, un vero e proprio modello. Durante l'età medievale, il concetto di rischio era legato principalmente alle attività commerciali e marittime. Gli scambi commerciali erano infatti spesso effettuati in luoghi lontani e pericolosi, come i mari infestati dai pirati, e comportavano notevoli rischi di perdite finanziarie. Nel XII secolo, a Genova, venne creata la prima forma di compagnia assicurativa marittima, per coprire i rischi di perdita di merci e navi. Inoltre, nel XIV secolo, venne sviluppata la pratica

dell'assicurazione sulla vita, grazie all'introduzione delle tontine[1]. In questo contesto, i mercanti svilupparono strategie per minimizzare il rischio, come la diversificazione degli investimenti e la stipula di contratti di assicurazione (Pergiovanni V., 1965). La città di Venezia, grazie alla sua posizione privilegiata, divenne uno dei principali centri del commercio marittimo medievale. Qui si sviluppò il concetto di "assicurazione a premio", che consisteva nella suddivisione del rischio tra diversi investitori, i quali avrebbero pagato una somma di denaro in cambio della garanzia di un eventuale rimborso in caso di perdite (Melis F., 1975).

Tuttavia, l'idea di una gestione sistematica del rischio non si diffuse ampiamente fino al Rinascimento, quando gli esploratori iniziarono a effettuare viaggi sempre più lunghi e pericolosi, alla ricerca di nuovi mercati e risorse. In questo contesto, l'italiano Luca Pacioli, considerato il padre della contabilità moderna, sviluppò un metodo per valutare il rischio di un'impresa commerciale, basato sull'analisi delle entrate e delle uscite. Durante l'età medievale, inoltre, la chiesa cattolica ebbe un ruolo importante nella gestione del rischio, soprattutto in campo agricolo. La coltivazione della terra, infatti, era soggetta a molte incertezze, come la siccità, le piogge torrenziali e le malattie delle piante. Fu promossa la creazione di organismi di mutua assistenza, come le confraternite agricole, che permettevano ai contadini di condividere il rischio e di aiutarsi reciprocamente in caso di calamità naturali. L'attenzione al rischio iniziò piano piano a diventare multidimensionale, ad aprirsi a differenti tematiche non solamente in relazione al mondo mercantile e del commercio.

[1] La tontina è un contratto finanziario e di investimento proposto in Francia da Lorenzo de Tonti, in cui gli aderenti versano una quota, in virtù della quale percepiscono poi interessi o rendite.

1.4.3 Età moderna

Come ha ricordato Peter L. Bernstein ("Risk as a History of Ideas", 1995), è solo dal Rinascimento, con il definitivo affermarsi della numerazione araba, che il rischio è stato indagato con criteri scientifici. Il Liber de Ludo Aleae (1525), del Cardano, può forse dirsi la prima vera trattazione riguardante un caso specifico di probabilità: quella connessa ad alcuni giochi di carte. A partire da allora, la misurazione del rischio avrebbe tenuto impegnate numerose generazioni di matematici, specie quelli più sensibili a questioni economiche e finanziarie.

Nell'età moderna, la gestione del rischio ha subito importanti evoluzioni grazie ai moltissimi studi e innovazioni tecnologiche. Uno degli eventi chiave di questo periodo è stata la nascita della statistica come disciplina scientifica. Nel XVII secolo, il matematico inglese John Graunt (1662) utilizzò i dati demografici per studiare l'incidenza della peste nella città di Londra, riuscendo a individuare alcune delle cause della diffusione della malattia. Nel XVIII secolo, il matematico svizzero Daniel Bernoulli applicò la teoria delle probabilità alla valutazione del rischio in campo assicurativo, dimostrando come il valore di un'assicurazione dipendesse dalla probabilità di verificarsi del rischio assicurato. Sono noti, tra gli altri, i contributi di Pascal e Fermat (che, a cavallo del '600, risolsero il "dilemma dei punti" che Pacioli aveva posto oltre un secolo e mezzo prima), di Abraham de Moivre (che per primo presentò la struttura della distribuzione normale) e del già citato Daniel Bernoulli (è suo il celebre "paradosso di San Pietroburgo").

1.4.4 Età contemporanea

Nel corso del XIX secolo, la tecnologia ha fatto importanti passi avanti, contribuendo alla nascita di nuove industrie e alla diffusione di nuove tecnologie. Tuttavia, questo progresso ha comportato anche l'insorgere di nuovi rischi, come gli incidenti industriali e le malattie professionali. Per questo motivo, si è resa necessaria la creazione di nuove norme di sicurezza e la diffusione di una cultura della prevenzione del rischio. Negli Stati Uniti, alla fine del XIX secolo, la Standard Oil Company ha sviluppato un modello di gestione del rischio che ha fatto scuola. In particolare, la compagnia ha creato un dipartimento di sicurezza industriale che si occupava di identificare i rischi associati alle attività produttive e di sviluppare soluzioni per prevenirli. In Europa, invece, la gestione del rischio è stata influenzata dall'esperienza della Prima guerra mondiale, che ha evidenziato la necessità di una gestione razionale delle risorse e di una pianificazione a lungo termine. In particolare, la Germania ha sviluppato una metodologia di analisi del rischio basata sull'individuazione dei punti deboli del sistema produttivo e sulla messa in atto di interventi di prevenzione mirati.

Con l'estensione delle conoscenze matematiche e del numero di rischiosità da indagare, la ricerca sul tema ha conosciuto una rapida crescita, al punto da assicurare al Risk Management – nel Novecento – il raggiungimento di una propria autonomia disciplinare, soprattutto nel campo degli studi finanziari. Uno sviluppo talmente incisivo che, secondo lo stesso Bernstein (1996), il controllo del rischio può persino esser considerato «What […] distingueshes the thousands of year of history from what we think of as a modern times».

Una tappa fondamentale per l'istituzionalizzazione della teoria economica del rischio e dell'incertezza è senza dubbio il volume Risk,

Uncertainty, and Profit, di Frank Knight (Risk, uncertainty and profit, 1921). Si tratta di un'opera nella quale, distinguendo appunto tra situazioni di rischio e situazioni di incertezza (nelle prime l'agente economico è in grado di stimare la probabilità del verificarsi di un evento; nelle seconde questa stima non è possibile), l'autore fissa i principali riferimenti di questa nuova formulazione teorica e costruisce su di essi una prima modellizzazione. Il contributo di Knight – negli anni a seguire – ha aperto la strada all'applicazione della teoria del rischio e dell'incertezza per la spiegazione di fenomeni economici e finanziari come i profitti, le decisioni di investimento, le aspettative, l'equilibrio economico generale, la struttura dell'impresa e la finanza aziendale. Nei successivi e più recenti decenni, il cammino di affermazione della disciplina è continuato grazie ai progressi della statistica inferenziale, mentre sul piano istituzionale sono fiorite iniziative ed enti di ricerca, associazioni di studiosi e riviste accademiche dedite all'esame del Risk Management; provvedimenti di legge, infine, e più recenti certificazioni hanno progressivamente dato una più precisa veste normativa ai principi di prudenza e di contenimento del rischio (Kloman H.F, 2010).

Il periodo che va dalla Seconda guerra mondiale alla metà degli anni '60 è stato un periodo formativo, caratterizzato da una fiorente intraprendenza e creatività da parte di uomini d'affari, con un grande sviluppo dei mercati finanziari. Sono apparsi nuovi rischi, quelli vecchi si sono aggravati e, spinta dalle risposte dei gestori del rischio, la funzione di gestione del rischio si è evoluta rapidamente e ha acquisito il suo titolo e una definizione fondamentale. La concezione moderna di rischio parte dal 1955, quando Wayne Snider, professore di Assicurazioni alla Temple University, suggerì che, poiché i gestori assicurativi si stavano ora concentrando sui rischi e sui

modi per controllarli, piuttosto che limitarsi all'acquisto di assicurazioni, avrebbero dovuto essere chiamati gestori del rischio (Crockford G., 1982) . Con la "Theory of Games and Economic Behavior" (Von Neumann J. e Morgenstern O., 1944) si iniziano gli studi scientifici ed empirici sul rischio. L'assunto di base si fonda sul fatto che ogni scelta che effettuiamo è caratterizzata da incertezza, e gli studi sull'analisi del rischio hanno quindi l'obiettivo di trasformare in probabilità calcolabile tale incertezza.

Il periodo dalla metà degli anni '60 ad oggi è stato caratterizzato da nuove sfide: i rischi derivanti dalla ricerca scientifica e dalle invenzioni ingegneristiche, una maggior attenzione alle questioni sociali e al futuro ecc. Negli anni '60, il concetto di rischio subì importanti sviluppi in diversi campi, ad esempio nel campo della medicina, con l'introduzione del concetto di "rischio relativo" nella valutazione degli effetti dei farmaci e delle terapie. Questa innovazione portò a una maggiore attenzione verso la valutazione dei rischi legati alla salute, e alla necessità di una gestione accurata del rischio nei trattamenti medici. Negli anni '80 nacque la regolamentazione internazionale del rischio. In quegli anni la gestione del rischio subì importanti sviluppi nell'ambito del settore finanziario, con l'introduzione di nuovi prodotti finanziari come i derivati, che comportarono una maggiore complessità nella valutazione del rischio. Questo portò alla creazione di nuovi strumenti di gestione del rischio, come la copertura dei rischi tramite la creazione di portafogli di investimento diversificati. Le istituzioni finanziarie hanno sviluppato modelli interni di gestione del rischio e formule di calcolo del capitale per proteggersi da rischi imprevisti e ridurre il capitale regolamentare. Allo stesso tempo, la governance della gestione del rischio è diventata essenziale, è stata introdotta la gestione integrata del rischio ed è stata creata la posizione di

Chief Risk Manager (CRM). Dagli anni '70 con Kahneman e Tversky (1979), il rischio è diventato sempre più complesso e multidimensionale, includendo la valutazione dei rischi derivanti dalla complessità dei sistemi, come le reti sociali e le infrastrutture critiche. La percezione del rischio è stata considerata un fattore chiave nella sua valutazione, insieme alla comunicazione. Ogni decisione in cui è presente il rischio include due aspetti distinti e inseparabili: i fatti oggettivi e la soggettiva visione legata alla possibile perdita o guadagno. L'evoluzione del concetto di rischio e del Risk Management ha seguito un percorso lungo e complesso nel corso della storia umana (Bernstein P.L., 1996). Negli anni più recenti, uno dei primi eventi che sollevarono preoccupazioni sulla gestione del rischio fu la crisi finanziaria del 1992, che portò alla svalutazione della lira italiana e alla crisi del Sistema Monetario Europeo. Questa crisi portò alla luce la vulnerabilità dei sistemi bancari e finanziari, mettendo in dubbio l'efficacia delle metodologie di valutazione del rischio fino ad allora utilizzate. Nel 1995 fu introdotto un nuovo modello di gestione del rischio chiamato "Value at Risk" (VaR). Questo modello, che rappresentò una vera e propria rivoluzione nella gestione del rischio, consisteva nell'utilizzo di un'analisi statistica delle fluttuazioni di prezzo per calcolare il massimo potenziale di perdita di un investimento in un determinato intervallo di tempo (Morgan J.P., 1995). Dalle pratiche divinatorie dell'antichità all'utilizzo di tecnologie avanzate nella gestione del rischio odierna, la comprensione e la gestione del rischio hanno subito numerosi sviluppi e cambiamenti. Gli eventi chiave e gli studi importanti hanno contribuito a definire le fasi di questo processo, portando alla creazione di una disciplina sempre più sofisticata e complessa. Oggi, la gestione del rischio è un'attività cruciale in quasi tutti i

settori, in cui l'uso di tecniche e strumenti avanzati è indispensabile per prevenire e mitigare i rischi.

Negli ultimi decenni, la gestione del rischio è stata influenzata anche da una serie di eventi globali, come gli attacchi terroristici dell'11 settembre 2001, che portarono alla creazione di nuove politiche di gestione del rischio a livello internazionale. Inoltre, la pandemia di COVID-19 ha rappresentato una sfida senza precedenti per la gestione del rischio, portando alla creazione di nuovi modelli di valutazione dei rischi e alla revisione delle strategie di gestione del rischio.

1.4.5 Milestones in letteratura

Alcuni importanti milestones in letteratura per quanta riguarda la natura del rischio:

1815 Pierre-Simon Laplace scrive "An Essay on Probabilities" in cui introdusse la teoria delle probabilità e la sua applicazione al calcolo del rischio.

1915 Friedrich Leitner pubblica "Die Unternehmensrisiken in Berlin", una dissertazione sul rischio finanziario e alcune risposte ad esso, come l'assicurazione.

1921 Frank Knight pubblica "Risk, Uncertainty and Profit", un libro divenuto poi chiave nel risk management. Per la prima volta vengono separati il concetto di incertezza, che non è misurabile, dal rischio, invece misurabile.

1921 "The Economics of Welfare" di Arthur Pigou introdusse il concetto di "costo sociale" per affrontare gli effetti negativi delle attività economiche sull'ambiente e sulla salute pubblica.

1928 John von Neumann pubblica il suo primo articolo sulla teoria dei giochi e le strategie, "Zur Theorie der Gesellschaftsspiele", in cui introduce il concetto di "utilità attesa" come strumento per prendere le decisioni in situazioni di incertezza. La sua teoria ha fornito un modo per quantificare e confrontare i rischi in modo razionale fornendo una base teorica per la valutazione e gestione del rischio anche se non tiene in considerazione i fattori soggettivi che verranno poi introdotti più avanti negli anni.

1956 Russel B. Gallagher pubblica "Risk management: new phase of cost control", uno dei primi riferimenti al concetto di risk management presente in letteratura

1964 Robert I. Mehr e Bob A. Hedges pubblicano "Risk Management in Business Enterprise" uno dei primi libri accademici pubblicati in materia di risk management in azienda, che non si focalizza solamente sul rischio finanziario.

1979 Daniel Kahneman e Amos Tversky pubblicano la "Prospect Theory", dimostrando che la natura umana può essere irrazionale, soprattutto di fronte al rischio.

1985 È pubblicata la "ISO 31000: Risk management - Principles and guidelines", La norma che definisce i principi e le linee guida per la gestione del rischio a livello organizzativo.

1987 il PMI pubblica la prima versione del "PMBOK", guida che ha lo scopo di documentare e standardizzare le pratiche del project management.

1992 "The COSO Report"- Il rapporto della Commissione sui sistemi di controllo interni dell'Organizzazione degli studi contabili statunitensi (COSO) presentò un quadro per la gestione del rischio aziendale e delle attività di controllo.

1996 Peter L. Bernstein pubblica "Against the Gods: The Remarkable Story of Risk" in cui si racconta la storia del concetto di rischio, della sua origine dal rinascimento a oggi.

2002 "Enterprise Risk Management - Integrated Framework" di COSO - Il quadro integrato di gestione del rischio di COSO offrì un approccio olistico alla gestione del rischio aziendale, che includeva la strategia, le operazioni e la comunicazione.

2004 Terza edizione del "PMBoK" in cui è inserito un capitolo sul Project Risk Management. In precedenza, il rischio era trattato solo come una delle nove aree di conoscenza del project management.

2007 "ISO 31000:2009: Risk management - Principles and guidelines" - La norma ISO 31000 del 2009 ha aggiornato le linee guida del 1985, fornendo un approccio più flessibile e integrato alla gestione del rischio a livello organizzativo.

2010 Nassim Nicholas Taleb scrive "The Black Swan", libro in cui introdusse il concetto di "Cigno Nero", eventi imprevedibili con un impatto significativo sul mondo, come la crisi finanziaria del 2008.

2015 La "ISO 9001:2015" richiede di applicare un approccio basato sui rischi alla gestione della qualità. Ciò comporta l'adozione di una visione globale dei rischi dell'attività aziendale e coinvolge l'alta direzione nell'intero processo di mitigazione dei rischi.

1.5 Risk Appetite

Come abbiamo visto, nel processo di gestione del rischio, ma più in particolare nella fase di identificazione e valutazione, è indispensabile tener conto della soggettività, la quale caratterizza le considerazioni effettuate. Ogni individuo ha infatti obiettivi, punti di vista, informazioni e propensione al rischio diverse. Tutto ciò, congiuntamente alle caratteristiche intrinseche della persona, contribuisce a generare valutazioni molto differenti sui rischi.

Mentre è molto complicato andare ad analizzare il differente punto di vista di un individuo, o il suo modo di ragionare, è relativamente semplice individuare, oltre agli obiettivi, il risk appetite

Sono presenti diversi concetti simili al risk appetite, e per evitare ambiguità, forniamo le seguenti definizioni (Hillson D., 2012):

- **Risk Appetite**: tendenza interiore nel prendersi un rischio in una data situazione.
- **Risk Tolerance**: ha un significato duplice, può essere sia quanto rischio si è disposti a tollerare che, in termini misurabili, l'ampiezza della variazione di tollerabilità del rischio. Nelle organizzazioni si identifica come la disponibilità a sopportare il rischio dopo il suo trattamento al fine di raggiungere i propri obiettivi (International Standards Organization (ISO), 2009).
- **Risk Attitude**: scelta di comportamento nei confronti del rischio. Si può essere avversi, neutrali o propensi al rischio comprendendo tutte le sfumature intermedie. Nelle organizzazioni si identifica con l'approccio che queste hanno per valutare o eventualmente perseguire, mantenere, adottare o allontanarsi dal rischio (International Standards Organization (ISO), 2009).

- **Risk Treshold**: soglia di accettabilità del rischio. Al di sopra di questa soglia il rischio non è accettabile e va affrontato (PMI, 2017).
- **Risk Capacity**: si riferisce alla quantità massima di rischio che un'organizzazione è in grado di sopportare (ISACA, 2012).

La distinzione tra risk appetite e risk tolerance è molto sottile. La tolleranza al rischio è il livello di rischio che un'organizzazione può accettare per singolo rischio, mentre la propensione al rischio è il rischio totale che l'organizzazione può sopportare in un dato profilo di rischio, solitamente espresso in forma aggregata.

I due termini sono correlati e molto vicini ma non sono interscambiabili. La tolleranza al rischio è la quantità di deviazione accettabile dalla propensione al rischio di un'organizzazione. Mentre la propensione al rischio è un concetto filosofico ampio e strategico che guida gli sforzi di gestione del rischio di un'organizzazione, la tolleranza al rischio è un concetto molto più tattico che identifica il rischio associato a un'iniziativa specifica e lo confronta con la propensione al rischio dell'organizzazione. Si può pensare alla tolleranza al rischio di un'organizzazione per un'iniziativa specifica come alla volontà dell'organizzazione di accettare il rischio che rimane dopo che tutti i controlli pertinenti sono stati messi in atto (ISACA, 2012).

1.5.1 L'appetito è una tendenza

In ogni attività, gruppo di attività, progetto, o strategia aziendale, quando si presenta un rischio di qualsiasi tipologia, è naturale porsi le seguenti domande:

- Quanto rischio **abbiamo**?

- Quanto ne **possiamo** affrontare?
- Quanto rischio **dovremmo** prenderci?
- Quanto rischio **vogliamo** prenderci?
- Quanto rischio ci **prenderemo effettivamente**?

Per poter rispondere a questo insieme di domande, chiaramente concatenate, bisogna prima comprendere il concetto di appetito, poi quello di Risk Appetite ed infine come questo debba essere gestito.

Appetito: Tendenza a soddisfare le proprie necessità o i propri bisogni[2]. L'appetito viene generato da motivazioni interne ed intrinseche che creano il desiderio di soddisfarlo. Ad esempio: Avere fame non significa avere appetito, si potrebbe chiedere "qual è il tuo appetito per il cibo?" Usiamo la fame come "proxy" per comprendere l'appetito. Successivamente possiamo valutare la fame usando una misurazione. In generale, quindi, quando si parla di appetito c'è bisogno di associargli una delega, perché è nascosto internamente.

Il Risk Appetite risponde alla domanda "quanto rischio vogliamo prenderci?".

Questo concetto incontra bisogni di rischio, che possono essere noti o meno, può riferirsi ad aspetti strategici, di progetto o di attività. Associando la definizione di appetito al rischio si comprende come questo sia un input interno e non è valutabile come una quantità di rischio. La quantità di rischio soddisfa l'appetito, ne è la sua espressione. Il valore di questa quantità verrà chiamato treshold (soglia).

L'importanza dell'associare la soddisfazione dell'appetito con una quantità di rischio è data dal fatto che l'appetito risponde al set di domande

[2] Definizione del vocabolario Treccani.

di cui sopra. Ogni decisione intrapresa è legata alle domande e la risposta a queste domande dipende dall'appetito al rischio.

1.5.1.1 Input e output dell'appetito

L'appetito al rischio è conseguenza di una serie di input e la sua manifestazione genera un output preciso e numerico.

Gli input del risk appetite sono: la situazione in cui si presenta un rischio, il contesto nel quale la situazione è inserita, e più nel particolare gli obiettivi che scegliamo di voler raggiungere in quella situazione.

Le decisioni vengono prese dagli individui, i quali avranno le loro **preferenze** e **propensioni** al rischio. Le preferenze sono gli aspetti intrinseci mentre la propensione è come questi vengono espressi.

I decisori influenzeranno singolarmente quanto rischio si prenderà. Questa decisione ha una declinazione nei gruppi/uffici e nella cultura del rischio aziendale. L'appetito degli individui, gruppi e organizzazione si contrappone alla situazione, essendo interni e influenzati da altri fattori, togliendo ad essa l'importanza che merita.

Gli output sono delle quantità precise e misurabili: le soglie/treshold. La soglia diviene la visione numerica (driver esterno) dell'appetito (driver interno). Il problema che si presenta è fortemente concettuale: si vuole raggiungere un valore numerico (spesso probabilistico) da poter utilizzare, sfruttando concetti (appetito, preferenza, propensione e cultura di persone, gruppi e aziende) che non vengono precisamente definiti, che sono intrinseci degli attori coinvolti e che quindi, semplicemente, non sono chiari. Una conseguenza molto probabile della scelta delle soglie di rischio, identificate tramite queste "tendenze," è che siano sbagliate, mal quantificate.

1.5.1.2 Dall'appetito all'attitude

Nella maggior parte dei casi l'appetito e tutto ciò che ne consegue devono essere moderati per poter raggiungere gli obiettivi prefissati. Ad esempio, se avessi molta fame (che soddisfa l'appetito) non dovrei andare a mangiare in un ristorante All You Can Eat se poco dopo ho un impegno che richiede un elevato sforzo fisico e mentale come un allenamento in sala pesi. Si evince, quindi, il bisogno di distinguere tra appetito semplice e appetito giudicato e controllato.

In prima istanza, bisogna controllare se la quantità di rischio che l'individuo vuole assumere sia effettivamente giusta e in linea con la capacità di gestire il rischio (**risk capacity**). Se la quantità voluta è superiore della capacità effettiva allora bisogna intervenire, prendendo delle scelte deliberate, per fare sì che il rischio intrapreso sia gestibile. Per poter decidere in maniera più precisa quanto rischio prendersi si utilizza la **risk attitude**, che può essere definita come la risposta **scelta** deliberatamente al rischio, mossa dalle percezioni. Essendo una scelta, possiamo decidere se essere più o meno avversi/propensi al rischio e, se questa decisione genera soglie non appropriate, si potrà sempre modificare. L'attitude offre la possibilità di moderare l'appetito al rischio, il quale è intrinseco e spinge verso un dato set di soglie sulle quali non si può intervenire.

Situazione, obiettivi, esposizione intrinseca al rischio, bias ed esperienza influenzano la percezione al rischio, la quale guida l'attitudine che si vorrà adottata. Quindi, si svolgono azioni nei confronti del rischio, le quali modificano il rischio intrinseco in rischio residuo, il quale, se servirà potrà essere gestito. Appetito e attitudine sono concetti che hanno input e output simili, infatti, definendoli in funzione di questi si può dire che:

- L'appetito è conseguenza della situazione e delle persone, le quali producono soglie da controllare in funzione della capacità.
- L'attitudine è basata sulle percezioni che provengono dalla situazione unita a driver consci e inconsci e ha come risultato la configurazione delle soglie.

Semplificando: ci interfacciamo con una situazione importante che ha un certo rischio associato e dobbiamo decidere quanto rischio prenderci. Bisogna comprendere che abbiamo una tendenza, la quale è influenzata da individui e gruppi. Successivamente si deve prendere decisione di posizionarci nello spettro dell'attitudine, avversi, neutrali o propensi. Questa scelta influenzerà le soglie, e quanto rischio ci prenderemo.

1.5.2 Fattori che influenzano il risk appetite

L'attitudine al rischio può variare in base a una serie di fattori, quali: settore, cultura aziendale, concorrenti, natura degli obiettivi perseguiti, solidità finanziaria e capacità dell'organizzazione. Vale anche la pena notare che la propensione al rischio può cambiare nel tempo. È sempre una buona idea valutare i rischi in base ai criteri di rischio periodicamente o continuamente, a seconda delle circostanze, delle risorse disponibili, delle competenze, delle tecnologie o dei sistemi. Molti studi dimostrano che l'assunzione di rischi non dipende solo dalle caratteristiche generali dei soggetti dell'esperimento, ma anche dal loro attuale stato fisico, mentale e psicologico (Berlinger E. e Vàradi K., 2015):

- **Fatica della decisione**: se siamo stanchi, diventiamo automaticamente più avversi al rischio. Prendere decisioni multiple esaurisce il sé (Baumeister R. F. e Tierney J., 2011).

- **Social Loaf**: le persone tendono a correre più rischi quando sono in gruppo che da sole. (Dobelli R., 2013)
- **Euristica affettiva**: se ci piace qualcosa o ci troviamo di buon umore, percepiamo il rischio come minore e i guadagni maggiori di quanto non siano in realtà.
- **Impulsi di genere**: come parte dell'esperimento, hanno mostrato fotografie di belle donne e, di conseguenza, i soggetti maschi partecipanti sono diventati percettibilmente più rischiosi. Questo, tuttavia, non ha funzionato con fotografie di donne meno belle o con il cambio di genere. (Baumeister R. F. e Tierney J., 2011)
- **Effetto ribalta**: le persone corrono molti più rischi in completo anonimato che sotto i riflettori. (Baltussen G., Van den Assem M. J. e Van Dolder D., 2014)
- **Effetto easy come, easy go (effetto denaro della casa):** trattiamo il denaro in modo completamente diverso a seconda che sia facile o difficile da acquisire. Se abbiamo vinto, trovato o ereditato il denaro, tendiamo a essere più accomodanti nello spenderlo e nel rischiarlo di quanto saremmo se lo avessimo guadagnato con un duro lavoro. (Thaler R. H. e Johnson E. J., 1990)
- **Effetto Minsky:** il successo aumenta la propensione al rischio, cioè la propensione al rischio aumenta come conseguenza di guadagni successivi (dipendenza dal percorso). (Minsky H. P., 1992)

Questi effetti sono in contrasto con la teoria dell'utilità perché mettono in discussione l'esistenza di una disposizione all'assunzione di rischi che sia stabile e costante nel tempo ed è caratteristica degli individui.

1.5.3 Risk appetite a livello aziendale

Ogni organizzazione ha una particolare **capacità di rischio**, definita come la quantità oggettiva di perdita che un'impresa può tollerare senza che la sua esistenza sia messa in discussione. La propensione al rischio è definita come la quantità di rischio che un'entità è disposta ad accettare nel perseguimento della propria missione. In alcuni casi, la determinazione della propensione al rischio può essere delegata dal consiglio di amministrazione all'alta direzione nell'ambito della pianificazione strategica.

La determinazione del rischio accettabile o la propensione al rischio e i criteri in base ai quali può essere valutata sono elementi essenziali per un gran numero di aspetti della sicurezza delle informazioni, nonché per la maggior parte degli altri aspetti delle attività organizzative. La propensione determina molti aspetti della strategia, inclusi gli obiettivi di controllo, l'implementazione del controllo, la sicurezza di base, i calcoli costi-benefici, le opzioni di gestione del rischio, la determinazione dei criteri di gravità, le capacità di risposta agli incidenti richieste, i requisiti assicurativi e le valutazioni di fattibilità, tra gli altri.

La propensione al rischio si traduce in una serie di standard e politiche per contenere il livello di rischio entro i limiti fissati. Questi confini devono essere regolarmente adeguati o confermati. Una volta definiti i limiti, i piani di azione da intraprendere per rispondere ai vari rischi, possono essere definiti attraverso un processo formale, che coinvolge tutta l'azienda o solamente il responsabile della gestione del rischio, e finché si è all'interno dei limiti definiti, questo ha una libertà abbastanza ampia di movimento.

L'accettazione del rischio generalmente non dovrebbe superare la propensione al rischio dell'organizzazione e, sicuramente, non deve

superare la capacità di rischio (che minaccerebbe la continua esistenza dell'organizzazione). (ISACA, 2012)

1.6 Concetto di rischio in ambito infrastrutturale

Spostando l'analisi sui settori dell'ingegneria civile, delle costruzioni e delle infrastrutture, il significato di rischio e tutto ciò che ne è legato ha una nuova declinazione, conseguenza dell'aumento di specificità del contesto di analisi.

I progetti che hanno come fine ultimo la costruzione di un prodotto infrastrutturale, come un palazzo, un ponte o una linea ferroviaria, hanno sia un gran numero di fonti di incertezza esterne che numerosi rischi interni ai processi di realizzazione e utilizzo dell'opera.

La gestione del rischio per questa tipologia di progetti risulta di cruciale importanza per minimizzare i potenziali effetti negativi dei rischi (massimizzando le potenziali opportunità) associati ad opere che nella quasi totalità dei casi, saranno sfruttate da un gran numero di persone per molti anni (il ponte di Brooklyn NY, terminato nel 1883 viene attraversato da oltre 116.000 macchine, 30.000 pedoni e 3.000 biciclette al giorno)[3]. Inoltre, la presenza di un sistema moderno ed efficiente di infrastrutture è una componente fondamentale dello sviluppo economico del paese, dell'integrazione territoriale e dell'aumento di competitività delle imprese. La definizione di infrastruttura sottende il concetto di beni e servizi, materiali e immateriali.

[3] Dati del New York City Department of Transportation consultabili al seguente **link**.

I paesi maggiormente industrializzati sono dotati di sempre più estesi e sofisticati sistemi infrastrutturali, le cosiddette Infrastrutture Critiche (IC), come le reti di distribuzione dell'energia e le infrastrutture del trasporto, così come specificato nella Direttiva del Consiglio Europeo, ma che possono riguardare anche altri settori come si vedrà meglio in seguito.

1.7 Normativa europea

Prima di analizzare gli aspetti ingegneristici del rischio infrastrutturale vengono introdotte le nozioni normative di maggiore interesse, essendo il suddetto rischio fortemente legato ad opere di grandissimo utilizzo.

La Direttiva Europea 114/08 CE[4] definisce "infrastruttura critica" (IC) un elemento, un sistema o parte di questo ubicato negli Stati membri ed essenziale al mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale dei cittadini, il cui danneggiamento o la cui distruzione avrebbe un impatto significativo.

La stessa Direttiva definisce "Infrastruttura Critica Europea" (ICE) un'infrastruttura critica ubicata negli Stati membri dell'UE la cui perturbazione o distruzione avrebbe un significativo impatto su almeno due Stati membri dell'UE. La rilevanza dell'impatto è valutata in termini intersettoriali. Il fatto che un'infrastruttura sia considerata critica dall'UE non significa che si rendono automaticamente necessarie misure supplementari di protezione. Le misure di protezione esistenti, che possono comprendere accordi bilaterali tra Stati membri, possono essere perfettamente adeguate e quindi rimanere immutate in caso di valutazione

[4] Direttiva dell' 8 dicembre 2008, n.114 del Consiglio dell'Unione Europea.

di IC/ICE. Inoltre, non bisognerebbe dimenticare di prendere in considerazione le IC che hanno origine o si trovano in un paese terzo, ma sono interconnesse o hanno potenzialmente un effetto diretto sugli Stati membri dell'UE. (Commissione Europea, 2005)

Il concetto di rischio nelle infrastrutture è molto ampio poiché, queste, sono soggette a numerose minacce: possono essere danneggiate, distrutte o manomesse a causa di atti deliberati di vandalismo o terrorismo, calamità naturali, negligenza, incidenti, pirateria informatica, attività criminose e comportamenti dolosi.

Un'eventualità di questo tipo diventa sempre più probabile dal momento che le nuove tecnologie e la liberalizzazione dei mercati (per esempio nel settore dell'elettricità e della fornitura di gas) fanno sì che molte infrastrutture siano parte di una rete più ampia. Ciò significa che può rendersi necessario un livello comune di protezione. Perché la protezione sia efficace è necessario che vi siano comunicazione, coordinamento e cooperazione a livello nazionale, dell'UE e internazionale tra tutti gli operatori del settore. Al fine di sostenere le attività degli Stati membri la Commissione delle Comunità Europee agevola l'individuazione, lo scambio e la diffusione delle migliori pratiche in materia di protezione delle infrastrutture critiche creando un quadro comune per la protezione delle infrastrutture critiche. La portata di tale quadro generale deve essere esaminata. (Commissione Europea, 2005)

1.8 Normativa italiana

La normativa e le raccomandazioni italiane prevedono l'applicazione sistematica dell'analisi di rischio, sostanzialmente, in due specifici ambiti relativi alla realizzazione di opere civili infrastrutturali: per la previsione dei rischi per la sicurezza e la salute dei lavoratori[5] e per la valutazione dei rischi per la sicurezza dell'esercizio delle gallerie stradali[6] e ferroviarie[7].

Nell'appendice "B" del D. lgs. n. 61 dell'11 aprile 2011[8] compaiono, in modo sintetico, alcune indicazioni circa gli elementi che il Piano di Sicurezza dell'Operatore (PSO) deve contenere. Il PSO deve necessariamente comprendere:

- L'individuazione degli elementi più importanti dell'infrastruttura. Cioè beni, risorse e attività la cui disponibilità dovrà essere sempre garantita e ai quali applicare le azioni preventive e difensive che permettano un'efficace protezione dell'infrastruttura.
- L'analisi dei rischi, realizzata sulla prefigurazione degli scenari di rischio più rilevanti e allo scopo di individuare le vulnerabilità degli elementi dell'infrastruttura e le conseguenze che deriverebbero dal mancato funzionamento di ciascun elemento sulla funzionalità dell'intera infrastruttura.
- L'identificazione delle misure e procedure più idonee alla prevenzione e protezione distinguendole tra misure permanenti e misure ad applicazione graduata.

[5] Decreto Legislativo 9 aprile 2008, n. 81
[6] Decreto Legislativo 5 ottobre 2006, n. 264
[7] Decreto Ministeriale 28 ottobre 2005, n. 89
[8] Decreto Legislativo 11 aprile 2011, n. 61

1.9 Le fasi e tipologie di rischio della costruzione

Nei progetti del settore delle costruzioni i rischi possono provenire da fonti di incertezza molto diverse e possono presentarsi in ogni fase del progetto.

In letteratura si è soliti identificare le principali fonti di incertezza nei progetti di costruzione tramite il framework **PESTLE**[9]:

- Political,
- Economic,
- Social,
- Technological,
- Legal,
- Environmental.

Il paper intitolato "Risk Management in construction projects" (Szymanski P., 2017), invece, suddivide i rischi in cinque macro-gruppi, legati principalmente a specifiche fasi del processo di costruzione:

- Design Preliminare,
- Gara d'appalto,
- Design dettagliato,
- Costruzione e
- Finanziamento dell'investimento.

La combinazione delle fonti di incertezza con le fasi che raggruppano i rischi vanno a identificare un insieme di rischi individuali associabili, nella maggior parte dei casi, ai progetti di costruzione. È chiaro che la loro

[9] Diversi articoli e paper non citano espressamente l'utilizzo del framework PESTLE ma tutti elencano tutte o quasi le fonti di incertezza che la compongono, risulta quindi più completo citare il framework in sé.
Il PESTLE è un framework molto utilizzato sia nei contesti aziendali che nelle prime fasi di progetti e sé stanti.

eventuale presenza e pericolosità dipenderà fortemente dal contesto di ogni singolo progetto. Non va dimenticato, inoltre, che nel tempo alcuni rischi potrebbero scomparire grazie alle innovazioni tecnologiche ma venire sostituiti da nuovi ancora non identificabili.

Al netto della precisazione, risulta intuitivo come i potenziali rischi per i progetti che abbiano come fine la costruzione di un'infrastruttura possano essere molti. Tra le fasi del progetto, la più importante e soggetta a maggior rischio è sicuramente la costruzione, invece, tra i rischi che si considerano più ricorrenti si evidenziano (Szymanski P., 2017):

- rischio di suolo mal riconosciuto,
- rischio di rottura equipaggiamento,
- rischio di assenza operai/dipendenti,
- rischio di basso livello materie prime,
- rischio ritardi nella consegna materiale da costruzione,
- rischio di controllo non sufficiente, ecc.

Prima di entrare nel vivo dell'analisi del significato del rischio nell'ambito infrastrutturale, bisogna capirne la complessità e le caratteristiche. Gli elementi critici principali correlati alla gestione dei rischi nelle infrastrutture sono principalmente due: la presenza di forti interdipendenze e la necessità di garantire una continuità nel servizio.

1.9.1 Interdipendenze infrastrutturali

Per valutare il rischio a cui è soggetta un'infrastruttura è necessario studiare tutte le interdipendenze che questa ha con altre infrastrutture. Bisognerà considerare le infrastrutture come sistemi adattivi complessi

(CAS), cioè insieme di elementi che congiuntamente formano sinergie, influenzate dalla storia passata e in grado di modellarsi al futuro.

Un modo efficace per studiare i CAS è considerarli come popolazioni di agenti interagenti. Un agente è un'entità con una posizione specifica, capacità proprie e memoria. La posizione dell'entità definisce dove si trova in uno spazio fisico o astratto. La maggior parte dei componenti dell'infrastruttura ha una posizione ed una capacità ed è influenzata dalle esperienze passate, quindi, può venir considerata come agente.

Le infrastrutture sono spesso connesse in più punti attraverso un'ampia varietà di meccanismi, in modo tale che esista una relazione bidirezionale tra gli stati di una data coppia di infrastrutture. Le infrastrutture interdipendenti mostrano anche un'ampia gamma di caratteristiche spaziali, temporali, operative e organizzative, che possono influire sulla loro capacità di adattarsi alle mutevoli condizioni del sistema. Infine, le interdipendenze e le conseguenti topologie dell'infrastruttura possono creare sottili interazioni e meccanismi di feedback che spesso portano a comportamenti e conseguenze imprevisti durante le interruzioni. (Wang H., 2021)

Possiamo identificare quattro classi principali di interdipendenza:

- Fisica;
- Informatica;
- Geografica;
- Logica.

1.9.2 Continuità operativa

Le infrastrutture critiche devono garantire la continuità nella fornitura di servizi essenziali, questa deve essere perciò protetta e controllata.

Per garantire la continuità operativa è necessario mettere in atto misure adeguate. Per le infrastrutture critiche civili, si è resa necessaria la predisposizione del Sistema di Gestione per la Continuità Operativa (SGCO), il quale garantisce all'organizzazione la sopravvivenza in caso di interruzione dell'operatività ed il ripristino delle attività critiche entro tempi e modalità predeterminati.

Le interruzioni nelle infrastrutture critiche sono generalmente classificate come guasti a cascata ed errori di causa comune. (Rinaldi S.M., Peerenboom J.P., Kelly T.k., 2001)

Un guasto a cascata si verifica il guasto di un'infrastruttura interessa uno o più componenti in un'altra infrastruttura, comportando l'indisponibilità parziale o totale di quest'ultima. Errori di causa comune. Si verificano quando due o più infrastrutture vengono interrotte contemporaneamente perché i componenti all'interno di ciascuna infrastruttura si guastano per una causa comune.

1.9.3 Stakeholder

Più che in ogni altro progetto, nei progetti di costruzione è molto importante la presenza degli stakeholder. Bisognerebbe in prima istanza differenziare se il progetto è pubblico, finanziato dalle istituzioni o se il committente è totalmente privato. Risultano d'interesse principalmente i progetti pubblici.

In questo caso gli stakeholder principali dal design preliminare fino all'ultimazione dei lavori si può generalizzare essere gli **organi di governo** e i **contribuenti/cittadini**. In funzione dell'opera, delle sue dimensioni e importanza lo Stato sarà rappresentato da attori differenti.

Differenziando i due stakeholder risulta che:

- nel caso degli **organi di governo**, il progetto sarà influenzato fortemente dagli avvenimenti politici, positivi o negativi che siano. Se, ad esempio, una giunta regionale committente di un'opera si dovesse sciogliere per un qualsiasi motivo il progetto potrebbe venir posticipato, bloccarsi, o addirittura interrotto definitivamente. Dati del Ministero delle infrastrutture e dei trasporti riportano che al 31/12/2021 in Italia ci sono 379 opere pubbliche incompiute. (Ministero delle Infrastrutture e dei Trasporti, 2022)
- Per quanto riguarda i cittadini, questi andranno considerati come "ago della bilancia". Potrebbe essere la loro insoddisfazione a far interrompere i lavori o implicare modifiche di scopo al progetto, in entrambi i casi con conseguenze di dilatazione di tempi e aumento di costi. Da un altro punto di vista potrebbero essere parte integrante del progetto di costruzione se questo dovesse essere visto come un'opportunità per i locali.

1.9.4 Analisi delle conseguenze

A valle delle analisi preliminari uno degli aspetti più importanti del rischio infrastrutturale è l'analisi delle conseguenze. Le conseguenze di un evento di guasto sono generalmente misurate in termini che interessano

direttamente le persone e il loro ambiente, come la perdita di vite umane o lesioni e perdite economiche.

Una delle principali difficoltà nella stima delle conseguenze è data dal confronto tra perdite economiche dirette (danni agli edifici, perdite di produzione), le perdite indirette (ritardi o disagi degli utenti, impatto sulla crescita economica, disoccupazione) e le perdite non monetarie derivanti dagli infortuni degli operai, dalla perdita di vite umane, dai danni all'ambiente fino alla disgregazione sociale.

Per un lungo periodo non è stata considerata una buona pratica discutere, almeno in pubblico, del valore di una vita umana. Di fatto sono state sviluppate diverse tecniche per fornire un mezzo per confrontare le diverse conseguenze di diverse attività, ad esempio valutando le preferenze dei decisori in termini di confronti a coppie tra diversi attributi. (Warner F., 1992)

Sono stati fatti vari tentativi per quantificare il valore economico di una vita umana; questi includono: (Fisher U., Castagna L.G., Violette D.M., 1989)

- mancati guadagni a causa di morte prematura;
- valore economico di una vita (pari a $\$D \cdot x$ dove $\$D$ è l'importo che un individuo è disposto a pagare per ridurre il proprio rischio di mortalità di $1 - x$);
- denaro speso in programmi governativi per vita salvata;
- indennizzo governativo dovuto per morte per incidente.

Tuttavia, un approccio più significativo consiste nell'utilizzare un indicatore sociale che rifletta la qualità della vita in una società o in un gruppo di individui in termini di contributo individuale al Prodotto Nazionale Lordo (PNL), aspettativa di vita, tempo per godersi la vita,

ecc., come l'indice di sviluppo umano o indice di qualità della vita, che possono essere utilizzati per determinare un costo implicito accettabile per evitare una fatalità. (Lind N. C., 1994)

2 Il Project Risk Management

Uno sguardo ai progetti

I progetti svolgono un ruolo fondamentale all'interno delle aziende: sono gli elementi attraverso i quali molte imprese ottengono la maggior parte dei loro profitti. Lo sviluppo di nuovi prodotti, la ricerca, l'innovazione, il miglioramento dei processi e la commercializzazione di beni e servizi si svolgono attraverso progetti.

Il progetto, per il PMI, rappresenta "uno sforzo temporaneo per creare valore attraverso un prodotto, servizio o risultato unico. Tutti i progetti hanno un inizio e una fine; hanno un team, un budget, un programma e una serie di aspettative che la squadra deve soddisfare. Ogni progetto è unico e differisce dalle operazioni di routine, le attività in corso di un'organizzazione, perché i progetti raggiungono una conclusione una volta raggiunto l'obiettivo" (PMI, 2017).

I progetti sono rischiosi per natura intrinseca:

- sono unici;
- sono complessi;
- si basano su assunzioni;
- dipendono da molte variabili;
- comportano cambiamenti;
- si sviluppano su lunghi periodi;
- coinvolgono persone.

La definizione di rischio all'interno della gestione dei progetti è analoga alla definizione del rischio aziendale con la differenza che quest'ultimo è esteso agli obiettivi strategici aziendali.

L'attenzione all'applicazione delle pratiche del Project Management è aumentata notevolmente negli ultimi anni. Insieme a questa, nel tempo è iniziato ad incrementare anche l'interesse inerente alla qualità dei progetti e al rischio. Nella norma ISO 9000:2015 (International Standards Organization (ISO), 2015) si richiede di applicare un approccio basato sui rischi alla gestione della qualità. Ciò comporta l'adozione di una visione globale dei rischi dell'attività aziendale e coinvolge l'alta direzione nell'intero processo di mitigazione dei rischi.

Il risk-based thinking va molto al di là delle azioni preventive perché prevede l'analisi del contesto e dei processi per identificare i rischi, prenderne nota e programmare azioni volte ad eliminarli o a ridurre la probabilità che si verifichino o, eventualmente, l'impatto del loro accadimento.

2.1.1 Incertezza di progetto

I rischi di progetto, quindi, sono prevalentemente causati dall'incertezza che li caratterizza.

La portata dell'incertezza è considerevole in qualsiasi progetto e la maggior parte delle attività di gestione del progetto riguarda la gestione dell'incertezza dalla prima fase di "ideazione" alla fase finale di "supporto" del ciclo di vita del progetto. Rivedendo le fasi di progetto, abbiamo:

- Inizializzazione;
- Pianificazione;
- Approvvigionamento;
- Esecuzione;

- Monitoraggio e controllo;
- Chiusura.

Ogni fase è un progetto nel progetto, e il livello di incertezza, così come il livello di impegno, varia di fase in fase. In Fig.1 si può osservare il cono d'incertezza.

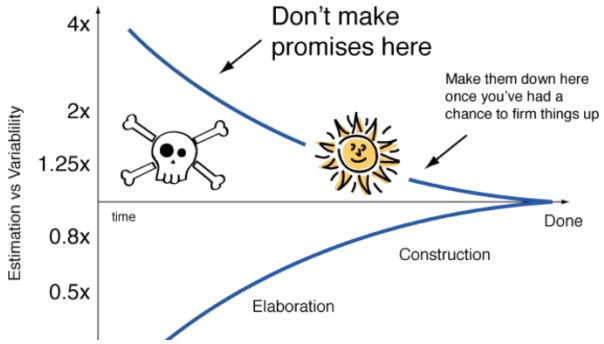

Figura 1 - Cono di incertezza

Nello stimare le cause del rischio si identificano cinque aree di incertezza principali (Chapman C. e Ward S, 2003):

- variabilità associata ai parametri di progetto;
- le ipotesi di base per stimare i parametri;
- Modelli e logiche applicate;
- obiettivi e priorità;
- le relazioni tra le varie parti del progetto.

2.1.1.1 Variabilità dei parametri di progetto

Una delle principali fonti di incertezza relative ai progetti è legata ai parametri del progetto cioè costi, tempi, qualità.

Le cause principali che possono causare questa incertezza sono:

- mancanza di una chiara specificazione di ciò che è richiesto;
- novità o mancanza di esperienza in una particolare attività;

- complessità in termini di numero di fattori di influenza e numero di interdipendenze tra questi;
- analisi limitata dei processi coinvolti nell'attività;
- possibile verificarsi di particolari eventi o condizioni che potrebbero avere qualche (incerto) effetto sull'attività.

2.1.1.2 Ipotesi sulla stima dei parametri

In assenza di un insieme di dati statistici sufficientemente esteso per determinare delle stime oggettive, risulta spesso necessario fare affidamento a stime soggettive delle probabilità di interesse. La qualità delle stime dipende da chi le ha prodotte, dal formato in cui vengono presentate, perché, come e quando sono state prodotte e su quali risorse ed esperienze si basano.

Una fonte di incertezza particolarmente importante è la natura delle ipotesi alla base delle stime. Tuttavia, le stime possono anche essere condizionate dal presunto non verificarsi di eventi di "forza maggiore" e da possibili cambiamenti nel contesto e nell'ambito del progetto. Gli effetti di tali eventi e cambiamenti possono essere difficili da quantificare, anche una volta identificati (Chapman C. e Ward S, 2003).

2.1.1.3 Modelli e logiche applicate

Nella fase di ideazione del progetto, la natura del deliverable finale di progetto e il processo per produrlo rappresentano le incertezze

fondamentali. In linea di principio, gran parte di questa incertezza viene rimossa nelle fasi di progettazione tentando di specificare cosa deve essere fatto, come, quando, da chi e a quale costo. In pratica, una parte significativa di questa incertezza può rimanere irrisolta. La natura delle ipotesi progettuali e logistiche e l'incertezza associata possono determinare parte dell'incertezze sulla base delle stime (Chapman C. e Ward S, 2003).

2.1.1.4 Obiettivi e priorità

L'obiettivo di migliorare le prestazioni del progetto presuppone chiarezza sugli obiettivi e sulle relative priorità tra il loro raggiungimento e la scelta di compromessi accettabili. Tentare la gestione del progetto o la gestione del rischio quando mancano queste assunzioni è impossibile. Le implicazioni relative alla natura degli obiettivi e alle priorità devono essere gestite tanto quanto l'incertezza su ciò che è realizzabile. È importante, perciò, stabilire obiettivi chiari e criteri di prestazione che riflettano i requisiti delle varie parti, comprese le parti interessate che non sono sempre riconosciute come attori (Morris P.W.G e Hough G.H, 1987).

2.1.1.5 Relazioni tra le parti di progetto

Una fonte importante di incertezza è la molteplicità di persone, unità aziendali e organizzazioni coinvolte in un progetto. I rapporti tra le varie parti possono essere complessi e possono comportare o meno contratti formali. Il coinvolgimento di più parti in un progetto introduce incertezza derivante dall'ambiguità in relazione a (Ward S., 1999):

- specificazione delle responsabilità;
- percezione di ruoli e responsabilità;
- comunicazione attraverso le interfacce;
- la capacità delle parti;
- condizioni dei contratti formali e loro effetti;
- meccanismi di coordinamento e controllo.

2.2 Project Risk Management

La gestione del rischio è importante nelle attività di routine dell'azienda, ma assume un ruolo primario nelle attività di cambiamento e/o innovazione, e cioè le attività di progetto.

Il risultato finale di una qualsiasi attività è composto da tre addendi: ciò che è stato pianificato, gli imprevisti accaduti e noti e i rischi, cioè eventi possibili, non pianificati e non accaduti, oppure accaduti ma non rilevati, non conosciuti o non compresi sufficientemente. I progetti devono essere gestiti in maniera che riescano a raggiungere gli obiettivi prefissati. È indispensabile, perciò, che questi ultimi siano identificati in maniera chiara e univoca, e che siano misurabili facilmente. Nonostante queste accortezze risulta molto complicato andare a misurare il successo di un progetto: bisogna considerare molti fattori differenti come il raggiungimento degli obiettivi, il tempo impiegato, il budget, la soddisfazione degli stakeholders e shareholders e le conseguenze sull'azienda.

Così come è difficile valutare il successo, anche il fallimento è complicato da valutare e spesso basta davvero poco per passare da un progetto di successo a un progetto fallimentare. La natura e la dimensione del progetto influenzano molto l'importanza e l'impatto della gestione dei rischi.

Si distinguono quindi il rischio di progetto dal rischio aziendale (enterprise risk), cioè quello esteso agli obiettivi della strategia aziendale. L'analisi dei rischi all'interno dei progetti dovrebbe essere integrata e proattiva, ma non risulta essere sempre così. In accordo con uno studio fatto dal PMI nel 2017, solo il 28% dei manager di progetto utilizza le pratiche di gestione del rischio in maniera regolare e sistematica. La gestione del rischio non deve rappresentare una fase appartenente alla gestione del progetto, ma deve essere presente, integrata e reiterata in ogni momento nel ciclo di vita del progetto e ad ogni scelta o cambiamento che viene effettuato. Infatti, essendo le fonti di rischio sia interne che esterne, e poiché sono elementi molto dinamici e spesso difficili da definire con certezza nel tempo e nello spazio, la natura dei rischi può variare: ne possono emergere di nuovi e possono modificarsi quelli già esistenti. Inoltre, poiché ogni progetto è differente, l'analisi dei rischi verrà effettuata con intensità e gradi differenti richiedendo un approccio sempre più agile e flessibile. Esistono delle pratiche comuni da adottare, ma è indispensabile che per ogni azienda, e spesso anche per ogni progetto, che venga svolto un adattamento in relazione alla natura e all'entità.

Il libro di riferimento che considereremo per le pratiche da adottare e seguire nella gestione del rischio di progetto sarà il PMBoK (PMI, 2017).

2.2.1 Rischi individuali e rischi globali

Il PMBoK classifica i rischi in due categorie:

- Rischi individuali di progetto: condizioni o eventi incerti, che se accadono hanno conseguenze positive o negative su uno o più

obiettivi di progetto. Rispondono alla domanda: quali sono i rischi del progetto?

- Rischi globali di progetto: l'effetto dell'incertezza sul progetto nella sua interezza, a partire da tutte le fonti di incertezza possibili, includendo i rischi individuali. Rappresentano l'esposizione degli stakeholders alle implicazioni delle variazioni nei risultati del progetto, sia positive che negative. Risponde alla domanda: quanto è rischioso il progetto?

Possiamo identificare perciò due livelli di rischio, uno inferiore relativo ai rischi individuali ed uno superiore relativo al rischio globale di progetto.

In generale il Project Manager è il responsabile delle singole fonti di incertezza sul progetto e si occupa di analizzare i rischi del progetto, mentre il Project Sponsor è il responsabile della rischiosità dell'intero progetto.

Il dualismo dei progetti sta nella differenziazione tra i "rischi di progetto" e il "rischio di progetto". Non si tratta solo di un formalismo semantico ma di due concetti che afferiscono a due differenti concezioni di rischio, che nascono e impattano su livelli differenti di progetto e richiedono approcci totalmente differenti.

L'errore più grande che si possa effettuare è quello di focalizzarsi solamente sui rischi individuali e credere che facendo così implicitamente si stia lavorando anche sul rischio globale di progetto. Il rischio globale di progetto non è ottenuto dalla somma lineare dei rischi individuali, ma essendo un rischio a sé stante, è necessario effettuare le stesse analisi effettuate sui rischi individuali, ponendo la giusta attenzione ai contributi dei singoli rischi, alle loro interazioni oltre che alle altre cause esterne.

Gestire il rischio significa agire su entrambi i livelli. Il rischio globale di progetto è un concetto univoco: ogni progetto ha un unico livello di rischio

globale, e questo varia al variare del tempo, in funzione di come vengono svolte le diverse fasi di progetto. Per approcciarsi al rischio globale di progetto al meglio è importante considerarlo a partire dalla fase di pianificazione, durante la quale vengono definiti lo scopo, la struttura e gli obiettivi del progetto. In questa fase lo sponsor definisce i benefici che vuole raggiungere e i limiti di tolleranza sulle deviazioni dagli obiettivi. In questa fase vengono coinvolti anche stakeholder e Project Manager.

2.2.2 Ruoli e responsabilità

Nel Project Team esistono molte figure differenti che agiscono su diversi livelli e modalità. Prima di analizzare questi ruoli nel contesto del PRM è importante dare delle definizioni perché spesso si crea confusione su tre figure principali:

- Project Sponsor: è una figura importante del progetto, si occupa di assicurare le risorse necessarie. Ha forte interesse nel progetto e ne è il referente presso la direzione aziendale, a cui risponde del suo successo o insuccesso. È la persona che determina l'avvio del progetto stesso. Può coincidere con il Project Owner o essere un rappresentante dell'azienda che ha l'autorità di prendere decisioni relative al progetto.
- Project Owner: colui che ha il pieno controllo sul progetto, è il responsabile della definizione degli obiettivi e della pianificazione e del soddisfacimento di questi nei tempi e costi prestabiliti. Può essere interno o esterno all'azienda.
- Project Manager: ha la responsabilità generale del progetto, della gestione del team e dei processi svolti.

All'interno del Project Team risulta indispensabile la figura del Project Risk Manager (PRM), responsabile dei processi di identificazione, valutazione e controllo delle minacce. Questa figura deve essere esperta e deve conoscere al meglio le tecniche consolidate del Project Risk Management, oltre che i processi interni alle fasi di progetto.

Il team di progetto racchiude diverse figure caratterizzate da diversi obiettivi e responsabilità. Il Project Risk Manager è la figura che si occupa di sviluppare una visione condivisa sul rischio: il Project Owner e il Project Manager, i quali hanno il ruolo decisionale, possono avere diverse attitudini che influenzeranno come i rischi verranno trattati.

In genere il Project Owner si focalizza sui rischi strategici mentre il Project Manager su quelli operativi. I rischi strategici riguardano gli effetti a lungo termine dovuti al progetto, mentre i rischi operativi sono i rischi correlati ai risultati diretti del progetto.

Il Project Risk Manager è il tramite tra queste due figure, esso garantisce una panoramica sui rischi e sulle opportunità di progetto nonché il loro piano di mitigazione facilitando i processi decisionali a livello direzionale. Il Project Risk Manager garantisce il rispetto dell'intero progetto facilitando la coordinazione e la comunicazione tra le diverse parti interessate.

Il Project Owner affianca il Project Risk Manager nella condivisione del rischio, fornendo informazioni tecniche e specifiche sui rischi e le opportunità, il Project Manager, invece, collabora con il Project Risk Manager definendo le migliori strategie nell'affrontare i rischi, avendo una conoscenza globale del processo stesso.

Il Project Risk Manager è affiancato dal Risk Owner, responsabile dei rischi, che ne subisce direttamente i danni e si occupa spesso di definire la strategia e i piani di azione. Il Risk Owner è "la persona responsabile del

monitoraggio del rischio e della selezione e implementazione di un'appropriata strategia di risposta al rischio" (Williamson B., 2019). In base al progetto, questa figura può coincidere con il PRM. Accanto a queste figure troviamo il team di esperti nella gestione del rischio e delle tecniche, supportati in genere da un team di analisti: è il gruppo che si occupa della gestione del progetto ed è interessato principalmente al raggiungimento degli obiettivi prefissati rimanendo nel budget e nel tempo stabilito (Turner J.R. e Müller R., 2004).

Il Project Management Office (PMO) supervisiona la gestione dei progetti all'interno di un'organizzazione.

Infine, gli stakeholder sono gli individui o le organizzazioni che hanno interesse diretto o indiretto nel risultato o in alcuni deliverables del progetto. Sono influenzati e influenzano a loro volta il progetto.

2.3 Processo di Project Risk Management

Come definito in precedenza, il processo di PRM è un susseguirsi razionale di attività che ha l'obiettivo di gestire i rischi di progetto in modo che questi non abbiano un impatto negativo e potenzialmente irrecuperabile sugli obiettivi. La natura complessa e l'unicità dei progetti hanno portato a una grande varietà di diverse definizioni e approcci al processo di Risk Management. I processi di gestione del rischio e le tecniche di supporto sono stati ampiamente sviluppati e implementati sia nella letteratura che nella pratica. La moltitudine di metodi richiede strumenti che suggeriscano in quali circostanze ciascuno di essi debba essere adottato. Tuttavia, questi criteri di solito non tengono conto né dell'insieme completo delle caratteristiche uniche del progetto e del suo contesto né

dell'atteggiamento di un'organizzazione nei confronti del rischio. Le Best Practices da adottare necessitano di un adattamento al progetto specifico, quindi alla sua complessità, al contesto, alla fase del progetto e al grado di maturità dell'azienda sul rischio (da Silva L.H.R., Crispim J.A, 2014).

Dagli anni '90 sono presenti differenti studi in letteratura mirati alla definizione di un processo di Project Risk Management.

Molte pratiche hanno strutture molto simili caratterizzate principalmente da tre macro-fasi:

- comprendere le caratteristiche e gli obiettivi del progetto e pianificare lo sforzo di gestione del rischio decidendone il livello, l'ambito e lo scopo;
- identificare i rischi, le loro cause, gli effetti e come si relazionano tra loro; valutare le probabilità di accadimento e gli impatti, stabilendo le priorità; elaborare strategie di risposta al rischio e stabilendo, infine, piani di emergenza;
- realizzare delle risposte al rischio, tramite il monitoraggio e controllo; identificare e valutare nuovi rischi emergenti, comunicare i risultati del processo di gestione del rischio e registrare tutte le conoscenze.

Altri, come ad esempio il processo di gestione del rischio sviluppato dal Project Management Institute (PMI, 2017) , includono solo attività relative all'identificazione del rischio, all'analisi qualitativa e quantitativa e alla risposta non presentando fasi volte a chiarire gli obiettivi del progetto o formalizzare le conoscenze acquisite durante la gestione del rischio. (Cagliano A.C., Grimaldi S. e Rafele C. , 2014)

2.3.1 Fasi del ciclo di vita del progetto

In ogni fase del ciclo di vita del progetto sono presenti differenti attività e obiettivi da raggiungere. In particolare, le fasi si differenziano tra loro per i diversi sforzi e impegni richiesti, le risorse e le informazioni possedute.

Le attività di gestione del rischio possono essere associate a ciascuna fase del ciclo di vita di un progetto (Chapman C. e Ward S, 2003).

L'identificazione delle fonti di incertezza avviene nella fase di pianificazione, la gestione dei rischi previsti e il monitoraggio dei cambiamenti nel profilo di rischio sono tipici della fase di esecuzione. Il grado di accuratezza delle informazioni è eterogeneo lungo il ciclo di vita del progetto. Inizialmente, il livello scarso di informazioni rende difficile valutare la probabilità di accadimento del rischio. Al contrario, nelle fasi successive, quando i rischi sono principalmente legati alle conseguenze delle decisioni prese nelle fasi precedenti del progetto o sono gli effetti di rischi già manifestati, le loro fonti, accadimento e impatti possono essere caratterizzati in modo più accurato grazie al maggior numero di informazioni disponibili.

In ogni fase di progetto è necessario tenere presente tutte queste considerazioni e adattare di conseguenza il processo di Project Risk Management. Inoltre, una visione orientata al ciclo di vita del progetto delle tecniche di gestione del rischio aiuta ad evitare la compartimentazione che si verifica quando ogni partecipante affronta i rischi con una prospettiva basata esclusivamente sui propri obiettivi, indipendentemente dalle altre parti del progetto e del ciclo di vita del progetto. (Cagliano A.C., Grimaldi S. e Rafele C. , 2014)

2.3.2 Grado di maturità dell'azienda

La maturità verso il rischio rappresenta la consapevolezza e la comprensione che la gestione del rischio è allo stesso livello delle attività operative, strategiche e gestionali. Non tutte le organizzazioni devono raggiungere il massimo livello di maturità riguardo l'analisi dei rischi, anche se i livelli più bassi dovrebbero essere presto abbandonati a favore di metodi che seguano principi riconosciuti e forniscano al management informazioni fruibili sul rischio del progetto che contribuiscano ad un buon processo decisionale.

I livelli più bassi di analisi del rischio possono essere implementati senza strumenti e formazione specializzati, sebbene esistano strumenti software che possono aiutare l'applicazione, ad esempio, dell'analisi qualitativa del rischio (Hulett D. T, 2001). Una scarsa consapevolezza nei confronti del rischio spinge ad applicazioni occasionali di tecniche informali di gestione del rischio a progetti specifici. In questi casi i problemi vengono erroneamente affrontati dopo il loro verificarsi. Comprendere la rilevanza del rischio, invece, consente di gestire in modo proattivo l'incertezza. Il grado di maturità nei confronti del rischio di un'organizzazione dipende dalla sua cultura del rischio, stimolata dal contesto informativo disponibile e dalla tipologia e dimensione dell'organizzazione stessa.

In letteratura esistono diversi modelli per valutare la maturità del rischio. Uno dei primi modelli è stato definito da Hillson (Hillson D., 1997) che propone quattro stadi, associati a loro volta a quattro attributi: cultura, processo, esperienza e applicazione:

- ingenuo: un'organizzazione non sente la necessità di gestire il rischio e non utilizza approcci strutturati nella gestione dell'incertezza;

- novizio: definisce un'organizzazione che riconosce i vantaggi della gestione del rischio e sta implementando una qualche forma di governance del rischio, ma manca di un processo formalizzato per svolgere questo compito;
- normalizzato: è il grado di maturità caratterizzato da un processo di rischio formalizzato incluso nelle attività aziendali di routine i cui benefici, tuttavia, non sono costantemente raggiunti in ogni progetto;
- naturale: un'organizzazione completamente consapevole del rischio e che gestisce in modo proattivo opportunità e minacce attraverso informazioni coerenti sui rischi.

Partendo da questa base, da altre analisi effettuate in letteratura, e dalla descrizione del processo di Project Risk Management definito dalla ISO 31000, si è ulteriormente sviluppato un suo modello di maturità su 5 livelli. (Proença D., Estevens J., Vieira R. e Borbinha J., 2017).

I livelli sono:

- Livello 0: Risk Management non esistente;
- Livello 1: Risk Management Iniziale;
- Livello 2: Risk Management Gestito;
- Livello 3: Risk Management Definito;
- Livello 4: Risk Management Gestito Quantitativamente;
- Livello 5: Risk Management Ottimizzato.

Le organizzazioni possono passare da un livello all'altro, ma per fare ciò è indispensabile la consapevolezza del loro livello e devono soddisfare tutti i criteri del livello in cui si trovano. La consapevolezza serve non solo a definire i passi necessari a un possibile passaggio di livello, ma è utile per

adattare in maniera corretta il processo di gestione dei rischi, definendo attività e tecniche in linea con il grado di maturità dei rischi dell'azienda.

Un elevato livello di consapevolezza dei rischi unitamente ad un'adeguata disponibilità di conoscenze consente di ottenere le informazioni oggettive che consentono la quantificazione del rischio. Sulla base di ciò, si può affermare che più un'organizzazione è matura nei confronti del rischio, più saranno le fasi del processo di gestione del rischio che implementerà. Le aziende con un basso grado di maturità eseguono solo l'identificazione del rischio o l'analisi qualitativa del rischio, mentre le organizzazioni con un alto livello di maturità si occupano di tutte le fasi del processo di gestione del rischio.

2.3.3 Fasi del Project Risk Management

Si prende come riferimento il framework adottato dal PMI. Il PMBoK identifica sette fasi principali nel processo di gestione del rischio:

- Pianificazione;
- Identificazione;
- Analisi qualitativa dei rischi;
- Analisi quantitativa dei rischi;
- Definizione del piano di risposta dei rischi;
- Implementazione delle risposte;
- Monitoraggio e controllo dei rischi.

2.3.3.1 Pianificazione

La pianificazione è la fase in cui si analizza il contesto del progetto, i suoi confini, gli obiettivi, le risorse, i vincoli e si definiscono le modalità di conduzione delle attività di gestione del rischio e le strategie. Ci si assicura che ci sia una coerenza tra l'impegno in termini di tempo e risorse e l'effettiva importanza del progetto a livello strategico, economico e di rischio intrinseco (il quale dipende dalla complessità, dal grado di innovazione, dal contesto e da tutte le caratteristiche che fungono da condizioni iniziali note). È molto importante coinvolgere gli stakeholders di progetto in modo da poter sfruttare a beneficio del progetto le loro conoscenze ed expertise e, inoltre, per allinearli da subito al processo di PRM.

Il piano finale, oltre che alla metodologia e strategia, contiene l'assegnazione dei ruoli e delle responsabilità, le tolleranze al rischio degli stakeholder, lo scheduling delle attività di Risk Management e definisce le categorie di rischio attraverso una Risk Breakdown Structure (RBS). La RBS è una rappresentazione gerarchica dei rischi di progetto identificati organizzata in categorie e sottocategorie che identificano le varie aree e cause dei rischi (PMI, 2009).

2.3.3.2 Identificazione

In questa fase l'obiettivo è creare una lista completa e dettagliata dei rischi (Registro dei Rischi o Risk Register) che possono interferire con il raggiungimento degli obiettivi del progetto. Il Risk Register non contiene solo i rischi individuati ma anche le loro caratteristiche, le aree di impatto, i responsabili e le azioni di mitigazione. Questa fase è effettuata analizzando

i dati storici, se sono presenti progetti simili, facendo benchmarking, consultando il Project Manager, lo sponsor e gli stakeholders. In alcuni casi è presente un compilatore automatico che analizza, compara e pulisce il database dei rischi. Questa fase è molto importante poiché è la base delle fasi successive di gestione del rischio. È necessario quindi non solo analizzare i possibili rischi futuri ma definire anche i rischi emergenti e quelli residui. Infatti, i rischi individuati in un certo istante di tempo possono scostarsi molto da quelli individuati in un'altra fase del progetto, in base ai cambiamenti del contesto. Questa fase, perciò, deve essere aggiornata continuamente. Il Risk Register è un documento comprensivo di tutte le informazioni associate ad ogni rischio e per questo motivo è importante sottolineare che la compilazione a valle dell'identificazione sarà molto diversa dal Register finale compilato e aggiornato a valle del monitoraggio e controllo.

2.3.3.3 Analisi qualitativa

È il processo in cui vengono priorizzati i rischi. Per farlo si usano, nella maggior parte dei casi, criteri relativi alla probabilità di avvenimento e alle conseguenze dell'accadimento. In particolare, si studiano e analizzano i rischi individuali di progetto. Il metodo utilizzato più comunemente è quello della costruzione della matrice di probabilità/impatto, che associa diversi livelli di peso (solitamente sono: basso, medio alto), sia alla probabilità di accadimento dell'evento, che all'impatto di questo sugli obiettivi. Il problema principale di queste stime è dato dalla complessità di valutare in maniera oggettiva sia la quantificazione del danno, che il valore della probabilità di accadimento.

Considerando che non è possibile, o è molto difficile, comparare danni di natura differente, è necessario andare a valutare tre caratteristiche principali sulla base delle quali poi valutare l'entità del danno stesso:

- La natura;
- L'estensione (severità e distribuzione);
- La tempistica (frequenza e distanza);

Nonostante queste considerazioni risulta comunque molto difficile valutare l'entità del danno in maniera oggettiva, poiché ognuno valuta la gravità di un evento in base alla propria percezione.

Il PMI presenta una serie di fattori che possono aiutare nello svolgimento dell'analisi qualitativa. Questi sono, in una piramide che va dal generale al particolare, un approccio concordato nella valutazione dei rischi, delle definizioni concordate riguardo i termini legati al rischio, la collezione di informazioni di alta qualità riguardo i rischi e l'iterazione dell'analisi qualitativa. (PMI, 2009)

Per quanto riguarda gli aspetti numerici si può dire che: la probabilità può riferirsi alla probabilità di un evento o di una conseguenza e può essere definita in vari modi (probabilità attesa, frequenza, in termini descrittivi) e anche essa è soggetta ad incertezza, mentre, la stima può variare in base al contesto, ai modelli di probabilità definiti, ai pregiudizi. (ISO 31010:2019)

2.3.3.4 Analisi quantitativa

L'obiettivo dell'analisi quantitativa è di valutare l'impatto del rischio sul progetto in termini di tempo, costo e qualità.

Si possono distinguere le analisi semi-quantitative e le analisi quantitative.

L'analisi semi quantitativa dei rischi fornisce un livello intermedio di valutazione tra quello descrittivo dall'analisi qualitativa e quello numerico dell'analisi quantitativa per mezzo di una stima a punteggio. Questa si svolge prima assegnando un indice alla probabilità ed uno all' impatto, poi moltiplicandoli tra loro; l'output di tale analisi è quindi un punteggio per ciascun rischio che ne identifica in maniera univoca la gravità rispetto ad un altro. L'analisi semi-quantitativa offre un approccio più consistente e rigoroso nella comparazione dei rischi rispetto all'analisi qualitativa ed evita alcune delle ambiguità che tale analisi può generare. Non necessita delle stesse abilità matematiche dell'analisi quantitativa né della stessa quantità di dati. Per questi motivi può essere applicata in caso mancassero dati puntuali. Tramite l'analisi qualitativa sono stati individuati i rischi sui quali è opportuno effettuare un approfondimento, tale approfondimento viene eseguito attraverso l'analisi quantitativa.

Si tratta di un processo che cerca di quantificare la conseguenza che un determinato evento avrebbe sul progetto, in modo da poterlo gestire nella maniera più opportuna.

Il PMBoK definisce l'analisi quantitativa come: "Il processo di quantificazione numerica dell'effetto combinato dei singoli rischi od altre sorgenti di incertezza sugli obiettivi di progetto".

In questo processo si utilizzano comunque i concetti di probabilità ed impatto ma essi sono stimati in maniera differente dall'analisi qualitativa, in particolare:

- La probabilità di accadimento è stimata utilizzando i dati storici;
- L'impatto è dato dall'effettiva perdita che si avrebbe se l'evento preso in considerazione si verificasse, tale perdita è misurata con un parametro relativo al progetto. (e.g. costo, tempo, qualità, ecc.).

I metodi statistici sono ampiamente utilizzati in questo tipo di analisi ed è necessaria la conoscenza delle distribuzioni di probabilità associate ai diversi fattori del modello. Sono utilizzate distribuzioni continue per rappresentare l'incertezza nelle componenti di durata delle attività o costo, e distribuzioni discrete per l'esito di un test o per un possibile scenario in un albero decisionale.

L'output di un'analisi quantitativa serve quindi per individuare le azioni di risposta al rischio più corrette ed essa dovrebbe essere ripetuta dopo la pianificazione delle stesse e insieme al monitoraggio, in modo da determinare se il rischio totale di progetto si sia sufficientemente abbassato.

Sono utilizzati differenti metodi e tecniche a supporto di questa analisi, come il metodo SWOT, l'analisi di sensibilità, l'albero delle decisioni e il metodo Monte Carlo.

2.3.3.5 Definizione piano risposta rischi

Sulla base delle analisi effettuate in precedenza e sulla propensione al rischio, vengono definiti dei piani di risposta che prevedono principalmente il perseguimento di una o più delle seguenti azioni:

- Avoid: nel caso in cui il livello di rischio del progetto è sfavorevole e al di fuori delle soglie definite per il progetto, evitare il rischio potrebbe essere la soluzione migliore. Evitare il rischio significa eliminare alla radice le fonti di incertezza che ne aumentano l'impatto. Svolgere azioni di questo tipo implica un grande sforzo in termini di costo e di tempo e vanno perseguite nel caso in cui "rischiare" di uscire dalle soglie definite avrebbe conseguenze irreparabili per il progetto o per l'impresa che lo sta svolgendo.
- Exploit: se il rischio di progetto è favorevole, significa che il rischio può avere un impatto positivo per il progetto, diventando un'opportunità e sfruttarlo sarà ideale. Si potrebbero aggiungere nuovi benefici per gli stakeholder chiave o aumentare le soglie per poter sfruttare l'opportunità sopraggiunta in toto.
- Transfer/Share: nel caso in cui il rischio di progetto è elevato ma non si hanno le risorse per gestirlo internamente può essere conveniente farlo gestire a terzi. La gestione del rischio si può svolgere tramite collaborazioni tra imprese oppure con semplici "premi" al delegato dal delegante.
- Mitigate/Enhance: mitigare il rischio di progetto sarà sensato nel momento in cui non c'è bisogno di evitare completamente il rischio né di sfruttarlo a proprio vantaggio. Si svolgono operazioni di mitigazione quando il rischio di progetto è vicino ad una soglia accettabile, andando a modificare le attività direttamente correlate a

questo o a singoli rischi ad alta priorità. È la strategia maggiormente applicata nel PRM perché non implica modifiche allo scope di progetto né modifiche troppo stringenti alle attività già pianificate.

- Accept: Nel caso in cui nessuna nelle precedenti alternative dovesse essere perseguibile, sia per motivi incontrollabili perché endogeni o perché il progetto ha un rischio associato molto basso si può accettare il rischio così com'è. Per far questo si potrà associare una Contingency Reserve all'intero progetto.

2.3.3.6 Implementazione

La fase di implementazione è direttamente collegata alla precedente. Consiste specificatamente al momento in cui, se ce ne dovesse essere bisogno, vengono implementati i piani di risposta ai rischi. Risulta molto importante il rispetto del piano e la comunicazione della decisione di implementazione di quest'ultimo. Nella fase successiva verranno valutati i risultati.

2.3.3.7 Monitoraggio e Controllo

Gli obiettivi primari della fase di monitoraggio e controllo sono: il tracciamento dei rischi identificati, il monitoraggio del rischio residuo, l'identificazione di nuovi rischi, l'assicurazione che le risposte ai rischi vengano eseguite nel momento giusto e la valutazione che queste siano efficaci lungo tutto il ciclo di vita del progetto.

Durante questa fase prende importanza l'aspetto comunicativo del PRM, i Risk Owner e gli altri responsabili devono essere sempre aggiornati che dei cambiamenti possono modificare le loro responsabilità. Questo vale sia nel caso un rischio non si dovesse presentare, con "l'eliminazione" della responsabilità sia nel caso in cui dovessero attivarsi dei rischi e si dovessero svolgere studi aggiuntivi per l'analisi degli impatti e degli eventi scatenanti.

Alla fine del processo di monitoraggio e controllo è consigliato valutare l'intero processo di PRM per identificare migliorie ed eliminare aspetti che si sono rilevati di poca efficacia, rimanendo sempre consci del fatto che ogni progetto e unico.

2.3.4 Un'ulteriore fase: gestione della conoscenza del rischio

Un'altra fase sta acquisendo importanza nella gestione del rischio, vale a dire il processo di gestione della conoscenza.

Al giorno d'oggi, creare, mantenere, trasferire e aumentare la conoscenza sono di fondamentale importanza per affrontare in modo efficiente la complessità dei progetti. Ciò è ancora più rilevante quando si affrontano i rischi a causa dell'elevata variabilità e delle scarse informazioni disponibili. (Cagliano A.C., Grimaldi S. e Rafele C. , 2014)

I progetti sono spesso creano disconnessioni informative, portando così a una comunicazione molto scarsa sul rischio, proprio come accade in molti altri campi e settori.

Al fine di supportare un'efficace gestione del rischio, il processo di gestione della conoscenza dovrebbe andare oltre la raccolta e la strutturazione delle informazioni. Questo processo dovrebbe orientare la

scelta delle tecniche da applicare nei diversi contesti in funzione sia del progetto stesso che della maturità verso il rischio dell'impresa che lo realizza, che è a sua volta funzione della quantità di informazioni disponibili. Inoltre, è necessario che ci sia un continuo aggiornamento e studio sulla conoscenza del rischio.

2.4 Tecniche di Risk Assessment

Ogni processo di gestione del rischio richiede l'applicazione di specifici strumenti scelta dai Risk Team, in funzione di possibilità, bisogno, contesto e progetto. Sono state definite una grande varietà di tecniche e strumenti in letteratura. Il testo di riferimento che useremo nel definire le tecniche di risk assessment sarà l'IEC 31010 (International Standards Organization (ISO), 2019), come mostrato in Figura 5.

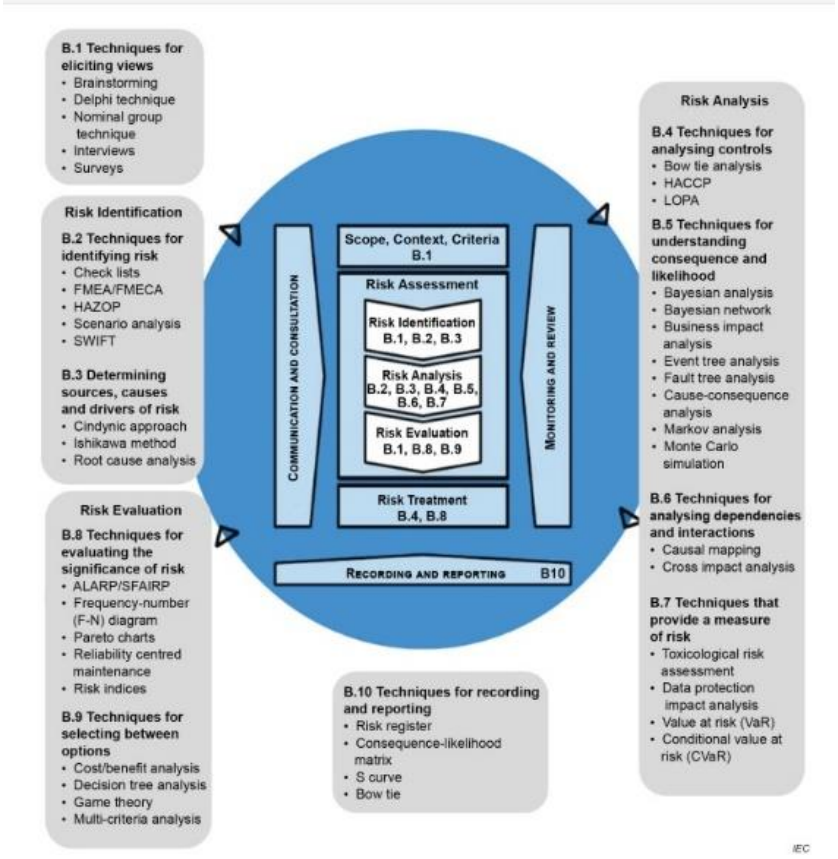

Figura 2 - Applicazione delle tecniche nel processo di Risk Management

In termini generali, le tecniche appropriate devono presentare le seguenti caratteristiche:

- devono essere giustificabili e adeguate alla situazione o all'organizzazione in esame;
- dovrebbero fornire risultati in una forma che aumenta la comprensione della natura del rischio e del suo trattamento;
- dovrebbero poter essere utilizzate in modo che siano tracciabili, ripetibili e verificabili.

Le ragioni per la scelta delle tecniche sono in funzione della loro pertinenza e idoneità. Questo vale perché, ad esempio, quando si integrano i risultati di diversi studi, le tecniche utilizzate e i risultati devono essere comparabili.

Le tecniche dovrebbero essere selezionate, basandosi su fattori quali:

- Gli obiettivi dello studio;
- L'importanza delle decisioni da prendere;
- Il tipo e la gamma dei rischi da analizzare;
- La potenziale grandezza delle conseguenze;
- Il livello di competenza, le risorse umane e le altre risorse necessarie;
- Dati e informazioni da ottenere;
- La necessità di modificare/aggiornare la valutazione dei rischi (alcune tecniche sono più modificabili di altre);
- Requisiti regolamentari e contrattuali.

Vari fattori influenzano la scelta di un approccio alla valutazione del rischio come la disponibilità di risorse, natura e grado di incertezza nei dati e nelle informazioni disponibili e la complessità dell'applicazione (International Standards Organization (ISO), 2019). Un criterio

comunemente utilizzato si basa sulla natura delle informazioni disponibili. Le tecniche qualitative richiedono molte informazioni e presentano i risultati sotto forma di descrizioni e raccomandazioni, mentre le tecniche quantitative si basano su dati numerici e statistici e analizzano il verificarsi e gli effetti dei rischi. Nessuna tecnica di gestione del rischio si adatta ad ogni fase del processo di gestione del rischio, ma ciascuna dà i suoi migliori risultati se applicata a una o poche fasi. Il passaggio da una fase del ciclo di vita del progetto a un'altra implica la disponibilità di informazioni più dettagliate e quantitative, portando a un diverso grado di incertezza. Pertanto, il focus di qualsiasi analisi del rischio e delle tecniche di gestione del rischio adottate deve variare con le fasi del ciclo di vita del progetto. Ad esempio, nella fase iniziale di identificazione avremo meno informazioni rispetto che nelle fasi successive.

In base alla maturità dell'azienda le tecniche possono essere suddivise in tecniche di base, che non richiedono competenze particolari, (brainstorming), tecniche intermedie usate in aziende con una certa esperienza nella gestione del rischio, e tecniche più avanzate, come l'analisi Monte Carlo.

2.4.1 Incognite del sistema

Le discussioni relativamente recenti sul concetto fondamentale di "rischio" e altre questioni relative alla sua analisi hanno sottolineato e rafforzato la comprensione comune che il risultato della valutazione del rischio è condizionato dalle conoscenze disponibili sul sistema e/o processo oggetto di analisi. Riconoscerlo porta ad accettare l'inevitabile esistenza di

un rischio residuo legato alle incognite del sistema e/o delle caratteristiche e dei comportamenti del processo (Aven T., 2012).

Di conseguenza, gli eventi e gli scenari in un modello di valutazione del rischio sono stati classificati in base alle conoscenze disponibili al momento della valutazione (Flage R., Aven T. , 2015):

1. Unknown-unknown: situazioni in cui non si è consapevoli di non sapere;
2. Unknown-known: situazioni in cui non si è consapevoli di ciò che si conosce;
3. Known-unknown: situazioni in cui si sa che si hanno delle lacune informative;
4. Known-known: conoscenze conosciute, si ha la consapevolezza di sapere.

Secondo Flage e Aven, gli eventi e gli scenari appartenenti a 1–2 e 4 sono dei "cigni neri", cioè eventi considerabili come outliers[10], quindi con irrisoria probabilità di accadimento con un impatto estremo, i quali si possono spiegare e comprendere dopo il loro accadimento, rendendoli prevedibili. La categoria known-unknown è rappresentativa dei rischi emergenti, cioè, rischi nuovi o rischi noti che, tuttavia, diventano evidenti in condizioni nuove o non familiari.

Da quanto sopra si può ritenere che la valutazione del rischio costituisca uno sforzo sistematico e strutturato per organizzare le conoscenze disponibili su eventi, processi e scenari che incidono su specifiche decisioni da prendere per la gestione del rischio. Per il processo decisionale, la valutazione del rischio deve fornire informazioni tracciabili per argomentare le decisioni; i risultati della valutazione del rischio devono

[10] In statistica si intende come 'outlier' un'osservazione lontana dal grosso dei dati.

essere comunicati in modo da consentire ai decisori di interpretarli correttamente per i loro scopi e di comprendere l'incertezza associata relativa alle conoscenze disponibili utilizzate per la valutazione. La valutazione del rischio fornisce il quadro per organizzare le conoscenze disponibili sul sistema di interesse, con l'obiettivo di comprendere come il sistema può fallire e dare priorità alle modalità di fallimento in modo che possano essere prese buone decisioni.

Quando viene eseguita una valutazione dei rischi per fornire una serie di informazioni, ci deve essere un modo per dire che è stata eseguita con tecniche adeguate e conoscenze sufficienti. Il controllo della qualità di una valutazione del rischio è essenziale, poiché l'opposizione a una particolare decisione spesso è legata ad un giudizio sulla validità della valutazione del rischio, più che sul valore o significato. (Apostolakis G.E , 2004).

2.4.2 L'assessment nelle fasi del progetto

Durante il ciclo di vita del progetto e in ogni fase del processo di gestione del rischio, la natura e la quantità delle informazioni disponibili determinano quali tecniche dovrebbero essere applicate. Nel fare questa analisi ci si baserà principalmente sull'articolo "Choosing project risk management techniques: a theoretical framework" (Cagliano A.C., Grimaldi S. e Rafele C. , 2014)

Nella fase iniziale di identificazione non sempre sono disponibili tutte le informazioni necessarie per un'analisi completa del rischio. Tale situazione richiede la costruzione di un quadro sistematico per ottenere giudizi soggettivi dagli esperti in modo chiaro e diretto. Le tecniche usate principalmente in questa fase avranno l'obiettivo di acquisire informazioni.

Si utilizzano interviste, il brainstorming, la tecnica Delphi e il giudizio di esperti. A valle dello svolgimento di una o più tecniche citate sarà possibile effettuare anche un'analisi dei punti di forza e di debolezza del progetto. L'analisi SWOT[11] si può considerare la tecnica che si usa a completamento della fase di identificazione. Nel caso di progetti ripetitivi, la maggiore disponibilità di informazioni consente l'utilizzo di tabelle dettagliate come la Failure Mode and Effects Analysis (FMEA) che consente di definire probabilità di accadimento e impatti economici e/o temporali per ogni evento alternativo. In questa situazione, si potrebbe passare a un'analisi quantitativa dei rischi attraverso l'uso di tabelle FMECA (Failment Mode and Effects Criticality Analysis), alberi decisionali e la Event Tree Analysis (ETA). In ogni caso, la quantità e il tipo di informazioni presenti in questa fase consentono una buona identificazione del rischio ma difficilmente riescono a soddisfare i requisiti della fase di valutazione/analisi.

I modi e i mezzi per raggiungere gli obiettivi del progetto diventano più chiari successivamente. Infatti, l'aumento delle informazioni disponibili, consente una più approfondita indagine dei rischi che avverrà quando il progetto sarà in fase esecutiva.

Ci si concentra sulla classificazione e prioritizzazione dei rischi individuati nella fase precedente, utilizzando strumenti che si affidano a informazioni qualitative ma anche quantitative. In base alla maturità dell'azienda si possono usare tecniche più o meno sofisticate andando ad analizzare non solo i rischi individualmente ma valutando anche le loro relazioni e interdipendenze (Analisi Bayesiana, Analisi di Markov etc.).

[11] Streghts-Weaknesses-Opportunities-Threats

La fase finale è quella di monitoraggio ma anche di report e record dei rischi. Nei prossimi paragrafi, verranno presentate singolarmente alcune tecniche di valutazione del rischio.

2.4.3 Tecniche di Valutazione del rischio

La valutazione dei rischi avviene successivamente all'identificazione ed ha l'obiettivo di fornire informazioni sugli specifici rischi, in modo da poter classificarli, prioritizzarli e aiutare nelle decisioni di gestione/mitigazione. Le fasi successive all'identificazione sono: l'analisi qualitativa, l'analisi semi-quantitativa e l'analisi quantitativa. Prima di presentare alcune delle tecniche usate in queste fasi bisogna soffermarci sul rischio dal punto di vista analitico. Il rischio viene sempre definito in funzione della probabilità di accadimento e della magnitudo o impatto relativi ad esso.

La norma ISO 31000 definisce la probabilità di accadimento del rischio come: la parola "probabilità" è usata per fare riferimento alla possibilità che qualcosa accada, che sia definito, misurato o determinato oggettivamente o soggettivamente, qualitativamente o quantitativamente e descritta usando termini generali o matematici.

Per quanto riguarda l'impatto, che la norma definisce "conseguenza", viene definito come "risultato di un evento che impatta sugli obiettivi" alla quale si aggiunge il concetto che una conseguenza può essere certa o incerta, può avere un effetto negativo o positivo il quale può essere diretto o indiretto sugli obiettivi. (ISO, 2018)

2.4.3.1 Analisi qualitativa

Nella fase di analisi qualitativa si svolgono principalmente l'analisi di diverse caratteristiche:

- Gravità del danno;
- Probabilità che tale danno si verifichi, che è funzione di: esposizione al pericolo; accadimento di un evento pericoloso; possibilità tecniche ed umane per limitare o evitare il danno.

Considerando la grande difficoltà nel comparare danni di natura differente, è necessario valutare tre caratteristiche principali sulla base delle quali risulterà più semplice identificare il danno associato alla realizzazione dell'evento rischioso:

- La natura;
- L'estensione (severità e distribuzione);
- La tempistica (frequenza e distanza).

2.4.3.1.1 Failure modes, effects and criticality analysis (FMECA)

Questa metodologia consente di analizzare sistemi complessi e processi scomponendoli in elementi più semplici. Per ogni elemento semplice l'obiettivo è analizzare come può fallire, le cause e gli effetti. Si definiscono:

- Componenti e sistemi impiegati;
- Modi di guasto dei componenti e sistemi;
- Effetti dei diversi modi di guasto;
- Classificazione che dà una valutazione dei guasti in base alla criticità.

L'output di questa analisi è una matrice le cui dimensioni sono la probabilità di impatto e le conseguenze.

2.4.3.1.2 Hazard and operability (HAZOP)

Analogamente alla FMECA, la tecnica HAZOP consente di evidenziare come un sistema potrebbe non rispettare il comportamento previsto. L'analisi viene svolta da un team di esperti, caratterizzati da diverse abilità. Il successo dell'applicazione è molto legato alle conoscenze tecniche possedute dal team e dall'accuratezza dei dati. I termini caratteristici di questa analisi sono:

- I nodi, cioè i parametri di processo fondamentali per capire eventuali malfunzionamenti;
- Intenzioni, cioè finalità teoriche che dovrebbe perseguire il sistema;
- Deviazioni, variazioni dai parametri caratteristici;
- Cause, ciò che induce gli scostamenti;
- Conseguenze, effetti delle deviazioni;
- Parole guida, termini usati per evidenziare le situazioni in modo efficace.

2.4.3.2 Analisi semi quantitativa

L'analisi semi quantitativa è uno strumento ibrido tra i metodi qualitativi e quantitativi. In genere l'output è composto da grafici che contengono all'interno matrici o sistemi di punteggio per gli elementi di rischio.

Lo standard MIL-STD-882c (Departement of Defense, 1993) individua un insieme di requisiti per la realizzazione di un programma di sicurezza (System Safety Program) con l'obiettivo di fornire specifiche progettuali e strumenti di controllo operativo, in grado di eliminare i pericoli individuati o, comunque, ridurre il rischio a livelli accettabili. La norma propone anche una metodologia semi-quantitativa per l'identificazione e la valutazione dei pericoli associati ad un generico sistema. Ad oggi, è lo schema maggiormente utilizzato, anche in forme "personalizzate" dall'utilizzatore, in cui vengono di volta in volta modificate le scale di probabilità e gravità. Gli output di questa metodologia sono:

- la matrice di rischio (Hazard Assessment Matrix),
- e un indice di rischio (Hazard Risk Index o HRI) attraverso il quale è possibile individuare le condizioni di maggior criticità per dare priorità agli interventi correttivi.

2.4.3.3 Analisi quantitativa

I metodi statistici sono ampiamente utilizzati in questo tipo di analisi ed è necessaria la conoscenza delle distribuzioni di probabilità associate ai diversi fattori del modello. Sono utilizzate distribuzioni continue per rappresentare l'incertezza nelle componenti di durata o costo e distribuzioni discrete per l'esito di un test o per un possibile scenario in un albero decisionale.

L'output di un'analisi quantitativa serve quindi per aiutare l'individuazione delle azioni di risposta al rischio più corrette. L'analisi dovrebbe essere ripetuta dopo la pianificazione delle stesse e insieme al

monitoraggio, in modo da determinare se il rischio totale di progetto si sia sufficientemente abbassato.

Sono utilizzate differenti metodi e tecniche a supporto di questa analisi, come il metodo SWOT, l'analisi di sensibilità, l'albero delle decisioni e il metodo Monte Carlo.

2.4.3.3.1 Metodo SWOT

L'analisi SWOT è uno strumento di pianificazione strategica semplice ed efficace che serve ad evidenziare le caratteristiche di un progetto, di un programma, di un'organizzazione e le conseguenti relazioni con l'ambiente operativo nel quale si colloca, offrendo un quadro di riferimento per la definizione di orientamenti strategici finalizzati al raggiungimento di un obiettivo.

L'analisi SWOT consente di ragionare rispetto all'obiettivo che si vuole raggiungere tenendo simultaneamente conto delle variabili sia interne che esterne. Le variabili interne sono quelle che fanno parte del sistema e sulle quali è possibile intervenire; quelle esterne invece, non dipendendo dall'organizzazione, possono solo essere tenute sotto controllo, in modo di sfruttare i fattori positivi e limitare i fattori che invece rischiano di compromettere il raggiungimento degli obiettivi prefissati.

La SWOT Analysis si costruisce tramite una matrice divisa in quattro campi nei quali si hanno:

- I punti di forza (Strengths);
- I punti di debolezza (Weaknesses);
- Le opportunità (Opportunities);
- Le minacce (Threats).

La buona riuscita dell'analisi dipende dalla capacità di individuare in modo approfondito tutti i fattori coinvolti e dalla possibilità di realizzare un'efficace lettura incrociata.

Fondamentale, inoltre, per questo tipo di analisi è circoscrivere l'oggetto e avere ben chiaro il proprio obiettivo, altrimenti l'analisi risulterà generica e di conseguenza inefficace.

2.4.3.3.2 Analisi dell'albero dei guasti

L'albero dei guasti è una metodologia, usata nello studio dei sistemi, che consente di evidenziare, in modo quantitativo, i rapporti esistenti tra gli eventi, a partire dagli eventi scatenanti fino ad arrivare a quelli intermedi.

Lo studio prende avvio dall'individuazione dell'evento accidentale (top event), e livello dopo livello secondo un approccio top-down, si attraversano gli eventi intermedi fino ad arrivare a quelli base. In questa analisi si può intervenire con gli strumenti di calcolo per individuare la soluzione a tutto il problema, valutando la probabilità di accadimento del top event a partire da parametri probabilistici associati ai singoli eventi della catena (International Standards Organization (ISO), 2019).

2.4.3.3.3 Analisi Monte Carlo

L'analisi Monte Carlo è un metodo basato su procedimenti probabilistici che prevede la simulazione probabilistica di fenomeni fisici attraverso la generazione di valori casuali da una nota distribuzione di probabilità. È utilizzato per stimare risultati di eventi incerti, su problemi che non

potrebbero essere risolti per via analitica. A differenza di un normale modello di previsione la simulazione Monte Carlo prevede una serie di risultati sula base di un intervallo di valori stimato invece che su input fissi. Crea un modello di possibili risultati sfruttando una distribuzione di probabilità come una distribuzione normale o uniforme, per qualsiasi variabile che abbia un'incertezza intrinseca. Si calcolano i risultati in modo iterativo cambiando ogni volta la serie di numeri casuali compresi tra il minimo e il massimo. Nell'utilizzo di questo metodo è richiesto un elevato numero di input per avere una maggiore precisione.

Il più grande limite di questo tipo di analisi è tuttavia la bontà del modello utilizzato: un modello non corretto o non sufficientemente dettagliato conduce ad esiti dell'analisi fallaci ed essi possono portare a decisioni che mettono a repentaglio l'intero progetto.

3 Processo di Identificazione

Nel presente capitolo verrà analizzata nello specifico l'identificazione dei rischi. In un primo momento si cercherà di definirla in maniera puntuale da un punto di vista letterario, mentre, successivamente verranno presentati gli strumenti più utilizzati e più utili per lo svolgimento del suddetto processo. Infine, verrà presentato il processo di identificazione nel caso di Italferr, impresa pubblica di ingegneria di proprietà di Ferrovie dello Stato Italiane (FS).

3.1 Descrizione dettagliata del processo di identificazione

Per la descrizione dettagliata del processo di identificazione si farà principalmente riferimento alla 6 ed. del PMBoK (PMI, 2017)e alla Practice Standard for Project Risk Management, entrambi testi del PMI. (PMI, 2009)

Il primo processo all'interno di quello iterativo di PRM da svolgere dopo la progettazione della gestione del rischio è l'identificazione. L'obiettivo ultimo dell'identificazione è di trovare e classificare tutti i rischi che possono impattare negativamente o positivamente gli obiettivi di progetto.

Nel primo ciclo del processo di PRM è impossibile identificare tutti i rischi soprattutto per la mancanza di informazioni complete sul progetto. Nei cicli successivi, quando il progetto sarà in fase esecutiva il contesto sarà cambiato, nuovi rischi saranno identificabili e nuove informazioni saranno disponibili per una rianalisi di quelli precedentemente identificati.

3.1.1 L'identificazione e fattori critici di successo

Per l'ottimale svolgimento dell'identificazione si potrebbe riassumere che l'unico input veramente utile sono le informazioni, quindi, l'analisi di contesto del progetto.

L'identificazione deve essere svolta già nella fase di iniziazione del progetto a monte dell'approvazione dello stesso per poi continuare lungo tutta il ciclo di vita del progetto fino alla chiusura. L'identificazione non è una scienza esatta e per questo deve essere un processo continuativo durante il progetto, specialmente nel momento in cui si raggiungono fasi in cui si presentano nuovi attori o cambiamenti di scenario, i quali possono presentare nuove esperienze e punti di vista all'identificazione dei rischi. In generale, l'obiettivo del Project Manager e del Risk Manager è di mantenere il controllo dei rischi più significativi. Per assicurarsi ciò il controllo dovrà estendersi a tutto il processo di gestione dei rischi tramite un'ottima documentazione associata allo svolgimento in maniera efficace e consistente delle attività. Nel caso in cui mancasse il controllo allora i motivi devono essere noti e dovrebbero essere presenti dei piani per gestirli.

Un'identificazione efficace deve:

- Essere sistematica, rigorosa e documentata. C'è bisogno di una metodologia che sia funzionale e facilmente comprensibile e comunicabile a tutti gli stakeholders e sponsor di progetto.
- Assicurarsi che il team di progetto sia conscio dei rischi più importanti in qualsiasi momento. Per fare ciò bisognerà includere elementi che mantengano elevata la comprensione dei rischi, come dei KPI[12].

[12] Key Performance Indicator. Sono degli indici quantificabili e critici che associano una valutazione numerica all'andamento di un determinato processo. A questi vengono associate soglie da rispettare o non superare.

- Identificare i rischi su tutti i livelli del progetto. I rischi non sono solamente associati alle attività da svolgere.
- Identificare anche i rischi "positivi". Le opportunità devono essere note al PM e al RM in modo che se possibile e conveniente possano essere perseguite per beneficiarne.
- Identificare anche i rischi che possono minare il raggiungimento degli obiettivi di business. Ogni progetto, solitamente fa parte di un portafoglio e/o programma dell'impresa che lo sta svolgendo. Un rischio potrebbe non solo rendere più complicato il raggiungimento degli obiettivi di progetto ma essere pericolo per l'impresa nella sua interezza. (Goncalves M., Heda R., 2014)

Per lo svolgimento del processo sono molto importanti le documentazioni disponibili, dato che, senza informazioni puntuali sul progetto sarebbe impossibile identificare rischi coerenti. Si citano:

- tutti i piani di progetto (piano dei tempi, piano dei costi, piano della qualità, piano degli approvvigionamenti, ecc…);
- Work Breakdown Structure (WBS), cioè la decomposizione gerarchica di tutto il lavoro che deve essere svolto dal team di progetto per raggiungere gli obiettivi e creare i deliverables;
- Issue log: documento in cui sono riportate tutte le issue, cioè quei rischi già avvenuti che hanno già impattato il progetto;
- Stakeholder register: registro nel quale sono riportati tutte le informazioni relative agli stakeholder di progetto come il ruolo nel progetto, la tipologia/categoria, il livello di interesse e potere nel progetto, ecc… Può essere utile per l'identificazione dei responsabili dei rischi.

- Registro delle lesson learned, il quale è utile soprattutto durante l'esecuzione del progetto e nelle fasi finale, perché viene compilato con le informazioni note a valle dell'accadimento di rischi precedentemente identificati e già avvenuti.

3.2 Strumenti per l'identificazione

Il processo di identificazione viene svolto per trovare tutti i rischi associati ad un progetto. Questo, viene ripetuto in maniera ciclica e ogni volta è svolto con un bagaglio informativo ampliato in funzione delle attività svolte nella finestra temporale passata tra le due iterazioni. In letteratura non esiste una visione unica su quali siano gli strumenti da usare, in realtà non vengono praticamente mai citati strumenti specifici utili alla ricerca di rischi. In generale, viene consigliato di svolgere riunioni documentando tutte le informazioni disponibili e tutte le idee su possibili scenari di rischio trovate dai vari partecipanti, che saranno solitamente gli stakeholder principali.

Risulta conseguenziale presumere che ogni impresa che svolge il PRM abbia un proprio processo di identificazione e che utilizza le tecniche più adatte al proprio contesto e ai progetti nei quali partecipa.

Successivamente verrà presentato il processo di identificazione in Italferr ma prima, si analizzerà come il PMBoK (PMI, 2017) consiglia di svolgere l'identificazione in termini di strumenti e tecniche.

3.2.1 Raccolta dei dati

Come già anticipato, i dati, ovvero le informazioni sono di cruciale importanza nella fase di identificazione. Di seguito sono elencate diverse tecniche per la raccolta dei dati:

- Checklist: le checklist sono liste di azioni, aspetti o rischi da dover considerare. Queste se utilizzate devono essere presenti prima della fase di identificazione essendo compilate con una serie di informazioni storiche provenienti da progetti finiti che abbiano similitudini con quello in essere. Possono considerarsi come liste di lesson learned di vecchi progetti, nelle quali saranno presenti i rischi più impattanti e le vulnerabilità più pericolose di vecchi progetti. Il problema delle checklist risiede nell'impossibilità di averne tali che siano complete; quindi, sarà importante ricordare che non renderanno con certezza l'identificazione più veloce o più semplice.
- Interviste: le interviste possono essere utili per raccogliere le opinioni di stakeholder o partecipanti al progetto molto esperti. In alcuni casi potrà essere consigliato intervistare esperti esterni. La debolezza delle interviste risiede nella possibilità di raccogliere opinioni influenzate troppo dall'opinione soggettiva dell'intervistato, o ancora peggio nell'intervistare persone che non aiutino in nessun modo l'identificazione, in entrambi i casi risultando come perdite di tempo.

3.2.2 Analisi dei dati

Vengono ora presentate tecniche di analisi dei dati raccolti in precedenza:

- Root cause analysis: si utilizza principalmente per cercare le cause o fonti che sono alla base di un evento che abbia impatti

negativi. Partendo da un problema specifico si cerca di individuare quale sia la minaccia che potrebbe avere come risultato la presenza del problema di partenza. Questa stessa tecnica si può usare anche nel caso delle opportunità.

- Analisi delle assunzioni e dei vincoli: Dato che ogni progetto si basa su una serie di assunzioni e vincoli generalmente considerati come veri a priori, svolgere un'ulteriore analisi cercando di confermarne la validità può essere utile per capire quali tra questi metta il progetto a rischio. Le minacce potrebbero essere conseguenza dell'inaccuratezza o incompletezza delle assunzioni mentre i vincoli se alleggeriti potrebbero comportare la nascita di nuove opportunità.
- Analisi SWOT: è la tecnica prende in esame punti di forza, debolezza, opportunità e minacce. È una delle tecniche più utilizzate nella gestione aziendale e risulta sempre molto utile per rafforzare la visione d'insieme del progetto e dei rischi associati. Scovare punti di forza o opportunità nascoste possono beneficiare il progetto, così come identificare nuove minacce o punti di debolezza può aiutare il team di rischio a riconsiderare le analisi svolte.
- Analisi dei documenti: controllare di documenti di progetto, per quanto possa essere faticoso, può essere utile nell'identificazione dei rischi. Una documentazione incompleta, all'interno della quale si trovino incertezze o ambiguità può generare dei rischi aggiuntivi, in alcuni casi nascosti, che possono minare il raggiungimento degli obiettivi di progetto.

3.3 Tecniche di identificazione di gruppo

Per valutare le tecniche di identificazione dei rischi svolte da gruppi di lavoro è importante comprendere le problematiche che potrebbero influenzare il gruppo nel raggiungere efficacemente i propri obiettivi (Chapman R. J., 1998).

Esistono diversi aspetti che influenzano le identificazioni di gruppo. Tra questi ci sono i vincoli propri del contesto che non possono essere modificati se non nel medio-lungo periodo. Questo è più esteso rispetto all'identificazione che, come singolo step, può durare dalle poche ore a un massimo di qualche giorno. Successivamente vanno considerati i fattori che caratterizzano il gruppo e che hanno valenza nel breve periodo, per questo motivo possono essere gestiti e modificati. Questi due insiemi di vincoli, combinandosi, hanno un effetto sui risultati della specifica tecnica utilizzata.

Tra i vincoli di contesto si evidenziano:

- le caratteristiche del gruppo, quindi la dimensione, gli obiettivi dei singoli individui e le loro caratteristiche;
- i compiti da svolgere, intendendone la natura, la chiarezza e la rilevanza;
- l'ambiente, quindi gli aspetti normativi e burocratici ma anche la posizione geografica e le varie relazioni interne al gruppo di lavoro.

Tra i fattori che possono essere gestiti nel breve periodo si trovano:

- lo stile di leadership, il quale dovrà variare in funzione del gruppo da controllare;

- processi e/o procedure che dovranno essere svolti comunque all'interno del lavoro di gruppo, si può però decidere chi svolgerà quali e perché;
- la motivazione, che sarà elevata se le attività da svolgere saranno abbastanza importanti per i singoli individui.

3.3.1 Brainstorming

Tra le tecniche di identificazione dei rischi si cita il brainstorming. Questa tecnica, proveniente dalla gestione aziendale prevede un processo che si evolve nei seguenti passaggi: ridefinizione del problema, generazione di idee, ricerca di possibili soluzioni e sviluppo delle soluzioni selezionate.

Secondo Osborn, che sviluppò il metodo negli anni '50 del '900, il brainstorming risulta efficace grazie a due aspetti. Innanzitutto, ragionare in gruppo è più produttivo che farlo singolarmente, poi nel lavoro di gruppo si generano *reinforcement* quando un'idea o una posizione viene immediatamente rafforzata dalle opinioni in accordo di altri partecipanti. (Osborn Alex F., 1953)

Osborn identificò anche quattro regole da seguire quando si effettua brainstorming:

- Le critiche sono escluse;
- Incoraggiamento del "*free-wheeling*[13]";
- Bisogno di quantità, più idee ci sono più è probabile che almeno una sia utile;

[13] Letteralmente "ruota libera", si intende la possibilità di presentare pensieri o idee senza limiti né vincoli.

- Combinazioni e miglioramento, approccio per cui si deve cercare di trovare idee sulla base di quelle già precedentemente esposte.

Per svolgere la tecnica è consigliato che il gruppo sia composto da una decina di persone eterogenee, quindi, con differenti punti di vista sul progetto. Il risultato dell'identificazione è influenzato dalla composizione del gruppo di lavoro in termini di personalità dominanti, forti differenze di status sociale e lavorativo, o minaccia di "sanzioni" tra membri. Anche se la prima regola di Osborn sottolinea che le critiche sono escluse, non è facile creare e moderare un ambiente in cui le critiche alle idee altrui vengano realmente escluse e/o posticipate. Criticare un'idea può farla perdere e consequenzialmente scoraggiare l'autore a proporne altre o comunque a partecipare al massimo delle sue possibilità.

Lo svolgimento del brainstorming deve essere completamente slegato dalle attività che i singoli partecipanti svolgono quotidianamente. Per questo motivo, le sessioni di brainstorming devono avere un titolo, un luogo e un orario ben definiti.

Si può certamente affermare che il brainstorming è molto più complicato di quanto sembri. Non è una semplice chiacchierata, dalla quale cercare di trovare qualche idea interessante, o nel caso in analisi, rischi realmente esistenti. Vi partecipano tante persone, che devono rispettare una serie di regole e che soprattutto devono trovare del tempo da dedicare alla sessione. In alcuni casi potrebbero trovarsi in situazioni in cui vi è grande urgenza, la quale avrà un impatto negativo sullo svolgimento dell'identificazione, perché, probabilmente le figure dominanti caratterialmente o in termini di potere decideranno da sole il dà farsi.

Concludendo, la tecnica di brainstorming può essere utile all'identificazione dei rischi nelle fasi iniziali di un progetto poco noto a diversi componenti del team, se si ha disponibilità di tempo e denaro tali da coprire sessioni che non raggiungono i risultati sperati.

3.3.2 Nominal Group Technique (NGT)

La NGT è una tecnica che venne sviluppata da Delbecq nel 1968. Il metodo si svolge nel modo seguente. Ogni componente di un gruppo di 7-10 persone scrive su un foglio le idee relative al problema in analisi, (nel caso specifico i rischi identificati). Dopo una decina di minuti ogni componente presenta a turno una delle idee/rischi a tutto il gruppo e, dopo una breve discussione, vengono documentati su una lavagna visibile a tutti. Il processo continua finché ogni membro non ha terminato tutte le idee/rischi. Infine, ogni componente del gruppo scrive la propria valutazione dei rischi più gravi/importanti ordinandoli. Come ultimo step vengono aggregate le valutazioni in modo da trovare la decisione del gruppo. (Delbecq A. L., 1968)

Le caratteristiche del processo della NGT pongono grande importanza sulle decisioni dei singoli partecipanti, superando le problematiche del brainstorming, tecnica che, come detto, può mettere in difficoltà alcuni partecipanti. Gli studi di Bouchard mostrano come la NGT abbia un numero medio di idee uniche, una media di idee totali presentate e una qualità delle idee tali da renderla una tecnica altamente produttiva. (Bouchard T. J. Jr., 1970)

Ciò che rende l'NGT così produttiva è, controintuitivamente, la mancanza di comunicazione. Dato che i rischi vengono scritti, presentati e

poi ordinati con un processo preciso, il gruppo riuscirà più facilmente a rimanere "in tema". Sarà più raro che si creino contrasti ideologici, mentre è più probabile che il contrasto possa essere legato all'oggettivo problema in considerazione. L'NGT depersonalizza i ragionamenti dei partecipanti portandoli a mantenere alta la razionalità e l'imparzialità nelle opinioni.

Come il Brainstorming, organizzare una sessione di NGT non è facile, come è tutt'altro che semplice trovare un gruppo eterogeneo ma che, allo stesso tempo, abbia un elevata conoscenza del progetto, del Risk Management e delle possibilità dell'organizzazione. Il moderatore è molto importante, in quanto deve assicurarsi che la procedura venga rispettata passo dopo passo e variazioni o perdite di tempo non sono ammesse. Un moderatore con poca leadership può compromettere il riuscimento della Nominal Group Technique. Concludendo, per assicurarsi che la NGT possa funzionare servirà un ambiente "asettico", privo di distrazioni e che sia diverso dal normale ambiente di lavoro. Rispettando questa serie di vincoli, l'NGT può essere utilizzata, sicuramente a favore del Brainstorming.

3.3.3 Tecnica Delphi

La tecnica Delphi, messa a punto dalla RAND Corporations negli anni '50 del '900, è un metodo per la collezione sistematica di giudizi provenienti da individui anonimi riguardo un particolare tema o problema. Per lo svolgimento della tecnica è consigliato l'utilizzo di tre gruppi separati di individui:

- Decisori: coloro che aspettano il risultato della tecnica, in modo da usarlo per i loro scopi. Nel nostro caso il PM il RM e lo Sponsor di Progetto;

- Staff: gruppo che definisce il primo e tutti i successivi questionari;
- Rispondenti: coloro che dovranno compilare i questionari.

La tecnica Delphi segue una struttura per cui ad un gruppo di individui anonimi viene posta una serie di domande alle quali rispondere associando un numero (solitamente da 1 a 5); successivamente viene presentato al gruppo il risultato aggregato tramite il quale i singoli individui possono decidere se modificare la propria risposta o mantenere quella precedentemente data. Questo processo viene ripetuto finché non si raggiunge l'iterazione conclusiva predeterminata. (Megan M. Grime, George Wright, 2016)

I partecipanti ricevono le domande individualmente, contattati direttamente sul proprio device. L'eliminazione del contatto sociale diretto, la fornitura dei feedback e la possibilità di rivedere le proprie posizioni sono i principi del metodo. Per quanto riguarda il feedback, i vari partecipanti lo ricevono in maniera tale che sia slegato dalla propria risposta, pertanto, loro rinviano la propria opinione senza svolgere un'analisi comparata delle differenze tra la loro prima stima e il risultato della stima di gruppo.

La tecnica Delphi non pone limiti al numero di partecipanti, solitamente si cerca di dimensionare il gruppo per rendere il risultato del lavoro statisticamente consistente. I membri sono anonimi, non hanno pressioni sociali o date dalla presenza di personalità forti, come nelle tecniche di cui sopra. Rispondere in solitudine e nell'anonimato rende molto più probabile una risposta totalmente sincera e razionalmente improntata verso l'obiettivo della tecnica.

I punti di forza possono essere considerati anche come punti di debolezza. La mancanza di rapporti sociali elimina la soddisfazione che si

riceve quando si risolve un problema, la mancanza di comunicazione può rendere complesso per i rispondenti interpretare i risultati. In caso di risposte conflittuali lo staff deve presentare come feedback due risultati alternativi che verranno votati. Questa procedura identifica le priorità del gruppo ma non risolve il conflitto.

Da un punto di vista di identificazione dei rischi, la tecnica Delphi può essere utile se sfruttata con il seguente approccio. Partendo da una conoscenza del contesto soddisfacente per tutti i partecipanti, lo staff organizza le prime iterazioni suddividendo un insieme noto di rischi in gruppi di rischio (ad esempio: rischi legati alle attività di produzione, rischi legati a burocrazia e norme, rischi legati alla mancanza di materie prime e/o fornitura in generale, rischi di interruzione lavori). I partecipanti con le loro risposte creeranno una lista di importanza dei gruppi di rischio. Ogni gruppo di rischio, composto da una lista di rischi viene quindi ripresentato ai partecipanti in ordine di importanza. Rispondendo i partecipanti creano una lista di importanza interna ad ogni gruppo. In funzione di tempo e possibilità si decide quali e quanti gruppi di rischio analizzare singolarmente. Successivamente lo staff elimina, per ogni gruppo, tutti i singoli rischi valutati come poco importanti. Infine, si chiede se al netto delle varie ordinazioni per ogni gruppo, ci sono dei singoli rischi che, in generale, siano di maggiore importanza, andando quindi a identificare una singola lista di rischi che si può poi utilizzare in fase di assessment.

3.4 Italferr

Italferr è una società per azioni partecipata al 100% da Ferrovie dello Stato. Il settore dell'azienda è l'ingegneria dei trasporti, con una maggiore attenzione verso l'ingegneria ferroviaria. Nel settore è la più grande azienda italiana e opera sia nel mercato italiano che internazionale.

Italferr quindi assiste il cliente in tutto il ciclo di vita del progetto, partendo dal procurement fino alla messa in servizio. Nel particolare le attività che Italferr offre sono:

- Project Management;
- Direzione e Supervisione Lavori;
- Quality Assurance e Quality Control;
- Contract Management;
- Procurement;
- Collaudi e Messa in Servizio;
- BIM Management;
- Project Risk Management.

Italferr ha oltre 2500 dipendenti dislocati in sedi a Roma, Milano, Torino, Napoli, Genova, Palermo, Firenze, Bologna, Bari, Verona e Reggio Calabria.

Dal 2021 Italferr si sta occupando principalmente dei progetti legati al PNRR[14] che sono molti e di grande difficoltà gestionale, dovuta alla sovrapposizione di risorse. L'obiettivo è di attrezzare con nuove tecnologie 4.220 chilometri di linee ferroviarie ad alta velocità e regionali. Tra i vari cantieri si citano, il raddoppio Roma-Pescara, l'asse Napoli-Bari e l'asse Palermo-Catania-Messina.

[14] Piano Nazionale di Ripresa e Resilienza: strumento del programma Next Generation EU dell'Unione Europea che conferisce all'Italia risorse totali per 191,5 miliardi di euro da impiegare tra il 2021 e il 2026.

Per tutti i progetti del PNRR e in generale per ogni progetto di Ingegneria Ferroviaria, Italferr svolge attività le di Project Risk Management grazie al proprio Risk Office. Del processo di Risk Management questa tesi si concentra sul processo di identificazione. Durante lo svolgimento del tirocinio è stato possibile comprenderne le fasi salienti e gli strumenti utilizzati. Nei prossimi paragrafi verrà analizzato e spiegato con un livello di dettaglio che ne permetta una chiara comprensione.

3.5 L'identificazione in Italferr

Come visto in precedenza secondo il PMBoK il processo di identificazione si compone, nella quasi totalità dei casi, di un insieme di riunioni che vertono verso il raccoglimento e l'analisi delle informazioni di progetto. Questo serve ai decisori a trovare i rischi individuali di progetto. Un approccio di questo tipo è difficile da protocollare. Inoltre, impiega un elevato numero di risorse e, potenzialmente, lunghi periodi di tempo.

Italferr avendo da gestire un grandissimo numero di progetti in tempi brevi ha sviluppato un'identificazione semi-automatizzata. Il processo di identificazione, infatti, si compie in poche ore lavorative spalmate lungo un periodo che solitamente può andare dai pochi giorni al massimo di una settimana di lavoro.

La mancanza di risorse unita all'approccio fortemente ingegneristico dell'azienda ha permesso che il processo di identificazione divenisse una "formalità" tecnica del Risk Office in concomitanza del Team di Commessa del progetto in analisi. I risultati ottenuti dal Risk Office sono stati una compressione dei tempi necessari all'identificazione e la possibilità di portare a termine questa fase con un numero di risorse limitato

mantenendo, però, elevati i tassi di raggiungimento degli obiettivi interni. Infine, la qualità dell'identificazione, con l'affinamento delle tecniche, è aumentata molto negli ultimi anni.

3.5.1 L'analisi di contesto

Uno degli aspetti più importanti della Gestione dei Progetti è il livello di comprensione del contesto da parte dei partecipanti al progetto. Se non si ha contezza di cosa succede al di fuori dei confini geografici, lavorativi ed economici del progetto, gli obiettivi di tempo, costo e qualità saranno molto più complicati da raggiungere. Sulla base di un'analisi di contesto ben svolta e strutturata sarà molto più semplice comprendere il progetto nella sua interezza.

L'identificazione quindi parte con la richiesta, da parte del Risk Office, di informazioni riguardo il contesto che possono

- mettere a rischio (sia positivamente che negativamente) il progetto,
- Influenzarlo,
- Farlo deviare dal normale svolgimento.

Queste informazioni arriveranno dal Team di Commessa tramite la compilazione di un documento Excel. Il documento è composto da un insieme di fogli, uno per ogni tipologia di fattore d'interesse del progetto.

3.5.1.1 Informazioni sul progetto e obiettivi

Le prime informazioni che vengono inserite sul documento sono relative al nome del progetto e all'evoluzione attesa del contesto. Queste non hanno un grande valore nell'identificazione ma servono semplicemente come informazioni di base.

Nella pagina successiva il Team di Commessa deve compilare le tabelle che riguardano gli obiettivi. Questi possono essere di quattro tipologie: Tempi di realizzazione dell'Opera, Tempi di consegna del Progetto, Costi dell'Opera a vita intera, Qualità dell'Opera e Redditività dell'Opera. Nel caso dei progetti PNRR l'obiettivo tempi risulta essere più importante dato che le risorse provenienti dall'UE possono essere usate strettamente entro il 31/12/2026.

In funzione degli obiettivi di progetto verranno inserite tre informazioni:

- Baseline,
- Livello Comfort,
- Livello di Fall-Down.

La prima si riferisce al livello pianificato per l'obiettivo, il livello di comfort indica quanto ci si può scostare dalla baseline senza ripercussioni, mentre il fall-down come suggerisce la traduzione (fallimento) non può essere superato, altrimenti vi è il rischio di fallimento del progetto e del management della commessa.

3.5.1.2 Vulnerabilità

Le vulnerabilità sono un fattore di contesto molto importante nell'identificazione dei rischi. Una vulnerabilità è un aspetto interno o esterno al progetto che lo mette a rischio in funzione dell'accadimento o

meno di determinati eventi. Si potrebbe definire alternativamente come un punto debole.

Un esempio decontestualizzato può essere il seguente: considerando le proprie capacità comunicative come una vulnerabilità, aumenteranno le probabilità che si presenti il rischio "forti incomprensioni" con le persone con cui si passa del tempo insieme.

Per quanto riguarda i progetti ferroviari di Italferr, il Risk Office ha identificato una lista, creata nel tempo ed in costante revisione ed aggiornamento, composta da 81 vulnerabilità.

Ciò che viene richiesto al Team di Commessa è di studiare le singole vulnerabilità e indicare se queste sono presenti o meno.

Le vulnerabilità vengono suddivise in funzione che siano interne (proprie alle attività di progetto, ad esempio, la gestione del personale) o esterne (ad esempio le interferenze strutturali) e anche in funzione del contesto di provenienza (gestionale, politico, ambientale, ecc…).

Solitamente le vulnerabilità si attestano intorno al 20-40% del totale. All'aumentare della loro presenza aumenteranno i rischi potenziali associati al progetto.

Qualora il Team di Commessa sia in dubbio se la vulnerabilità impatti sul progetto o meno, viene lasciata attiva così da rappresentare una possibile fonte di rischio per il progetto.

3.5.1.3 Stakeholder

Nell'identificazione dei rischi gli stakeholder interessati al progetto sono uno dei driver più importanti. Possono creare, mitigare, amplificare ed

eliminare scenari di rischio solo grazie alla loro presenza/assenza. Uno stakeholder influenza il progetto sia come persona che come decisore.

La gestione degli stakeholder è una delle attività più importanti della gestione dei progetti; quindi, questi diventano una variabile importantissima nel processo di identificazione dei rischi.

All'interno dei progetti di Italferr sono presenti un gran numero di stakeholder. Il Risk Office ne ha identificati 48, divisi in 6 gruppi.

La loro presenza o assenza viene inserita dal Team di Commessa che deve fornire le informazioni di contesto direttamente sul foglio Excel.

3.5.1.4 Attività

Ogni progetto è suddiviso in attività e queste, disarticolate in gruppi e sottogruppi compongono la WBS (Word Breakdown Structure). La WBS è: "un albero di attività orientate ad un obiettivo, che organizza, definisce e visualizza graficamente tutto il lavoro che deve essere fatto per raggiungere gli scopi finali di un progetto." (Nonino F., Tonchia S., 2013) Una volta organizzato e "spacchettato" tutto si potranno inserire le singole attività a livello di Gantt.

Ogni progetto è unico e per questo sarà composto da un insieme di attività diverse da qualsiasi altro progetto, anche molto simile. Visto il livello alto di analisi, il Risk Office ha scelto di creare una lista di macro-attività che sono proprie dei progetti di costruzione e in particolare dei progetti di Ingegneria Ferroviaria.

Questa lista è organizzata tramite una logica temporale e sequenziale. Infatti, vi sono una serie di attività di Progettazione legate alla "Consegna di un Progetto" e successivamente le macro-attività legate alla "Consegna

di un'Opera" che si concludono con le attività di Consegna dell'Opera e Chiusura del Progetto.

In totale vi sono 44 singole attività identificate che il Team di Commessa dovrà indicare se da svolgere o se sono già state concluse e/o superate.

3.5.1.5 Opere

Le opere fanno parte dell'ultimo insieme di variabili che il Team di Commessa dovrà compilare sempre secondo la modalità presente/non presente. Per opera Italferr intende le costruzioni e impianti che dovranno essere costruiti durante lo svolgimento del progetto.

La lista è composta da 15 opere tra le quali si citano le Opere Civili, gli Impianti e il Ballast e Armamento. Quest'ultima corrisponde al piazzamento dei binari lungo il percorso, nel particolare il Ballast è il pietrisco che si trova tra le assi perpendicolari/traversine.

Anche nel foglio delle Opere il Team di Commessa dovrà inserire se vi è presenza o assenza delle singole opere all'interno del progetto.

3.5.1.6 Issue e Rischi Preliminari

Per completare l'insieme di informazioni utili agli analisti per identificare i rischi servono anche le Issue e i Rischi Preliminari.

Secondo Italferr le Issue sono gli eventi già accaduti che hanno un impatto sugli obiettivi, quindi, sono note a differenza dei rischi che invece sono eventi futuri che potrebbero accadere. (Mastrobuono G., 2023)

Essendo già accaduta, una issue non può essere gestita direttamente, in funzione del suo impatto si potranno prendere o meno decisioni riguardo altre attività e/o vincoli di progetto.

Le Issue devono essere comunicate perché hanno grande influenza sugli obiettivi di progetto. Le Issue possono essere gestite secondo due approcci alternativi, o attivamente, dovendo quindi recuperare sull'aumento dei costi o allungamento dei tempi tramite azioni di mitigazione oppure si inseriscono all'interno della baseline, traslandola. Il secondo caso si attiva solo ed esclusivamente a valle dell'inserimento dell'issue a contratto, modificando obiettivi ed eventuali penali associate.

Nel file di contesto il Team di Commessa deve descrivere le issue, associandole all'obiettivo impattato, l'impatto che hanno e se questo sia peggiorativo o migliorativo.

I rischi preliminari sono l'insieme di rischi che il Team di Commessa si aspetta possano colpire il progetto in esame e che possano portare uno slittamento degli obiettivi di progetto. Per ogni rischio preliminare si dovrà sapere se questo è un'opportunità o una minaccia e quale obiettivo impatterà. Ognuno dovrà essere descritto tramite un linguaggio che sia il più esplicativo possibile in termini di evento scatenante e conseguenze dell'accadimento.

3.5.2 Costruzione della lista di Rischi

Una volta ricevuti in input tutti i dati di contesto sul progetto, gli analisti svolgono una serie di attività con l'obiettivo di creare una Watch List. Questa funge da lista semi-definitiva dei rischi, creandola, il Risk Office è come se svolgesse la quasi totalità dell'identificazione in maniera

autonoma. La Watch List iniziale consiste nell'elenco di tutti i possibili scenari di rischio o rischi associabili al progetto. La Watch List è un documento intermedio che verrà analizzato da analisti e Team di Commessa con l'obiettivo di eliminare gli scenari di rischio non pertinenti il progetto e poi successivamente valutare i rimanenti in modo da creare il Risk Register del progetto. La Watch List è un documento che permette a Italferr di recuperare moltissimo tempo tra la fase di identificazione e quella di assessment. Finendo la prima si svolgono contemporaneamente le prime attività della seconda. L'assessment poi terminerà con gli studi sul rischio di progetto e le stime degli analisti sugli obiettivi di progetto. Sulla base di queste stime si deciderà se e come mitigare insieme al Team di Commessa.

Per costruire la Watch List gli analisti devono svolgere una serie di attività, sempre servendosi di Excel, che verranno presentate nei prossimi paragrafi.

3.5.2.1 Studio dell'analisi di contesto

Come primo step, gli analisti studiando l'analisi di contesto, comprendono quali sono le attività che verranno svolte, gli stakeholder coinvolti ecc…

Questo studio pre-identificazione unito all'esperienza degli analisti serve loro a entrare a pieno nel progetto e, inoltre, a formare le prime opinioni riguardo quali potranno essere gli scenari di rischio più importanti.

3.5.2.2 Gli scenari di rischio

In Italferr negli anni è stata creata una lista di scenari di rischio che funge da database di rischi. Questi hanno una grandissima utilità sia operativa che analitica. Gli scenari non sono stati inventati dal nulla, discussi e poi accettati come realistici, bensì gli analisti hanno svolto una serie di attività di ingegneria inversa a partire dalle analisi di rischio precedentemente svolte negli anni. Gli scenari identificati ad oggi sono oltre 200.

La descrizione degli scenari segue la seguente logica: "DATO CHE è successo qualcosa, POTREBBE succedere qualcos'altro, CHE INNESCA eventi che portano un impatto sugli obiettivi." La conseguenza dell'accadimento dello scenario sarà una deviazione sul grado di raggiungimento degli obiettivi.

La logica è composta da quattro parti, la prima è la **causa**, la seconda è **l'evento incidente**, la terza viene definita **dinamica d'impatto**. Infine, successiva all'accadimento dello scenario vi è la **conseguenza**.

Gli scenari non sono solo descritti, infatti, ognuno è associato ad una tupla di informazioni che sono:

- Event-ID: codice univoco per ogni scenario;
- Fase: la fase può essere progettazione o realizzazione;
- Attività: una di quelle facente parte del foglio attività compilato dal Team di Commessa;
- Opera di riferimento: una di quelle facenti parte del foglio opere compilato dal Team di Commessa;
- Obiettivo Impattato: uno dei cinque elencati nel paragrafo 1.3.1
- Minaccia/Opportunità
- Vulnerabilità: le vulnerabilità associate possono essere più di una, il Risk Office definisce che ogni scenario di rischio può essere

associato un massimo di quattro vulnerabilità. Uno scenario non deve obbligatoriamente essere associato ad una vulnerabilità. La scelta su quali vulnerabilità sono associate ai vari scenari è stata fatta dal Risk Office secondo una logica per cui la vulnerabilità è ciò che facilità il presentarsi della causa scatenante;

- Stakeholder: come per le vulnerabilità gli stakeholder possono essere più di uno, fino a un massimo di quattro. Uno scenario non deve essere obbligatoriamente associato ad uno stakeholder, esistono scenari che non impattano né vengono influenzati dalla presenza di stakeholder.

3.5.2.3 Studio degli Scenari e Rischi preliminari

Uno scenario si attiva se la tupla associata è completamente attiva. Questo significa che l'insieme informativo (Fase, Attività, Opera, Obiettivo, Vulnerabilità, Stakeholder) relativo al singolo scenario è stato attivato in fase di analisi di contesto dal Team di Commessa.

Event-ID	Indice di Rilevanza	Fase	Chk	Attività	Chk	Opera di riferimento	Chk
XX	1	Realizzazione	1	Costruzione	1	Gallerie	1

Tabella 1 - Esempio Scenario Attivo (prima parte)

Potrebbe Succedere che	Obiettivo Impattato	Chk	Minacce / Opportunità	Vulnerabilità 1	Chk	Stakeholder 1	Chk
- potrebbero verificarsi delle frane in galleria - il verificarsi di tali eventi potrebbe causare sospensioni delle attività e la successiva necessità di eseguire interventi di ripristino al fronte per il riavvio dello scavo allungando i tempi di consegna dell'opera	Tempi di realizzazione dell'Opera	1	Minaccia	Fragilità ambientale: Fragilità del territorio e pericolosità idraulica.	1	Appaltatore	1

Tabella 2 - Esempio Scenario Attivo (seconda parte)

Le colonne "Chk" si attivano con "1" nel momento in cui il fattore della colonna precedente è stato attivato nel file di Analisi del Contesto da parte del Team di Commessa.

Se anche solo un singolo fattore dell'insieme non è stato attivato lo scenario di rischio non sarà attivo e quindi non inerente al progetto.

Event-ID	Indice di Rilevanza	Fase	Chk	Attività	Chk	Opera di riferimento	Chk
XY	0	Progettazione	0	Direzione Lavori	1	Tutte	1

Tabella 3 - Esempio Scenario Non Attivo (prima parte)

Potrebbe Succedere che	Obiettivo Impattato	Chk	Minacce / Opportunità	Vulnerabilità 1	Chk	Stakeholder 1	Chk
- potrebbero esserci criticità connesse alle attività di Direzione Lavori - alcune di queste criticità potrebbero causare ritardi - i ritardi potrebbero allungare i tempi di consegna dell'opera	Tempi di realizzazione dell'Opera	1	Minaccia	Complessità nella gestione del personale.	1	Direzione Lavori	1

Tabella 4 - - Esempio Scenario Non Attivo (seconda parte)

Nel caso rappresentato in tabella la fase "Progettazione" non fa parte del progetto, il quale evidentemente l'ha già superata. Per questo motivo lo scenario non è attivo, informazione che viene confermata dall'Indice di Rilevanza.

L'informazione per cui l'assenza di un singolo fattore elimini lo scenario deve essere presa "con le pinze" dato che l'analisi di contesto viene svolta dal Team di Commessa il quale, anche se composto da esperti in Project Management, potrebbe aver omesso inavvertitamente o commettendo un errore qualche fattore dal progetto. In tal caso ci saranno scenari non attivi che rappresentano appieno situazioni che potrebbero accadere durante lo svolgimento del progetto. Al contrario si dovrà anche considerare la situazione in cui il Team di Commessa possa aver inserito qualche fattore che potrebbe essere escluso. Questi fattori in più potrebbero attivare scenari irrealistici o non inerenti al progetto.

Sulla base di queste considerazioni gli analisti studiano gli scenari attivi e iniziano un lavoro di confronto, chiamato "check di copertura" tra scenari attivi e non e i rischi preliminari. Per condurre lo studio assicurando un'analisi completa, prima di iniziare gli analisti "sdoppiano" tutti quei rischi preliminari che hanno effetto su più obiettivi. Ad esempio, se un semplice rischio come "possibili frane in luogo X" ha un impatto sia su tempi che costi, si determineranno due rischi uguali con obiettivi differenti.

Durante il check di copertura si cercano gli scenari di rischio che coprono i singoli rischi preliminari. Ogni rischio può essere coperto da più scenari.

Obiettivo	Descrizione	Cop 1	Rilev	Copertura 1	Cop 2	Rilev	Copertura 2
Tempi di realizzazione dell'Opera	**Interferenza Comunale**	YX	1	MINACCIA - Tempi di realizzazione dell'Opera - potrebbe avvenire una modifica dei requisiti di progetto da parte del Committente per variazioni della normativa e/o per richieste degli Enti - il rispetto dei requisiti modificati potrebbe richiedere una durata della costruzione maggiore di quanto inizialmente pianificato	YY	1	MINACCIA - Tempi di realizzazione dell'Opera _____ - la risoluzione delle interferenze potrebbe essere più lenta ed onerosa di quanto previsto - la risoluzione delle interferenze potrebbe generare ritardi nelle lavorazioni

Tabella 5 - Esempio di Copertura Rischio Preliminare

Il motivo della scelta dello scenario è a discapito del singolo analista che la effettua. Trovare uno scenario che copra un rischio preliminare significa che lo scenario in analisi contiene concettualmente al suo interno l'evento descritto dal rischio. Scenari specifici saranno associati a rischi specifici, mentre scenari più generali potrebbero coprire un gran numero di rischi

specifici. Si evince che non vi è omogeneità tra i vari scenari e per questo motivo un check di copertura ben svolto potrebbe comunque avere problematiche di completezza.

Infatti, una delle peculiarità del check di copertura è la scoperta di scenari di rischio non attivi che coprono in maniera diretta alcuni rischi preliminari.

Obiettivo	Descrizione	Cop1	Rilev	Copertura 1
Tempi di realizzazione dell'Opera	**Problematiche ambientali 2** - potrebbe essere rilevato materiale inquinato da sostanze che ne rendono obbligatoria la bonifica. Eventuali ritrovamenti potrebbero richiedere azioni mitiganti non programmate	ZX	0	MINACCIA - Tempi di realizzazione dell'Opera _____ - nell'ambito della realizzazione dell'appalto, potrebbe essere rilevato materiale inquinato da sostanze che ne rendono obbligatoria la bonifica - Il ritrovamento di materiale inquinato e la successiva bonifica potrebbero ritardare la costruzione
Costi dell'Opera	**Problematiche ambientali 2** - potrebbe essere rilevato materiale inquinato da sostanze che ne rendono obbligatoria la bonifica. Eventuali ritrovamenti potrebbero richiedere azioni mitiganti non programmate	ZY	0	MINACCIA - Costi dell'Opera _____ - nell'ambito della realizzazione dell'appalto potrebbe essere rilevato materiale inquinato da sostanze che ne rendono obbligatoria la bonifica -L'Appaltatore potrebbe ottenere il riconoscimento di oneri addizionali in ragione della bonifica imprevista di materiale inquinato

Tabella 6 - Esempio di Mancata Copertura Rischio Preliminare

Nell'esempio in tabella si può notare che il rischio preliminare, precedentemente sdoppiato interessando sia tempi che costi, è coperto dagli scenari ZX e ZY che non fanno parte della lista di scenari attivi (si evince dalla colonna "Rilev").

Dell'insieme di scenari non attivi che coprono uno o più rischi preliminari, gli analisti dovranno identificare quali fattori non sono stati attivati durante l'analisi di contesto. Successivamente dovranno decidere se attivarli o meno.

Anche se lo scenario non attivo fosse l'unico a coprire un determinato rischio preliminare, che si decida immediatamente di attivare il fattore/i

d'interesse (stakeholder, attività, vulnerabilità, …) significherebbe cambiare il contesto del progetto e in qualche caso potrebbe renderlo differente dalla realtà. Inoltre, un nuovo fattore può attivare nuovi scenari, i quali dovranno essere gestiti e analizzati.

Rispettare la corrispondenza tra realisticità dell'analisi di contesto, scenari di rischio e rischi preliminari è uno dei requisiti più difficili da gestire per l'analista.

A partire da queste condizioni è importante richiamare l'attenzione sull'importanza della comunicazione. Un Team di Commessa che ha ben compreso l'attività di compilazione dell'analisi di contesto minimizza le ambiguità tra scenari attivi e rischi preliminari. Dall'altro canto un Risk Office che aggiorna costantemente il proprio database e che rivede i legami tra fattori e scenari, avrà meno difficoltà nello scegliere se un fattore deve o meno essere aggiunto tra le variabili di progetto.

In ogni caso quello che succede immediatamente dopo il check di copertura è una riunione tra analista e PM/PMA e altri esponenti del Risk Office e del Team di Commessa.

3.5.3 Riunione di Identificazione con il Team di Commessa

Una volta svolta la copertura degli scenari con i rischi preliminari con eventuali aggiunte di fattori che attivano nuovi scenari gli analisti si trovano compilato, nel file Excel di identificazione, il foglio denominato "Output Assessment".

Questo foglio, composto da tutti gli scenari di rischio associati a tutti i fattori che li hanno attivati, servirà in realtà da input al file Excel che si utilizzerà in fase di Assessment.

Il foglio “Output Assessment” del file di identificazione diverrà nel file di assessment il foglio “Input Assessment”. Questo, sarà quindi composto da tutti gli scenari identificati e quelli che sono stati in precedenza associati alla lista di rischi preliminari avranno la descrizione del rischio preliminare associato nella sezione “descrizione modificata”.

Anche se il foglio è chiamato “Input Assessment” verrà utilizzato nella riunione di identificazione con il Team di Commessa che prenderà le decisioni definitive.

La riunione serve per analizzare la lista di scenari di rischio ed eliminare quelli non inerenti al progetto. Se a posteriori di tutte le eliminazioni ci sono vulnerabilità che non sono più associate a nessun rischio queste non vengono più considerate nel progetto.

In ogni caso, il risultato della riunione, quindi, il numero di rischi rimanenti nella lista sarà in funzione della propensione al rischio del singolo PM. Questo comporta un’ulteriore difficoltà per l’analista, il quale si troverà a mediare, in sede di riunione, le scelte del PM in caso sia troppo avverso o propenso al rischio. In generale a fine riunione la lista che si ottiene è più corta rispetto a quella presentata dagli analisti in prima battuta. Il numero di rischi che vengono eliminati dipende dalla propensione al rischio del singolo PM.

La lista che si viene a creare a valle della riunione viene definita “Watch List” ed è un insieme di rischi da attenzionare da parte del Team di Commessa ed è composta come segue: ogni rischio viene numerato, gli viene associata una sorgente di rischio, viene descritto il suo evento incidente, l’obiettivo impattato ed infine l’effetto ipotizzato.

La Watch List sarà l'effettivo documento di input per la successiva fase di assessment dalla quale verrà creato il Risk Register, composto dai rischi più pericolosi per il progetto e che potrebbero necessitare di mitigazione.

3.6 BPMN del processo di identificazione dei rischi

Per avere una visione completa e integrata del processo di identificazione si è scelto di riportarlo tramite l'utilizzo della rappresentazione grafica nota come Business Process Model and Notation.

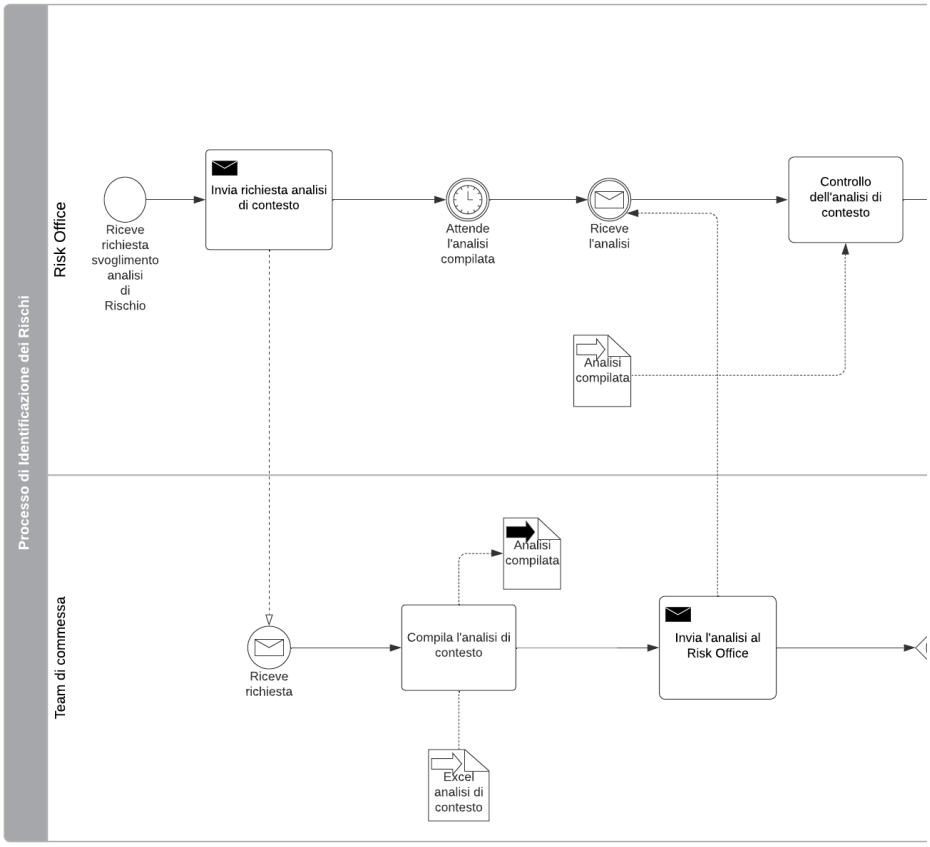

Figura 3 - Prima parte del BPMN del processo

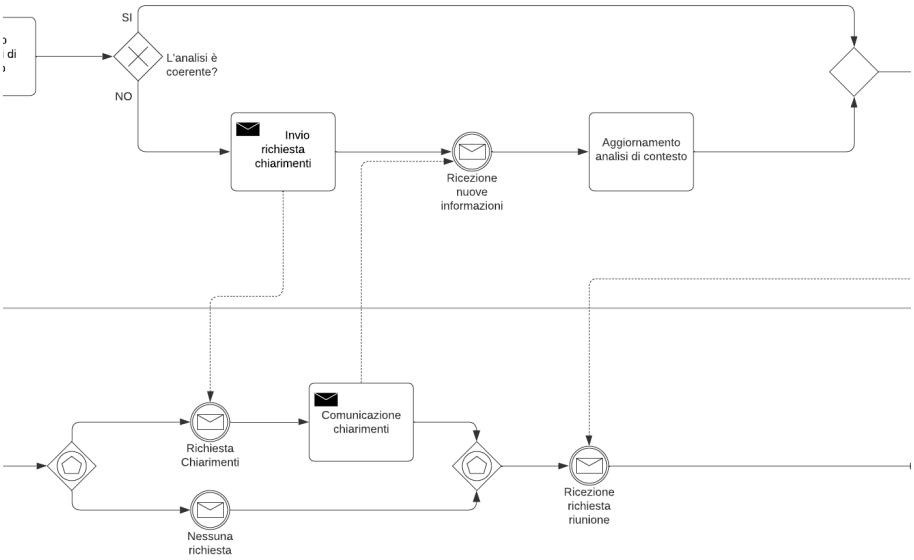

Figura 4 - Seconda parte del BPMN del processo

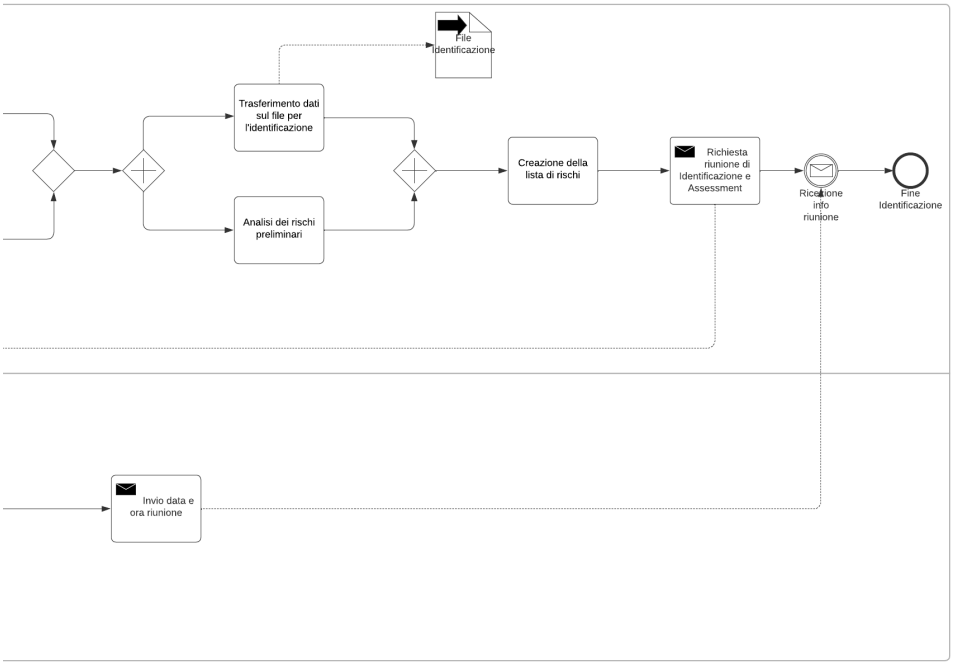

Figura 5 - Terza parte del BPMN del processo

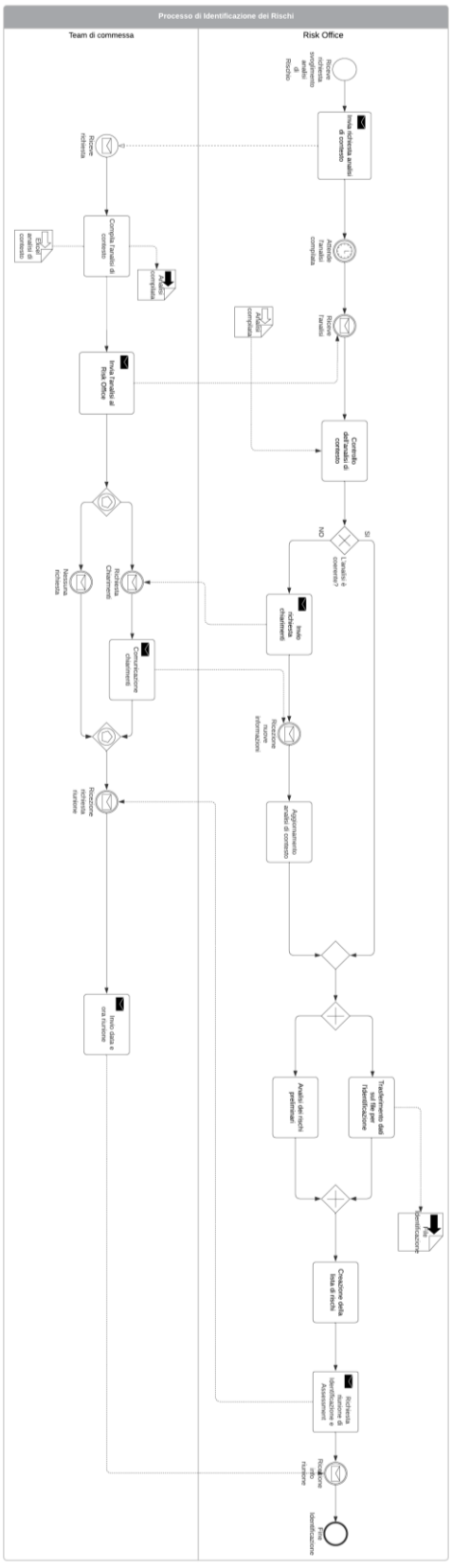

Figura 6 - BPMN intero

4 Risk Identification con l'IA: indici di valutazione della qualità dei risultati

Gli obiettivi dello studio

In Italferr l'identificazione si suddivide in due step principali: la creazione della lista automatizzata di scenari di rischio e l'analisi di copertura della lista dei rischi preliminari presentata dal Team di Commessa (TdC).
La prima è il risultato di un processo che si svolge grazie all'inserimento dell'analisi del contesto, compilata dal TdC, in uno strumento Excel nel quale è presente il database di rischi ferroviari. In output si riceve la lista automatizzata composta da tutti i rischi relativi al progetto. La seconda lista viene compilata "a mano" dal Project Manager con tutti i rischi che ritiene siano propri del progetto. Su questa viene fatto un check di copertura dagli analisti tramite il quale vengono associati ai rischi identificati dal PM quelli del database. Le due liste concorrono alla creazione della Watchlist durante una riunione con il Team di Commessa. Durante la riunione si svolge anche l'assessment, che avviene con la compilazione del Risk Register. Nel Risk Register vengono inseriti tutti i rischi che, a valle delle analisi svolte con la matrice Probabilità-Impatto (Kendrick, 2015), hanno un livello di rischio di valore MEDIO e ALTO[15].

Il presente studio si concentrerà esclusivamente sul processo di identificazione automatizzata di rischi senza entrare negli ambiti di: Check

[15] In alcuni casi dei Project Manager decidono di tenere in considerazione anche i rischi di livello BASSO

di copertura, Watchlist, Risk Register, Assessment né tanomeno il successivo Monitoraggio e Controllo.

Il Risk Office ha l'obiettivo di implementare l'Intelligenza Artificiale come terzo metodo per l'identificazione. Si ritiene, infatti, che l'identificazione tramite AI possa venire in forte aiuto nei progetti che non possono asserire al database di Italferr, il quale è composto principalmente da rischi d'ambito ferroviario. Nel Risk Office sono stati già fatti dei test sull'AI, in particolare, grazie alla tesi sperimentale "Applicazione di un'Intelligenza Artificiale di tipo LLM nel Project Management: limiti e potenzialità nell'identificazione dei rischi" (Milazzo, 2023). Da questa, si è evinto come l'Intelligenza Artificiale possa essere uno strumento per l'identificazione di nuovi scenari a partire da un insieme molto limitato di informazioni di input. Continuando a perseguire l'obiettivo di cui sopra si è deciso di svolgere, tramite l'IA, una serie di test di associazione uno a uno tra i rischi della lista automatizzata e un insieme di vulnerabilità, simulando l'associazione che dovrebbe avvenire tra i rischi identificati autonomamente dall'Intelligenza Artificiale. Per valutare se l'identificazione dell'AI e la conseguente associazione con le vulnerabilità sono da considerarsi buone per procedere con altri test si è deciso di costruire degli indici. Gli indici sono stati costruiti, in prima istanza, per valutare l'efficienza del processo di identificazione automatizzata di Italferr così che poi possano essere implementati nella valutazione dell'identificazione svolta dall'Intelligenza Artificiale. Lo scopo è di assicurarsi che il processo Italferr sia l'adatto benchmark per espandere il contesto di applicazione del PRM a nuovi settori e ambiti ingegneristici.

L'analisi sull'Intelligenza Artificiale non può essere svolta se non si conosce l'efficienza del processo di creazione della lista automatizzata,

quindi, dato che lungo lo svolgimento del processo vengono create più liste, si è deciso di valutare l'efficienza della sola lista automatizzata di rischi.

La lista automatizzata è il risultato dell'inserimento dell'analisi di contesto compilata dal Team di Commessa nel file di elaborazione progettato negli anni da Italferr. Come precedentemente spiegato, un rischio presente nel database sarà attivo (facente parte della lista) se e solo se tutti i fattori ad esso associati siano stati precedentemente attivati dal TdC.

La lista di scenari è composta da tutti gli scenari che possono realisticamente presentarsi e generare scostamenti sul grado di raggiungibilità degli obiettivi. La lista non viene creata con uno scopo decisionale, è il primo insieme di rischi individuali del progetto a disposizione degli analisti. Il processo di identificazione viene usato quotidianamente dal Risk Office di Italferr per svolgere le attività di PRM dei propri progetti. Negli anni sono state fatte diverse valutazioni dell'efficienza di processo, successivamente si è deciso di implementare l'approccio legato al miglioramento continuo. È mancata, quindi, negli ultimi tempi una valutazione che fotografasse il processo per rivalutarlo in funzione degli obiettivi di cui sopra. Valutare l'efficienza di questo strumento può essere utile per comprendere se e come debbano essere aggiunte modifiche e/o miglioramenti. Per avere informazioni che permettano un'analisi dell'efficienza si è scelto di costruire degli indici semplici ed esplicativi. Nello specifico, gli indici saranno di completezza e di assenza delle vulnerabilità.

Essendo l'implementazione dell'Intelligenza Artificiale l'obiettivo ultimo dell'elaborato si è deciso di presentare prima la costruzione e i

risultati degli indici di efficienza del processo e successivamente i risultati delle associazioni tra rischi e vulnerabilità fatti dall'IA.

4.1 Gli indici per l'analisi di efficienza della lista automatizzata

Per valutare l'efficienza del processo di creazione della lista di rischi individuali identificati si è scelto di utilizzare due indici principali:

- l'indice di completezza della lista automatizzata e
- l'indice di assenza delle vulnerabilità.

Il primo valuta la completezza della lista, quindi ricerca l'insieme di rischi che non sono stati identificati ma che avrebbero dovuto esserlo. Nell'ottica del Risk Management è noto come sia importante identificare, almeno all'inizio, un maggior numero di rischi considerando anche quelli che probabilmente verranno scartati o non faranno effettivamente parte del progetto. Il ragionamento risiede a partire dal concetto secondo cui è molto più facile eliminare un rischio non inerente che identificarne di nuovi che potrebbero essere stati dimenticati.

Vi è poi un indice di assenza delle vulnerabilità. Come presentato nel precedente capitolo, una vulnerabilità è un fattore di debolezza nel contesto del progetto. Si può associare ad un moltiplicatore di probabilità dell'accadimento di minacce. Si è deciso, quindi, di valutare quante vulnerabilità presenti nel progetto non sono associate a nessun rischio.

4.1.1 Il concetto di Vulnerabilità

Una vulnerabilità si può definire come "la condizione determinata da fattori o processi fisici, sociali, economici e ambientali che aumenta la suscettibilità di un processo/progetto all'impatto delle interferenze provenienti dal contesto e dagli stakeholder".

Una vulnerabilità in un progetto lo rende suscettibile a determinati eventi o catene di eventi che possono presentarsi durante il ciclo di vita di quest'ultimo. La relazione tra vulnerabilità e rischio è diretta, senza la prima se dovesse presentarsi il secondo, questo ha meno possibilità di manifestarsi come una vera e propria minaccia o opportunità. La mancanza di vulnerabilità impedisce l'accadimento dei rischi, mentre, al contrario, la loro presenza li rende impattanti sugli obiettivi.

Dal concetto di vulnerabilità parte l'analisi dell'efficienza del processo di identificazione automatizzata. In ogni analisi di contesto il TdC deve attivare tutte le vulnerabilità che crede essere presenti nel progetto in questione. Come detto precedentemente sono presenti molti altri fattori che concorrono all'attivazione di un rischio tra cui: stakeholder, attività, opere, fase del progetto e obiettivi. La presenza attiva di questi ultimi non genera un rischio se combinandoli tra di loro non si presenta una qualche vulnerabilità. Alternativamente ci si può aspettare che la presenza di una vulnerabilità che non è associata a nessun rischio (perché uno dei rimanenti fattori è disattivato) comunque possa mettere in difficoltà il progetto. Questo può avvenire se questa venisse sfruttata da un fattore di contesto differente da quelli ad essa associata nel database Italferr. È ragionevole, infatti, aspettarsi l'avvenimento di un rischio già presente nel database con una nuova configurazione oppure l'avvenimento di un rischio che non si è ancora mai presentato nei progetti di Italferr. Questo viene giustificato dalla decisione di inserire nel database i rischi nella loro configurazione più

frequente il che non impedisce una potenziale modifica della configurazione.

Il Risk Office non considera alcuni fattori più importanti di altri. Per creare un'analisi che segua un metodo logico, si è però deciso di dare un'importanza maggiore al concetto di vulnerabilità. Nel particolare a tutte le vulnerabilità attive ma associate a 0 rischi.

Le vulnerabilità identificate da Italferr sono 81 e quando si svolge l'identificazione automatizzata si riceve in output nella scheda a loro assegnata l'informazione del numero di rischi attivi associati a ognuna di esse.

Descrizione completa della Vulnerabilità	Attivo	Associati a Rischi
Vulnerabilità 1	0	0
Vulnerabilità 2	1	5
Vulnerabilità 3	1	0
Vulnerabilità 4	0	0
Vulnerabilità 5	0	0
Vulnerabilità 6	1	1
Vulnerabilità 7	1	0
Vulnerabilità 8	1	0
Vulnerabilità 9	1	2

Tabella 7 - Visualizzazione delle vulnerabilità dopo l'identificazione

Nella Tabella 1 sono evidenti le diverse tipologie di vulnerabilità in un progetto. Ci sono:

- vulnerabilità non attive, quindi non importanti e da scartare nell'analisi;

- vulnerabilità attive e associate a un certo numero di rischi;
- vulnerabilità attive e non associate a rischi.

Su queste ultime si concentra il focus dell'analisi. L'analisi di basa sull'assunto già espresso secondo cui se una vulnerabilità è presente ha un effetto di moltiplicatore della probabilità di accadimento di un rischio e in alcuni casi anche del suo potenziale impatto. Inoltre, si considera nelle condizioni di base dell'analisi la possibilità che durante la compilazione dell'analisi di contesto il TdC possa aver commesso errori di attivazione sia delle vulnerabilità che di altri fattori. Questa eventualità si considera solo nell'alternativa in cui l'errore sia di NON attivazione di fattori in realtà attivi e non nel caso in cui siano stati attivati fattori non presenti nel contesto del progetto. Nel secondo caso si genererebbero scenari di rischio attivi che comunque sarebbero eliminati nelle fasi successive del progetto.

4.2 L'indice di Assenza delle Vulnerabilità

L'indice di assenza delle vulnerabilità calcola in maniera semplice e immediata la percentuale di vulnerabilità attive con zero rischi associati sul totale delle vulnerabilità attive nel progetto fornisce la lista estesa di queste vulnerabilità. Le informazioni che si ricavano dall'indice servono al Risk Office per comprendere il livello di accuratezza dell'identificazione automatizzata in relazione alle vulnerabilità presenti nel progetto. Il concetto di vulnerabilità è uno dei più complessi da comprendere per il Team di Commessa. L'attivazione delle vulnerabilità risente maggiormente delle valutazioni soggettive del TdC sul progetto. Se attivare, ad esempio, un'attività è semplice, (se si dovrà svolgere l'attività "costruzione impianti" questa sarà attivata perché presente nella WBS) attivare una vulnerabilità come "Estrema difficoltà o sostanziale impossibilità, per l'Appaltatore, di espletare l'incarico nella sua interezza" implica avere una conoscenza

dell'Appaltatore tale da poter valutare l'incarico a lui assegnato in funzione di quelle che sono le sue possibilità operative. L'obiettivo dell'identificazione è coprire il più possibile le vulnerabilità attinenti al progetto. Si presenta quindi il duplice problema dell'attinenza di una vulnerabilità al progetto sopra espresso unito al problema di avere una buona associazione teorica tra vulnerabilità e il database degli scenari di rischio. Bisogna sottolineare, prima della costruzione dell'indice, come i progetti debbano essere divisi in due insiemi: i progetti in fase di progettazione e quelli in fase esecutiva. Per una questione di assenza di informazioni ci si aspetta che nei primi l'indice di assenza delle vulnerabilità sia maggiore e/o più volatile. Per le identificazioni svolte in fase di progettazione ci si aspettano risultati più consistenti e robusti con un valore medio dell'indice che tenda a diminuire.

4.2.1 Costruzione dell'Indice

L'indice prende in input solo ed esclusivamente la scheda Vulnerabilità del foglio Excel atto all'identificazione automatizzata.

Le vulnerabilità vengono associate ai vari livelli di tassonomia che sono suddivisi dal generale al particolare come segue:

- **Esterno/Interno**: suddivisione che informa se la vulnerabilità provenga entro i limiti del progetto o provenga da fattori esterni che potrebbero influenzarlo;
- **Contesto**: i contesti da cui possono provenire le vulnerabilità sono diversi e Italferr ha definito i successivi 7: Operativo, Contrattuale, Gestionale, Tecnologico, Ambientale, Politico e Sociale e Commerciale;

- **Elementi di complessità**: gli elementi di complessità si possono definire come gli aspetti del contesto che sono alla base degli insiemi specifici di vulnerabilità;
- **Fattore specifico**: i fattori specifici sono una particolarizzazione degli elementi di complessità che ne aumentano il livello di specificità
- **Vulnerabilità**: le vulnerabilità, descritte con un breve testo specifico, rappresentano l'ultimo livello della tassonomia. Sono 81.

Per ogni vulnerabilità, inoltre, si hanno le informazioni riguardo l'attivazione e il numero di rischi attivi a loro associate. Risultano d'interesse le vulnerabilità associate ad un gran numero di rischi e le vulnerabilità attive associate a 0 rischi o anche definite "attive e assenti". Riguardo le prime si considerano tutte quelle che sono associate ad almeno cinque o più rischi. Queste saranno critiche per il progetto e di forte interesse per il Risk Office in sede di Assessment, riuscire a gestire la vulnerabilità tramite la raccolta delle informazioni riguardanti gli attori che ne sono protagonisti e gestire soprattutto i rischi associate ad esse può generare un effetto positivo concatenato. Per quanto riguarda le vulnerabilità attive e assenti invece il focus si sposta nell'ambito della validità del processo automatizzato. Avere un gran numero di vulnerabilità che rientrino in questo insieme può essere dato da un problema comunicativo e di comprensione del TdC con il Risk Office sul concetto di vulnerabilità, oppure da problemi di scrittura e similitudini tra vulnerabilità. La lista vulnerabilità è stata creata cercando di soddisfare a pieno la tassonomia di Italferr. Questo, in altre parole, implica l'esistenza di vulnerabilità che non si sono mai presentate all'interno dei progetti ma che sono state comunque inserite nel database. Con questa configurazione si

crea un trade-off. Da un lato, la lista di vulnerabilità risulta essere completa e coerente con la tassonomia. Dall'altro, ragionando a partire dai livelli più alti della tassonomia, il PM potrebbe decidere di attivare in blocco tutte le singole vulnerabilità che fanno parte dell'insieme "Contrattuale" appartenente al livello di tassonomia Contesto, il quale contiene 16 vulnerabilità, semplicemente partendo da informazioni generiche sul progetto che riguardano problematiche sul contratto. Questa situazione comporterebbe sicuramente un aumento nel numero di vulnerabilità attive e assenti e anche, in parte minore, un aumento nel numero di rischi identificati.

4.2.1.1 Costruzione Analitica

Dal foglio delle vulnerabilità si estraggono, tramite una serie di interrogazioni di conteggio, dapprima tutte le vulnerabilità attive e successivamente l'insieme di vulnerabilità attive con 0 rischi associati.

N° Vuln. Attive	N° Vuln. Attive e Assenti
38	15

Tabella 8 - Conteggio delle Vulnerabilità

Successivamente si calcola tramite la seguente formula, il tasso di assenza delle vulnerabilità:

$$Indice\ di\ Assenza\ delle\ Vulnerabilità: \frac{N°\ Vulnerabilità\ Attive\ e\ Assenti}{N°\ Vulnerabilità\ Attive}$$

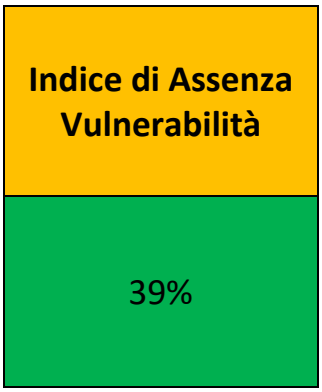

Tabella 9 - Indice Di Assenza delle Vulnerabilità

Alla cella in cui è presente l'indice vengono assegnate delle regole di colorazione in funzione del livello dell'indice stesso.

Si è deciso che la cella si colorerà simulando un semaforo in funzione delle seguenti soglie:

- Verde se: $Indice\ di\ Assenza\ Vulnerabilità \leq 50\%$
- Giallo se: $50\% < Indice\ di\ Assenza\ Vulnerabilità \leq 75\%$
- Rosso se: $Indice\ di\ Assenza\ Vulnerabilità > 75\%$

Le soglie sono state decise a valle dei primi risultati e confermate dalle analisi successive alla terminazione di tutti i test, insieme al Risk Office.

A lato è presente anche la lista con le descrizioni delle singole Vulnerabilità Attive e Assenti, così che gli analisti possano identificare pattern e legami, soprattutto a valle di nuove informazioni sul progetto. Ricordando la ciclicità del processo di PRM, si sottolinea come avere la lista aggiornata a fasi successive dell'avanzamento di progetto permette agli analisti di svolgere confronti tra le due liste.

Vulnerabilità attive e assenti
Contratto Committente-Appaltatore: Vulnerabilità 1
Contratto Committente-Italferr/Soggetto Tecnico: Vulnerabilità 2
Necessità di Coordinamento SO e Gruppi di Lavoro: Vulnerabilità 3
Sistema di Gestione Ambientale: Vulnerabilità 4
Sistema di Gestione Qualità: Vulnerabilità 5
Sistema di Gestione Salute e Sicurezza: Vulnerabilità 6
Complessa gestione di appaltatori e fornitori: Vulnerabilità 7
Complessità nella gestione del personale: Vulnerabilità 8
Complessità nella pianificazione: Vulnerabilità 9
Necessità di sottoporre il prodotto ad un ente che può chiedere modifiche: Vulnerabilità 10
Volatilità degli input: Vulnerabilità 11
Eventi naturali catastrofici avvenuti recentemente: Vulnerabilità 12
Interferenze con strutture/infrastrutture: Vulnerabilità 13
Tensioni Sociali: Vulnerabilità 14

Tabella 10 - Lista di vulnerabilità attive e assenti

La lista è stata presentata in tabella 4 con le vulnerabilità costruite come negli sheet di lavoro del Risk Office. Cioè:

"Fattore Specifico: Descrizione della vulnerabilità[16]".

[16] Le specifiche descrizioni sono state omesse

4.2.2 Risultati

Per valutare l'efficienza del processo in termini dell'assenza delle vulnerabilità all'interno della lista automatizzata di rischi identificati, sono stati presi in esame 21 progetti.

I progetti sono:

- 16 in fase di realizzazione e,
- 5 in fase di progettazione.

Nei risultati si è deciso di riportare anche le informazioni relative al numero di vulnerabilità attive per una migliore contestualizzazione.

Progetto	Fase del Progetto	Vulnerabilità Attive	Vulnerabilità attive associate a 0 rischi	Indice di assenza delle vulnerabilità
Progetto 1	Realizzazione	40	21	53%
Progetto 2	Realizzazione	55	25	45%
Progetto 3	Progettazione	44	18	41%
Progetto 4	Realizzazione	74	37	50%
Progetto 5	Realizzazione	74	37	50%
Progetto 6	Progettazione	69	38	55%
Progetto 7	Realizzazione	73	40	55%
Progetto 8	Realizzazione	72	34	47%
Progetto 9	Realizzazione	37	16	43%
Progetto 10	Realizzazione	40	21	53%
Progetto 11	Realizzazione	53	26	49%
Progetto 12	Realizzazione	57	29	51%
Progetto 13	Realizzazione	73	40	55%

Progetto 14	Realizzazione	71	42	59%
Progetto 15	Progettazione	48	25	52%
Progetto 16	Realizzazione	74	37	50%
Progetto 17	Realizzazione	16	3	19%
Progetto 18	Progettazione	67	34	51%
Progetto 19	Progettazione	66	34	52%
Progetto 20	Realizzazione	40	19	48%
Progetto 21	Realizzazione	72	34	47%

Tabella 11 - Risultati dell'indice di assenza delle vulnerabilità

4.2.3 Commenti

L'indice di assenza delle vulnerabilità presenta dei risultati che hanno una media pari al 48,73%. Lo studio svolto pone una grande importanza sulle vulnerabilità, quindi, i risultati, in prima istanza, sembrerebbero non essere ottimali. Un gran numero di vulnerabilità attive e non associate a dei rischi aumenta la vulnerabilità generale di progetto, soprattutto considerando che queste vulnerabilità verranno "dimenticate" dal TdC e dal Risk Office. Va anche detto che il Risk Office tende a tenere conto di tutto ciò che può avere anche un minimo impatto, quindi una volta svolta l'identificazione automatizzata si svolgono studi per comprendere a pieno il progetto in analisi e la lista stessa. Come già detto, il check di copertura della lista di rischi scritta manualmente dal TdC (il quale consiste

nell'associare rischi appartenenti al database a quelli scritti in linguaggio naturale per una questione di completezza) ha come risultato, in caso servisse, l'aggiunta di nuovi rischi nel database e nella lista identificata o nell'attivazione di rischi precedentemente non attivi. Una maggiore comprensione dei limiti del progetto ha sicuramente un effetto positivo, infatti, la consapevolezza dell'assenza di determinate vulnerabilità tiene in allerta il Risk Office nel caso in cui, cambiando il contesto, queste diventino parte integrante della creazione di nuovi rischi.

L'analisi dei risultati non si può limitare a quanto già descritto, in quanto, va ricordato che le vulnerabilità totali sono 81. Andando ad analizzare la media di vulnerabilità attive si trova che questa è pari a 57,85. Questo dato rapportato alle 81 vulnerabilità indica che i Team di Commessa dei progetti di Italferr attivano, mediamente, il 71,42% delle vulnerabilità. Se rapportiamo questi dati al fatto che la maggior parte dei progetti analizzati è in fase di realizzazione e che quindi circa la metà degli scenari di rischio, cioè quelli associati alla fase di progettazione (evidentemente superata), sono disattivati si conclude che una parte delle vulnerabilità, soprattutto quelle legate alle attività, quindi, ai rischi della progettazione non potranno avere rischi attivi a loro associate. Questo, in parte spiega i risultati ottenuti dall'indice.

Il motivo della grande percentuale di vulnerabilità attive che rende l'indice così elevato va anche imputato al significato di vulnerabilità. Il processo di identificazione ideato e utilizzato negli ultimi anni da Italferr è fortemente innovativo nell'ambito del Project Management e pone un forte peso sul concetto di vulnerabilità a prescindere dalla presenza o meno di rischi ad essa associati. Una vulnerabilità impone le condizioni di base perché un rischio ancora mai identificato o "dimenticato" si possa

presentare. I Team di Commessa sono esortati dal Risk Office ad attivare quante più vulnerabilità vedono nel progetto. Il fatto che poi molte rimangano "nell'etere" dell'identificazione non pone il progetto in una situazione di elevata pericolosità aprioristica. Al contrario, la coscienza della loro presenza aumenta l'approccio di totale controllo, nei limiti che il contesto permette, del progetto. Unendo quest'ultima analisi a come funziona l'attivazione di un rischio si trova un ulteriore giustificazione nel valore medio di assenza delle vulnerabilità. Come già detto, perché un rischio si attivi devono essere attivi tutti i fattori ad esso associati e, al contrario, perché non si attivi basta che solo uno di questi fattori non sia attivo. Si ricorda che i fattori associati ad un rischio sono:

- Fase del progetto;
- Obiettivo;
- Attività;
- Opera;
- Vulnerabilità;
- Stakeholder.

La mancata di attivazione di uno solo di questi fattori, perché non presenti nel contesto di progetto, aumenta le possibilità che delle vulnerabilità rimangano appunto attive ma associate a 0 rischi.

Concludendo l'analisi dei risultati bisogna sottolineare la forte coerenza nei risultati. Su 21 progetti presi in analisi il valore minimo dell'indice è stato il 19%, dato considerabile come un outlier dato che il secondo valore minimo è pari al 41% mentre il valore massimo è stato il 59%.

Il 96% percento dei progetti ha un valore dell'indice compreso tra il 40% e il 60%. La coerenza e la consistenza dei risultati rendono l'associazione rischi-vulnerabilità notevolmente efficiente.

4.3 L'indice di Completezza

Nello svolgere l'identificazione automatizza l'obiettivo principale è quello di presentare al Team di Commessa una lista di rischi che racchiuda tutti i possibili rischi che il progetto può incontrare durante il suo ciclo di vita. Il numero di rischi presenti lista è influenzato dal contesto e dalle valutazioni del TdC. Come assunto alla base dell'indice si è deciso di definire la completezza di una lista di rischi come segue:

"Una lista di rischi è completa se non si trovano rischi appartenenti al progetto non presenti al suo interno."

Un progetto per il quale si valuta aver selezionato tutti i rischi potenzialmente presenti avrà una lista di scenari di rischio completa. La definizione si rifà alle valutazioni di agenti interni al progetto, in particolare Risk Manager e Project Manager. Questo vincolo, sebbene possa far sembrare la definizione riduttiva e non generalmente applicabile, serve per rispettare uno dei concetti principali del Project Management secondo il quale ogni progetto è unico. A valle di similitudini che si possono trovare tra progetti, ci sono troppi fattori di contesto che rendono impossibile valutare la completezza generalmente.

Partendo dalla definizione, sono state svolte analisi sul funzionamento del processo di identificazione automatizzata per "simulare" una valutazione di RM e PM. Si è innanzitutto deciso che le associazioni tra fattori e rischi fossero tutte giuste, che il database sia completo e che le analisi di contesto compilate dal TdC non abbiano al loro interno errori. Per riassumere, l'assunto di base per il modello che costruisce l'indice è che tutte le informazioni a disposizione rappresentano perfettamente la realtà in cui è calato il progetto.

Come è stato già espressamente descritto, il processo rende un rischio attivo, quindi facente parte della lista, se e solo se tutti i fattori di contesto a lui connessi sono attivi. Si ricorda che i fattori sono:

- Fase del progetto,
- Obiettivo,
- Opera,
- Attività,
- Stakeholder,
- Vulnerabilità.

Per valutare la completezza della lista bisogna valutare tutte le informazioni di contesto. Sulla base di queste si fa una ricerca nel database cercando tutti quei rischi che dovrebbero far parte della lista di rischi. Il funzionamento dell'indice è molto semplice; viene riportata di seguito la formula per il calcolo:

$$Indice\ di\ Completezza = \frac{n°\ rischi\ dell'identificazione\ automatizzata}{n°\ rischi\ dell'identificazione\ automatizzata + n°\ di\ rischi\ da\ attenzionare}$$

maggiore è l'indice percentuale tra rischi trovati con l'identificazione automatizza e gli stessi sommati dal numero di rischi trovati con la ricerca e maggiore sarà il valore della completezza della lista automatizzata. Nel momento in cui si trova un rischio non attivo che dovrebbe far parte della lista l'indice aumenta e la completezza peggiora. In altre parole, per valutare la completezza si cercano quei rischi che si definiscono "da attenzionare". Questi potrebbero realisticamente far parte del progetto ma sono rimasti fuori data la loro combinazione di fattori specifici.

Si ricorda che sa anche solo un fattore specifico è "messo a 0", cioè viene considerato non facente parte del progetto da parte del Team di Commessa, il rischio sarà disattivato. Seguendo la logica dell'indice di assenza delle vulnerabilità anche l'indice di completezza sfrutta la vulnerabilità come concetto decisionale della presenza o assenza di un rischio tra quelli che devono essere "attenzionati". In particolare, fa riferimento alle vulnerabilità attive associate a zero rischi.

4.3.1 Costruzione dell'indice

L'indice è il risultato di una serie di operazioni che si svolgono tra i vari fogli appartenenti al file Excel che svolge l'identificazione automatizzata. Tra gli altri, si prendono in input le informazioni generate da alcuni passaggi che costituiscono la costruzione dell'indice di assenza delle vulnerabilità.

La costruzione si basa su una ricerca, tramite la formula FILTRO all'interno del foglio "Scenari" del file. Nel foglio "Scenari" sono presenti tutti i rischi del database con l'aggiunta di una colonna di check affianco ad ogni singolo fattore associato al rischio. Il valore del check sarà pari a 1 se il fattore è stato attivato nell'analisi di contesto e pari a 0 nel caso contrario.

Event-ID	Indice di Rilevanza	Fase	Chk	Attività	Chk	Opera di riferimento	Chk
XX	1	Realizzazione	1	Costruzione	1	Gallerie	1

Tabella 12 - Esempio Scenario Attivo (prima parte)

Potrebbe Succedere che	Obiettivo Impattato	Chk	Minacce / Opportunità	Vulnerabilità 1	Chk	Stakeholder 1	Chk
- potrebbero verificarsi delle frane in galleria - il verificarsi di tali eventi potrebbe allungare i tempi di consegna dell'opera	Tempi di realizzazione dell'Opera	1	Minaccia	Fragilità ambientale: Fragilità del territorio e pericolosità idraulica.	1	Appaltatore	1

Tabella 13 - Esempio Scenario Attivo (seconda parte)

Nelle tabelle 12 e 13 si può vedere come si presenta un rischio attivo appartenente al foglio "Scenari".

4.3.1.1 Filtrare la lista di rischi

Per filtrare la lista di rischi si è deciso usare in prima istanza quattro vincoli.

I vincoli per filtrare la lista sono:

- Indice di rilevanza deve essere pari a "0";
- La fase deve essere pari a "1";
- L'obiettivo deve essere pari a "1";
- Le vulnerabilità devono essere pari a "1";

Vengono quindi presi in considerazione tutti i rischi non attivi che hanno associata una combinazione di fattori che li rende potenzialmente appartenenti al progetto. Si è deciso di mantenere variabili le attività, le opere e gli stakeholder perché tra tutti sono quei fattori che possono venire considerati come più flessibili all'interno del progetto.

Contrariamente, la fase deve essere attiva, un rischio di progettazione in un progetto in fase di realizzazione non ha senso di esistere in quanto la prima è stata già superata.

L'obiettivo deve essere obbligatoriamente un obiettivo di progetto, un rischio che se dovesse presentarsi potrebbe peggiorare la redditività del progetto quando questa non viene considerata come obiettivo non può far parte della lista dei rischi. Le vulnerabilità devono essere attive perché, come già detto, sono assimilabili a dei moltiplicatori delle possibilità di accadimento di un rischio e, inoltre, hanno una funzione analitica per i passaggi di costruzione dell'indice successivi.

Event-ID	Indice di Rilevanza	Fase	Chk	Attività	Chk	Opera di riferimento	Chk
79	0	Tutti	1	Definizione Dati di Base	0	Tutte	1

Tabella 14 - Prima sezione di un Rischio appartenente al Passaggio Intermedio

Potrebbe Succedere che	Obiettivo Impattato	Chk	Minacce / Opportunità	Vulnerabilità 1	Chk
- il Committente potrebbe fornire input poco chiari od intempestivi (ad esempio per interventi non sufficientemente dettagliati) - la carenza di input certi potrebbe generare un mancato avvio o dei ritardi nelle attività	Tempi di realizzazione dell'Opera	1	Minaccia	Volatilità degli input: Incertezze nella Definizione dei Dati di Base.	1

Tabella 15 - Seconda sezione di un Rischio appartenente al Passaggio Intermedio

Vulnerabilità 2	Chk	Vulnerabilità 3	Chk	Vulnerabilità 4	Chk	Stakeholder 1	Chk	Stakeholder 2	Chk	Stakeholder 3	Chk
	1		1		1	Committente	1		1		1

Tabella 16 - Terza sezione di un Rischio appartenente al Passaggio Intermedio

4.3.1.2 La ricerca di corrispondenza tra vulnerabilità attive e assenti e vulnerabilità della lista filtrata

Le vulnerabilità sono il fattore sfruttato per creare la discrezione nella presenza o assenza di un dato rischio. Si è deciso di associare, per ogni

rischio appartenente all'insieme dei rischi filtrati del passaggio precedente, un calcolo della corrispondenza delle vulnerabilità a loro associate con le vulnerabilità facenti parte dell'insieme di vulnerabilità attive e assenti.

Le vulnerabilità attive e assenti sono l'insieme di vulnerabilità trovato in un passaggio intermedio della costruzione dell'indice di assenza delle vulnerabilità. Ciò che avviene è un confronto tra il testo delle vulnerabilità dei singoli rischi con i testi delle vulnerabilità dell'insieme "attive e assenti". Se si trova una corrispondenza positiva viene associato un valore pari a "1" nella colonna "Corrispondenza Vx" in caso contrario il valore associato sarà pari a "0".

Corrispondenza V 1	Corrispondenza V 2	Corrispondenza V 3
0	0	0
0	0	0
1	0	0

Tabella 17 - Corrispondenza tra Rischio e Vulnerabilità attiva associata a 0 Rischi

4.3.1.3 L'output dell'indice

Svolto il passaggio di corrispondenza tra le vulnerabilità si riportano nel foglio di output i soli rischi che avranno almeno una corrispondenza con la lista di vulnerabilità tramite una formula FILTRO.
La scelta della singola corrispondenza è dovuta dal fatto che il numero di vulnerabilità associate ai rischi varia da 1 a 3. Si è deciso che per i rischi associati a più d'una vulnerabilità (meno del 25%), una singola vulnerabilità attiva basta a renderli contestualizzati nel progetto a tal punto da essere quantomeno analizzati dagli analisti.

Event-ID	Indice di Rilevanza	Fase	Chk	Attività	Chk	Potrebbe Succedere che
132	0	Realizzazione	1	Costruzione	1	- alcune organizzazioni non governative potrebbero opporsi al progetto - le organizzazioni potrebbero intraprendere azioni di protesta - la gestione di queste proteste potrebbe rallentare le attività

Tabella 18 - Prima sezione del Rischio da Attenzionare

Obiettivo Impattato	Chk	Vulnerabilità 1	Chk	Stakeholder 1	Chk	Corrispondenza V 1	Corrispondenza V 2	Corrispondenza V 3
Tempi di realizzazione dell'Opera	1	Tensioni Sociali: Ostilità degli Stakeholder esterni al Progetto.	1	Organizzazioni non governative	0	1	0	0

Tabella 19 - Seconda sezione del Rischio da Attenzionare

Nell'esempio in tabelle 12-13 si può vedere come il numero di vulnerabilità associate sia solo una, la corrispondenza con la seconda e terza non può esserci. In questo esempio si fa notare come a essere disattivato sia lo stakeholder "organizzazioni non governative" quando è stato deciso dal TdC che la vulnerabilità "Ostilità degli stakholder esterni" fosse presente. La situazione mette chiaramente analisti e PM nella condizione di decidere se varrà la pena disattivare la vulnerabilità o attivare gli stakeholder.

A fianco della lista di rischi da attenzionare viene presentato l'output finale dell'indice cioè:

$$\frac{n° \, rischi \, dell'identificazione \, automatizzata}{n° \, rischi \, dell'identificazione \, automatizzata + n° \, di \, rischi \, da \, attenzionare}$$

Un esempio viene riportato nella tabella successiva.

Indice di completezza
96,72%

Tabella 20 - Indice di Completezza

4.3.2 Risultati

I risultati dei 21 progetti presi in analisi vengono presentati nella seguente tabella.

Progetto	Fase del Progetto	N° Rischi Identificati	Rischi da Attenzionare	Indice di Completezza
Progetto 1	Realizzazione	59	2	96,72%
Progetto 2	Realizzazione	78	4	95,12%
Progetto 3	Progettazione	68	2	97,14%
Progetto 4	Realizzazione	94	0	100,00%
Progetto 5	Realizzazione	94	0	100,00%
Progetto 6	Progettazione	77	5	93,90%
Progetto 7	Realizzazione	76	3	96,20%
Progetto 8	Realizzazione	78	2	97,50%
Progetto 9	Realizzazione	60	4	93,75%
Progetto 10	Realizzazione	60	2	96,77%
Progetto 11	Realizzazione	75	0	100,00%
Progetto 12	Realizzazione	73	1	98,65%
Progetto 13	Realizzazione	76	3	96,20%
Progetto 14	Realizzazione	67	7	90,54%
Progetto 15	Progettazione	52	8	86,67%
Progetto 16	Realizzazione	87	0	100,00%
Progetto 17	Realizzazione	39	0	100,00%
Progetto 18	Progettazione	82	2	97,62%
Progetto 19	Progettazione	74	2	97,37%
Progetto 20	Realizzazione	55	2	96,49%
Progetto 21	Realizzazione	78	2	97,50%

Tabella 21 - Risultati dell'Indice di Completezza

Quando l'analista riceverà in output il risultato dell'indice e le informazioni sui singoli rischi, dovrà studiare e comprendere se i rischi da

attenzionare siano da aggiungere o meno al progetto. Per fare questo, si dovranno svolgere delle valutazioni che tengono conto del contesto di progetto e delle opinioni del TdC. Si è deciso che per i progetti studiati la completezza, come per l'indice di assenza delle vulnerabilità verrà valutata in funzione di tre fasce che coloreranno la cella in funzione del risultato. In generale si può dire che la completezza della lista automatizzata sarà:

- Ottima se l'indice è $\geq 95\%$
- Buona se i rischi da attenzionare sono $90\% \leq x < 95\%$
- Limitata se i rischi da attenzionare sono $< 90\%$

La scelta delle tre fasce di valutazione della completezza è stata fatta a valle dei primi test. Questa scelta è in linea con i risultati conseguiti da Italferr negli ultimi anni con il PRM nei progetti in cui ha partecipato attivamente.

4.3.3 Commenti

Nel valutare l'efficienza del processo di identificazione automatizzata, l'indice di completezza è di grande aiuto. Come già detto trovare anche solo un rischio, che dovrebbe far parte della lista, al di fuori di questa compromette la qualità del processo e, successivamente, pone il progetto in una posizione di ulteriore incertezza. Nel momento in cui dato rischio si dovesse presentare dovrà essere trattato immediatamente come una issue e il suo impatto non potrà essere evitato.

I risultati dell'indice di completezza, considerando le soglie di valutazione precedentemente esposte, sono i seguenti:

- 17 progetti nella fascia di OTTIMA completezza;
- 3 progetti nella fascia di BUONA completezza;
- 1 progetti nella fascia di LIMITATA completezza.

Inoltre, il numero medio di rischi da attenzionare è 2,43.

Si può immediatamente constatare come i risultati dell'indice applicato al processo di Italferr siano molto soddisfacenti. Per la maggior parte dei progetti sono stati identificati la quasi totalità dei rischi e questo, al netto delle valutazioni specifiche su quelli da attenzionare, rende molto alta la possibilità che questi non incappino in issue o in situazioni di grave incertezza.

Se si associano i risultati al numero medio di rischi identificati (71,52) questi risultano essere ancor più positivi. Il processo di identificazione automatizzata di Italferr assicura un'elevata efficienza nel cercare e trovare i rischi di progetto.

Facendo riferimento ai risultati dell'indice di assenza delle vulnerabilità si può aggiungere come l'elevata presenza di vulnerabilità non associate ad alcun rischio non metta in difficoltà l'indice di completezza, il quale usa proprio questa tipologia di vulnerabilità per trovare i rischi da attenzionare. Per completare l'analisi dei risultati si aggiunge che, svolgendo delle valutazioni in concomitanza degli analisti di Italferr si è eliminato circa il 30% dei rischi trovati dall'indice. Questo risultato porta con sé una doppia valutazione.

- Prima di tutto, significa che gli effettivi rischi da attenzionare diminuiscono migliorando ancora l'efficienza del processo e il risultato dell'indice;

- Inoltre, significa che i rischi trovati dall'indice dovranno essere valutati dal PM e dal TdC e, quindi, rendono l'indice uno strumento di effettivo supporto al Project Risk Management di Italferr.

4.4 L'efficienza del processo di identificazione tramite l'intelligenza artificiale

Tra gli obiettivi di medio periodo del Risk Office in Italferr l'implementazione dell'intelligenza artificiale all'interno dei processi di Risk Management è uno dei più importanti. L'IA si può sfruttare per:

- l'ottimizzazione dell'identificazione dei rischi;
- il supporto dei documenti interni;
- la valutazione del Risk Register;
- l'analisi dei dati (in termini di correlazione, classificazione, semplificazione, monitoraggio e controllo);
- il supporto delle decisioni strategiche.

Prima di poter comprendere come l'intelligenza artificiale può essere implementata operativamente all'interno dei vari processi del Risk Office c'è bisogno di svolgere una serie di test. Questi devono verificare le potenzialità d'utilizzo dell'IA e quanto si potrebbe efficientare il lavoro svolto quotidianamente aumentandone la velocità senza peggiorare la qualità dei risultati che ad oggi il Risk Office riesce ad ottenere autonomamente.

4.4.1 La scelta sull'intelligenza artificiale

Il Risk Office ha già iniziato a svolgere dei test sull'intelligenza artificiale. Nel particolare, sono stati svolti dei test con l'intento di "ottenere scenari di

rischio quanti più vicini a quelli identificati dall'azienda, partendo dagli stessi input". (Milazzo, 2023) Lo studio si è incentrato nell'utilizzo di Large Language Model (Zhao et al, 2023), cioè modelli linguistici di deep learning che permettono l'interazione tramite il linguaggio scritto.

Tra i modelli utilizzati si trovano: ChatGPT, ChatSonic e Bard. Tra questi tre, i migliori risultati li ha avuti ChatGPT e per questo motivo l'analisi di efficienza del processo di identificazione automatizzata è stata svolta esclusivamente con questo LLM.

4.4.2 L'analisi proposta

L'obiettivo dello studio è comprendere se i risultati degli indici sopra descritti sono ragionevolmente raggiungibili tramite ChatGPT. Inoltre, gli indici sono stati costruiti anche per valutare quella che sarà la futura identificazione tramite intelligenza artificiale. Questa ricalcherà l'identificazione automatizzata, quindi gli indici saranno di grande supporto per l'implementazione. Si darà in input un sottoinsieme dei dati iniziali di contesto e tramite delle richieste specifiche si comprenderà quanto l'IA riesca a replicare i risultati precedentemente ottenuti.

4.4.3 Test sull'indice di assenza delle vulnerabilità

Con l'intento di voler implementare l'IA nel processo di identificazione automatizzata si è scelto di svolgere dei test sull'associazione tra rischi e vulnerabilità. Il test si compone dell'inserimento in input di un insieme di rischi e di un insieme di vulnerabilità chiedendo quindi a ChatGPT di associare ogni rischio del primo insieme ad una e una sola vulnerabilità.

I dati inseriti sono da considerare di ottima qualità perché sono il risultato delle identificazioni automatizzate dei rischi svolte negli ultimi due anni (2022-2023) in azienda.

Questi sono stati poi presentate ai vari Team di Commessa dei progetti effettivamente svolti da Italferr e da tutte le altre aziende del gruppo Ferrovie dello Stato partecipanti. Una volta inseriti i due insiemi di dati e richiesta l'associazione, si confrontano le associazioni dell'IA con quelle presenti in database. Chiaramente, più le associazioni saranno coerenti con quelle del database e migliori saranno i risultati del test.

4.4.3.1 Input

Per svolgere il test sono stati presi casualmente sette progetti tra quelli studiati precedentemente per valutare l'efficienza del progetto. Per ognuno di questi è stata estratta la lista automatizzata, composta in media da più di 70 rischi e, da queste, ne sono stati estratti tre in maniera completamente casuale. In aggiunta sono state prese nove vulnerabilità per ogni progetto con il seguente criterio:

- Le tre vulnerabilità appartenenti agli scenari di rischio casualmente selezionati;
- Tre vulnerabilità aventi in comune lo stesso fattore specifico delle tre precedenti (si ricorda che il fattore specifico è il livello di tassonomia immediatamente superiore alla descrizione della vulnerabilità);
- Tre vulnerabilità completamente casuali;

Inoltre, la scelta delle vulnerabilità da inserire nel prompt è stata fatta considerando anche le "vulnerabilità attive", le "vulnerabilità non attive" e le "vulnerabilità attive e associate a 0 rischi". Non considerando le tre vulnerabilità associate ai rischi scelti, rimangono sei vulnerabilità. Queste sono state distribuite nel modo seguente:

- Due non attive, quindi non facenti parte del contesto di progetto;

- Due attive e associate a 0 rischi, quindi presenti nel contesto di progetto ma non presenti nei rischi della lista automatizzata;
- Due attive e associate a n-rischi. Presenti, quindi, sia nel contesto che nella lista automatizzata.

Trovati i due insiemi si è cercato il prompt adatto per fare sì che ChatGPT associasse in maniera univoca una sola vulnerabilità ad ogni rischio. Per riuscirci è stata cambiata la struttura di ogni singolo scenario di rischio[17].

Per semplificare l'analisi da parte di ChatGPT si è deciso di associare una lettera ad ogni rischio e un numero ad ogni vulnerabilità, così che in output si ricevano le combinazioni lettera-numero. Questo ha generato qualche problema, in quanto, le combinazioni in output, a prescindere dalla vulnerabilità scelta, non rispettavano l'ordine numerico assegnato.

Le vulnerabilità sono state elencate in maniera totalmente casuale, così da non creare predicibilità nelle risposte giuste. Inoltre, per quanto questo non abbia un impatto considerevole, si è deciso di svolgere i test sui sette progetti creando ogni volta una nuova discussione, per simulare un "ambiente asettico" per l'IA.

Per avere dei risultati che non provenissero da una singola iterazione, nella quale il caso e l'incertezza potrebbero influenzarli, si è deciso di ripetere il test altre tre volte cambiando le 6 vulnerabilità aggiuntive.

[17] Nel database Italferr i rischi sono suddivisi in più frasi, da dei "trattini". I trattini rendono complessa, per l'IA, la comprensione dello scenario. Infatti, tenendoli all'interno del prompt viene considerata solo ed esclusivamente la frase successiva al primo trattino. Togliendoli, senza intaccare il senso della frase, tramite una semplice sostituzione con delle virgole il problema viene risolto.

4.4.3.2 Prompt

Il prompt funzionante per lo scopo dello studio è il seguente:

"Il primo insieme è composto da tre elementi A, B e C:

A: "*primo rischio"*

B: "*secondo rischio"*

C: *"terzo rischio"*

Il secondo insieme invece è composto da 9 elementi numerati da 1 a 9:

1: *"prima vulnerabilità"*

2: *"seconda vulnerabilità"*

3: *"terza vulnerabilità"*

4: *"quarta vulnerabilità"*

5: *"quinta vulnerabilità"*

6: *"sesta vulnerabilità"*

7: *"settima vulnerabilità"*

8: *"ottava vulnerabilità"*

9: *"nona vulnerabilità"*

Riesci ad associare un singolo elemento del secondo insieme a ogni elemento del primo? L'associazione da fare deve essere la più sensata da un punto di vista logico."

4.4.3.3 Risultati

I primi risultati dell'associazione tra rischi e vulnerabilità svolte sono presentati nelle prossime quattro tabelle. I valori che il tasso di associazione può ottenere sono 3:

- 33% se l'associazione è corretta per un solo rischio di input;
- 67% se l'associazione è corretta per due rischi di input;
- 100% se l'associazione è corretta per tutti e tre i rischi di input.

A valle di ogni test verrà riportato il valore medio dell'associazione dell'insieme dei sette progetti.

4.4.3.3.1 Primo Test

I risultati del primo test svolto sui sette progetti sono i seguenti:

Progetto	Tasso di Associazione
P1	67%
P2	33%
P3	67%
P4	67%
P5	67%
P6	67%
P7	100%

Tabella 22 - Risultati primo test con l'IA

Valore medio del primo test: **67%**

4.4.3.3.2 Secondo Test

I risultati del secondo test svolto sui sette progetti sono i seguenti:

Progetto	Tasso di Associazione
P1	67%
P2	67%
P3	67%
P4	100%
P5	100%
P6	67%
P7	100%

Tabella 23 - Risultati secondo test con l'IA

Valore medio del secondo test: **81%**

4.4.3.3.3 Terzo test

I risultati del terzo test svolto sui sette progetti sono i seguenti:

Progetto	Tasso di Associazione
P1	67%
P2	33%
P3	67%
P4	67%
P5	100%
P6	67%
P7	100%

Tabella 24 - Risultati terzo test con l'IA

Valore medio del terzo test: 72%

4.4.3.3.4 Quarto test

I risultati del quarto test svolto sui sette progetti sono i seguenti:

Progetto	Tasso di Associazione
P1	67%
P2	67%
P3	67%
P4	100%
P5	67%
P6	67%
P7	100%

Tabella 25 - Risultati quarto test con l'IA

Valore medio del quarto test: 76%

I risultati sono stati presi considerandone la media e riportati nel grafico successivo per una migliore visualizzazione.

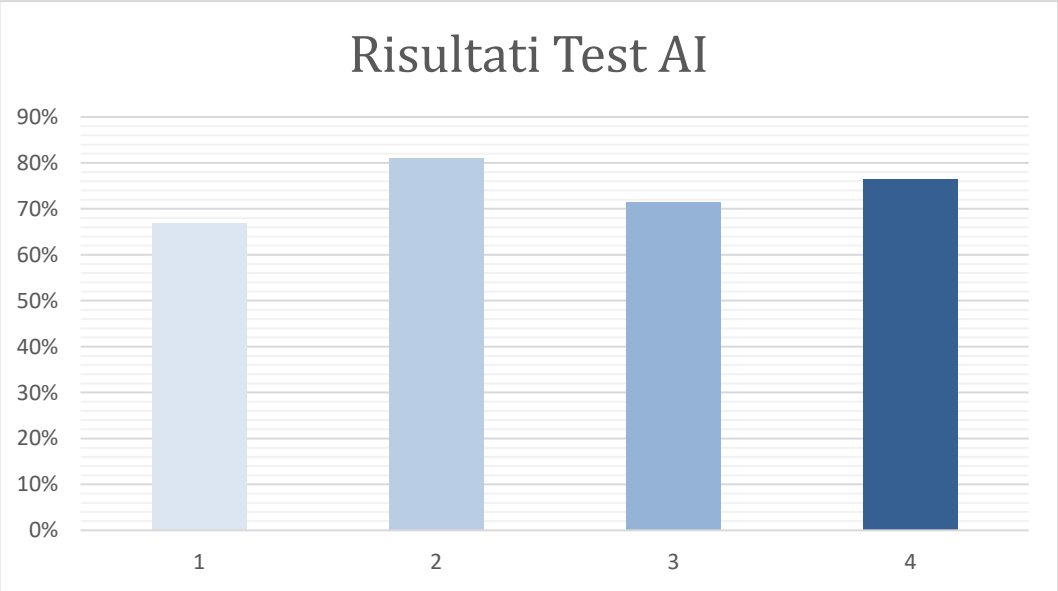

Figura 7 - Istogramma della media dei test con l'IA

4.4.3.4 Commenti

Considerando che l'IA non è stata precedentemente addestrata a rispondere alle richieste fatte, i risultati sono ottimi. La totale casualità dei progetti, dei rischi e delle vulnerabilità scelte unita alla ripetizione dei test evidenzia come la strutturazione del database di Italferr e l'associazione tra rischi e vulnerabilità sia facilmente comprensibile da un'intelligenza artificiale non precedentemente addestrata. Questo permetterà sicuramente al Risk Office di sfruttare l'Intelligenza Artificiale per svolgere nuove identificazioni e di sfruttare le sue potenzialità negli step del PRM successivi all'identificazione.

La varianza nei risultati dei quattro test è spiegata dalla decisione di cambiare le sei vulnerabilità inserite in input. Mantenendo sempre le stesse in output i risultati non sono cambiati, per questo è stato deciso di modificare leggermente il contesto (leggermente perché comunque sono stati rispettati i vincoli sulle vulnerabilità presentati in 4.4.3.1).

Per quanto riguarda gli errori commessi si analizzano le motivazioni come segue:

- La maggior parte degli errori nell'associazione si sono presentati a valle di una confusione dell'intelligenza artificiale con il fattore specifico. L'IA ha associato la vulnerabilità errata ma con lo stesso fattore specifico (si ricorda essere il livello immediatamente superiore della tassonomia) che si è scelto di inserire intenzionalmente per provare a confonderla.

Gli altri errori nelle associazioni sono avvenuti per tutti i rischi che non presentavano un collegamento diretto con la giusta vulnerabilità loro associata nel database. La mancanza di una parola specifica in comune, o comunque un concetto abbastanza semplice che legasse rischio e vulnerabilità ha fatto in modo che l'IA scegliesse la vulnerabilità da

associare in alcuni casi in maniera casuale e nei restanti soddisfacentemente ma errando.

Conclusioni

Con l'elaborato si è cercato di effettuare nuovi passi avanti verso l'implementazione dell'Intelligenza Artificiale nei processi di Risk Management di Italferr. Per avere i mezzi necessari allo svolgimento del lavoro è stata utile un estesa formazione sui concetti di rischio, Project Risk Management e, infine, sull'Identificazione dei rischi.

La base di partenza dello studio sperimentale svolto sono stati i risultati già ottenuti in Italferr riguardo la possibilità di riuscire a identificare una lista di rischi tramite un'Intelligenza Artificiale di tipo LLM. Il processo di identificazione in Italferr viene svolto con due metodologie. L'identificazione automatizza e l'identificazione svolta autonomamente dal Project Manager. La prima è stata fortemente utilizzata per poter perseguire l'obiettivo di implementazione dell'IA.

Lo studio sperimentale è partito dal concetto di vulnerabilità, cioè quel fattore di debolezza del contesto che può essere sfruttato perché si presentino degli scenari di rischio. Si è deciso di comprendere se, la vulnerabilità (centrale per l'identificazione automatizzata) fosse concettualmente comprensibile dall'intelligenza artificiale. Inoltre, sono stati sviluppati degli indici per il processo di identificazione automatizza che possono essere direttamente usati sui risultati dell'IA. Nell'elaborato sono stati presentati prima gli indici e poi i testi sull'Intelligenza Artificiale. Gli indici creati sono: l'indice di assenza delle vulnerabilità che trova quante vulnerabilità non sono presenti nella lista automatizzata sul totale di vulnerabilità presenti nel progetto e l'indice di completezza, un indice percentuale che descrive il livello di completezza della lista automatizzata. Entrambi sfruttano le vulnerabilità attive e associate a nessun rischio come strumento primario per la loro costruzione.

I risultati, in linea con quelli conseguiti da Italferr negli ultimi anni hanno mostrato un livello di efficienza di processo molto elevato. Il loro scopo finale però è quello di essere usati per valutare la qualità delle liste di rischi identificate tramite l'IA. I test con l'Intelligenza Artificiale (nel particolare ChatGPT) sono stati svolti con l'obiettivo di capire se questa, senza alcun tipo di addestramento riuscisse ad associare rischi e vulnerabilità.

I risultati, considerando il contesto sono stati ottimi. Se con i primi studi si è potuto dimostrare che l'IA è un ottimo strumento per l'identificazione, con il presente elaborato è stato fatto un importante passo avanti, perché ora sarà possibile valutare la qualità delle liste di rischi, sfruttando la struttura del preesistente e altamente efficiente database Italferr. Questo elaborato non è altro che un ulteriore punto di partenza per nuovi studi. Ci si riferisce alla possibilità di portare avanti test che arrivino alla valutazione dei Risk Register tramite l'IA, ma, soprattutto alla possibilità di svolgere analisi di rischio in nuovi settori, ancora mai esplorati da Italferr. Il prossimo passo sarà infatti quello di industrializzare l'Intelligenza Artificiale nel PRM rendendola il terzo strumento per l'identificazione in Italferr.

Bibliografia

Apostolakis G.E . (2004). "How useful is quantitative risk assessment?". *Risk Analysis*, 24 (3) : 515-520.

Aven T. (2012). "The risk concept—historical and recent development trends". *Reliability Engineering & System Safety*, 99: 33-44.

Ballou D., Pazer H. (2003). Modeling completeness versus consistency tradeoffs in information decision contexts. *IEEE Transactions on Knowledge and Data Engineering*, 240-243.

Baltussen G., Van den Assem M. J. e Van Dolder D. (2014). "Risky Choices in the Limelight". *Review of Economics and Statistics*, 98 (2): 318-332.

Baumeister R. F. e Tierney J. (2011). *Willpower: Rediscovering the Greatest Human Strength.* New York: Penguin Books.

Berlinger E. e Vàradi K. (2015). "Risk Appetite". *Public Finance Quarterly*, 60(1): 49-62.

Bernstein P.L. (1995). "Risk as a History of Ideas". *Financial Analysts Journal*, 51: 7-11.

Bernstein P.L. (1996). *Against the Gods. The Remarkable Story of Risk.* New York: John Wiley & sons.

Birkmann J. (2007). "Risk and vulnerability indicators at different scales:Applicability, usefulness and policy implications". *Environmental Hazards*, 7: 20-31.

Bouchard T. J. Jr. (1970). Personality, Problem Solving Procedures and Performance in Small Groups. *Journal of Applied Psychology*.

Cagliano A.C., Grimaldi S. e Rafele C. . (2014). Cagliano A.C., Grimal"Choosing project risk management techniques A theoretical framework". *Journal of Risk Research*, 18(2): 232-248.

Cardano G. (1525). *Liber de ludo aleae.* Edizione a cura di Tamborini M., Milano: Franco Angeli (2006).

Chapman C. e Ward S. (2003). *Project Risk Management: Processes, Techniques and Insights. (2°ed.).* John Wiley & Sons Inc.

Chapman R. J. (1998). The effectiveness of working group risk identification and assessment techniques. *International Journal of Project Management*.

Chen C., Cho M., Huang H. (2016). Development of Energy Cloud for Energy Saving of Kaohsiung City. *3rd International Conference on Green Technology and Sustainable Development (GTSD)*, 39-44.

Commissione Europea. (2005, novembre 17). Libro Verde relativo a un programma europeo per la protezione delle Infrastrutture Critiche. Bruxelles.

Covello V.T e Mumpower J. (1985). "Risk Analysis and Risk Management: An Historical Perspective". *Risk Analysis*, 5: 103-120.

Crockford G. (1982). "The Bibliography and History of Risk Management: Some Preliminary Observation". *The Geneva Papers on Risk and Insurance - Issues and Practice*, 7: 169-179.

da Silva L.H.R., Crispim J.A. (2014). "The project risk management process, a preliminary study". *Procedia Technology*, 16 : 943-949.

DAMA International. (2020). *DMBOK.* Technics Publications.

Delbecq A. L. (1968). *The World within the Span of Control Managerial Behaviour in groups of Varied Size.* Business Horizons.

Departement of Defense. (1993). *Military Standard System Safety Program Requirement "MIL-STD-882C" .*

Dobelli R. (2013). *The Art of Thinking Clearly.* New York: Harper USA.

Dunović I.B, Radujković M., Vukomanović M. . (2013). "Risk register development and implementation for construction projects". *GRAĐEVINAR*, 65: 23-35.

Fischhoff B. e Kadvany J. (2011). *Risk: A Very Short Introduction.* Oxford: OUP Oxford.

Fisher U., Castagna L.G., Violette D.M. (1989). "The Value of Reducing Risks of Death: A Note on New Evidence". *Journal of Policy Analysis and Management*, 8(1): 88-100.

Flage R., Aven T. . (2015). "Emerging risk – Conceptual definition and a relation to black swan". *Reliability Engineering and System Safety*, 144: 61-67.

Giddens A. (1990). *The consequence of modernity.* Stanford: Stanford University Press.

Goncalves M., Heda R. (2014). *Risk Management for Project Managers.* New York, USA: ASME.

Graunt J. (1662). *Natural and political observations mentioned in a following index, and made upon the bills of mortality.* Londra: Royal Society.

Hillson D. (1997). "Towards a risk maturity model". *The International Journal of Project & Business Risk Management*, 1(1): 35-45.

Hillson D. (2002). "Extending the risk process to manage opportunities". *International Journal of Project Management*, 20: 235-240.

Hillson D. (2002). Use a Risk Breakdown Structure (RBS) to understand your risks. *Project Management Institute Annual Seminars & Symposium.* San Antonio: Project Management Institute.

Hillson D. (2012). *Understanding Risk Appetite.* Dal sito https://www.youtube.com/watch?v=JtM68YIS19o&t=2589s&ab_channel=RiskDoctorVideo: (visitato il 28 marzo 2023).

Hulett D. T. (2001). "Key characteristics of a mature risk management process". *Proceedings of the European Project Management Conference/PMI Europe*.

Institute of Risk Management (IRM). (2003). *Standard di Risk Management.* Bruxelles: FERMA.

International Standards Organization (ISO). (2009). *ISO 73 – Risk Management Vocabulary.*

International Standards Organization (ISO). (2015). *ISO 31000:2015 - Risk management.*

International Standards Organization (ISO). (2018). *ISO 31000:2018 - Risk management [ebook].* www.iso.org.

International Standards Organization (ISO). (2019). *IEC 31010:2019.*

International Standards Organization (ISO). (2019). ISO 31010:2019.

ISACA. (2012). *CISM review manual.* Isaca.

ISO. (2018). *ISO 31000.* ISO.

Jaeger C., Renn O., Rosa E. e Webler, T. (2002). *Risk and Rational Action.* Londra: Earthscan.

Jarke M., Lenzerini M., Vassiladis P. Vassiliou Y. (1995). *Fundamentals of Data Warehouses.* Springer.

Judah S., Duncan A. D., Chien M., Friedman T. (2020). *5 Steps to Build a Business Case for Continuous Data Quality Assurance.* Gartner.

Kahn B.K., Strong D.M., Wang R.Y. (2002). "Information quality benchmarks: product and service performance". *Communications of the ACM*, 45(4) : 184-193.

Kahneman D. e Tversky A. (1979). "Prospect Theory: An Analysis of Decision under Risk". *Econometrica*, 47(2) : 263-292.

Kahneman D. e Tversky A. (1979). Prospect Theory: An Analysis of Decision under Risk. *Econometrica*, Vol. 47, No. 2 : 263-292.

Kloman H.F. (2010). *A brief history of risk management. In Fraser J. e Simkins B.J., Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives.* John Wiley & Sons Inc.

Kloman H.F. (2010). A brief history of risk management. *Enterprise risk management: Today's leading research and best practices for tomorrow's executives*, 9-29.

Knight F. H. (1921). *Risk, uncertainty and profit.* Boston: Houghton Mifflin.

Kontogiannis, T., Leva, M.C., Balfe, N. (2017). "Total Safety Management: Principles, Processes and Methods". *Safety Science*, 100(b): 128-142.

Leva M.C., BalfeN., McAleer B., Rocke M. . (2017). "Risk registers Structuring data collection to develop risk intelligence". *Safety Science*, 100(b): 143-156.

Lind N. C. (1994). "Target Reliability Levels from Social Indicators". *Structural Safety and Reliability*, 1897-1904.

Martinovičová D., Beranová M., Polák J., Drdla M . (2010). Theoretical aspects of risks categorisation. *Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis*, 58(3):131-136.

Mastrobuono G. (2023). L'approccio al rischio in Italferr. *Qualità*.

Megan M. Grime, George Wright. (2016). Delphi Method. *WIley StatsRef: Statistics Reference Online*.

Melis F. (1975). *Origini e sviluppi delle Assicurazioni in Italia.* Roma: Istituto Nazionale delle Assicurazioni.

Ministero delle Infrastrutture e dei Trasporti. (2022, luglio 4). *Opere pubbliche: 379 opere incompiute, 64 in meno rispetto al 2020 (-14,4%)*. Tratto da mit.gov.it: https://www.mit.gov.it/comunicazione/news/opere-pubbliche-379-opere-incompiute-64-meno-rispetto-al-2020-144

Minsky H. P. (1992). *The Financial Instability Hypothesis.* New York: The Jerome Levy Economics Institute of Bard College.

Monferini et al. (2013). A compound methodology to assess the impact of human and organizational factors impact on the risk level of hazardous industrial plants. *Reliability Engineering & System Safety*, 280-289.

Morgan J.P. (1995). *RiskMetrics—Technical Document.* New York: Morgan Guaranty Trust Company.

Morris P.W.G e Hough G.H. (1987). *The anatomy of major projects: a study of the reality of project management.* Chichester: Wiley & Sons Ltd.

Müller D., Te Y., Jain P. (2017). Improving data quality through high precision gender categorization. *IEEE International Conference on Big Data*, 2628-2636.

Nonino F., Tonchia S. (2013). *La guida del Sole 24 Ore al Project Management.* Milano: IlSole24Ore.

Osborn Alex F. (1953). *Applied Imagination.* New York: Scribner.

Patterson F.D., Neailey K. (2002). "A Risk Register Database System to aid the management of project risk". *International Journal of Project Management* , 20: 365-374.

Pergiovanni V. (1965). "Norme, scienza e pratica giuridica tra Genova e l'Occidente medievale e moderno". *Annali della Facoltà di Giurisprudenza dell'Università di Genova*, 4: 230-275.

Pirozzi M. (2020). *la prospettiva degli stakeholders.* Milano: Franco Angeli.

PMI. (2009). *Practice Standard for Project Risk Management.* Newtown Square, Pennsylvania USA: Project Management Institute, Inc.

PMI. (2017). *Guida al Project Management Body of Knowledge (Guida al PMBOK®). (6° ed.).* Pennsylvania: PMI, Inc.

Porter M.E. e Kramer M.R. (2011). "Creating Shared Value - How to reinvent capitalism and unleash a wave of innovation and growth". *Harvard Business Review*, 89: 62-77.

Proença D., Estevens J., Vieira R. e Borbinha J. (2017). "Risk Management: A Maturity Model Based on ISO 31000". *IEEE 19th Conference on Business Informatics (CBI)*, 99-108.

Redman T.C. (1996). *Data quality for the information age.* Boston, MA: Artech House.

Renn O. . (2004). "Perception of risks". *Toxicology letters*, 149 (1-3) : 405-413.

Rinaldi S.M., Peerenboom J.P., Kelly T.k. (2001). Identify, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21(6) : 11-25.

Slovic P. (2000). *The perception of risk.* New Tork: Taylor & Francis.

Szymanski P. (2017, dicembre 1). "Risk Management in construction projects". *Procedia Engineering*, 208:174-182.

Thaler R. H. e Johnson E. J. (1990). "Gambling with the House Money and Trying to Break Even: The Effects of Prior Outcomes". *Management Science*, 36 (6): 643-660.

Turner J.R. e Müller R. (2004). "Communication and co-operation on projects between the project owner as principal and the project manager as agent". *European Management Journal*, 22 (3) : 327-336.

United Nations International Strategy for Disaster Reduction (UN/ISDR). (2004). *Living with Risk. A Global Review of Disaster ReductionInitiatives.*

Ginevra: United Nations International Strategy for Disaster Reduction (UN/ISDR),2004. Livin UN Publications.

Von Neumann J. e Morgenstern O. (1944). *Theory of Games and Economic Behavior.* New Jersey: Princeton University Press.

Wang H. (2021). "Assessing the Effects of Applying Different Simulation Models on Resilience Evaluation of Critical Infrastructure Systems". *IEEE 3rd International Conference on Frontiers Technology of Information and Computer (ICFTIC).*

Ward S. (1999). "Requirements for an effective project risk management process". *Project Management Journal*, 30(3): 37-43.

Warner F. (1992). *Risk: Analysis, Perception and Management.* Londra: The Royal Society.

Williamson B. (2019). *Lo standard per la gestione del rischio in portafogli, programmi e progetti.* Project Management Institute (PMI).