Safety Risk Management

ISO 31000, ISO 45001, OHSAS 18001

Erica Blasizza, Andrea Rotella

Wolters Kluwer

Presentazione

I costanti cambiamenti sociali, politici, tecnologici, economici che avvengono attorno a noi, impongono un costante adattamento alle mutate condizioni; come tutte le evoluzioni, sia il cambiamento che il necessario processo di adattamento sono forieri di rischi e ciò è vero tanto per le persone quanto per le organizzazioni.

Sebbene quasi nessuno ragioni in questi termini quando opera una scelta, il concetto di rischio è proprio l'elemento centrale.

È una realtà faticosa da accettare, ma sono proprio i rischi, in particolare quelli che possono produrre esiti positivi, che guidano i comportamenti delle aziende ed i mercati: i rischi non nascondono solo lati negativi.

L'errore sarebbe quello di concentrarsi solo sull'uno o sull'altro, negandosi le opportunità che il rischio annida al proprio interno o esponendosi pericolosamente alle conseguenze peggiori del rischio.

E, pur volendo, sarebbe impossibile sottrarsi alla loro presenza: nulla è gratis e dove è presente la possibilità di un risultato, si insidia la possibilità di una perdita.

La scelta è tra governare o essere governati dal rischio.

Con questa consapevolezza, molte organizzazioni si sono dotate di strumenti per un'appropriata e attiva gestione del rischio, non solo per fronteggiare gli esistenti obblighi normativi, ma anche per migliorare la propria efficienza nel raggiungimento degli obiettivi.

Questo è particolarmente vero per i rischi legati alla sicurezza, presenti e trasversali in qualunque attività di impresa e particolarmente sensibili ai mutamenti e alle scelte che l'organizzazione effettua nel perseguimento dei propri, legittimi obiettivi di business.

Nell'implementazione di un'attiva strategia di *safety risk management*, le organizzazioni non sono sole, ma possono rifarsi alle esperienze internazionali che si sono accumulate nel tempo e che sono state raccolte, principalmente, in tre norme.

La prima, la ISO 31000:2018, è una linea guida generale per l'implementazione di un sistema di *risk management.*

La seconda, la ISO 45001:2018, è uno standard per l'implementazione di un sistema di gestione specificatamente rivolto alla sicurezza e salute sul lavoro che, nel prossimo futuro, supererà definitivamente l'altro, ben noto ed analogo standard OHSAS 18001:2007 i cui requisiti sono stati adottati da oltre 15.000 imprese in Italia.

Il presente lavoro nel primo Capitolo tratta il tema più generale del rischio, del suo rapporto con l'incertezza e presenta modelli di organizzazione che hanno fronteggiato con successo le sfide nei confronti della complessità.

Il secondo Capitolo presenta i contenuti della nuova norma ISO 31000:2018 e l'approccio al *risk management* in generale.

Il terzo Capitolo del libro fornisce le indicazioni necessarie per impostare un sistema per la *safety risk management* alla luce della nuova norma ISO 45001:2018 e dello standard OHSAS 18001:2007, evidenziando gli aspetti di innovazione della prima e le modalità con le quali integrare eventuali sistemi già implementati secondo lo standard OHSAS 18001 per renderli coerenti col nuovo standard. Gli esempi applicativi e i contenuti delle procedure necessarie sono presentati sotto forma di agevoli schede.

CAPITOLO 2
I contenuti della nuova norma ISO 31000:2018 e l'approccio generale al *risk management*

di Andrea Rotella

SOMMARIO: 1. Lo standard ISO 31000:2018 - 1.1. *Risk governance* complessiva - 1.2. Il *framework* - 1.3. Il processo di *risk management* - 1.3.1. Identificazione dei rischi - 1.3.2. Analisi dei rischi - 1.3.3. Ponderazione del rischio - 1.3.4. Trattamento del rischio - 1.3.5. Monitoraggio, riesame, registrazione e *reporting* - 1.4. Annex SL.

1. Lo standard ISO 31000:2018

La prima versione della ISO 31000 risale al 2009 e fu il risultato di un gruppo di lavoro composto dai rappresentanti di 25 paesi che analizzarono gli standards e le *best practices* in materia di *risk management* esistenti all'epoca, creando una nuova architettura, con una terminologia aggiornata, che era il risultato delle comuni esperienze e poteva essere applicata a culture organizzative e sociali differenti.

La stesura della norma non fu esente da incidenti. In fase di stesura, il *IEC Advisory Committe on Safety* (ACOS) ritirò il proprio contributo in disaccordo con la volontà del resto del gruppo di lavoro di voler inserire tra i rischi anche quelli per la sicurezza. ACOS sosteneva che questi rischi costituissero un caso particolare e dovessero essere esclusi dagli scopi generali di un processo di *risk management* in quanto qualunque rischio per le persone è da considerarsi inaccettabile.

Questa osservazione non venne accolta dal gruppo di lavoro che rispose che una visione così restrittiva avrebbe semplicemente dovuto condurre alla decisione di sospendere la maggior parte delle attività umane, poiché esse contemplano la presenza di rischi per le persone, e ritenendo, al contrario, che un processo uniforme per la gestione dei rischi potesse essere di grande utilità.

Inevitabilmente, dopo la pubblicazione della norma, le esperienze acquisite nei quasi 60 paesi che l'hanno adottata come standard nazionale, evidenziarono la presenza di alcune carenze e la necessità di un aggiornamento.

Nel 2011 venne così creato un comitato di progetto presso la ISO, presto divenuto il comitato tecnico TC 262 per la revisione della norma che, dopo un lungo lavoro, ha portato a febbraio 2018 alla pubblicazione del

nuovo standard ISO 31000 con le seguenti maggiori novità rispetto alla versione precedente:

- riduzione del numero delle definizioni da 29 a 8;
- rivisitazione dei principi per la gestione del rischio;
- rafforzamento dell'importanza della leadership condotta dal top management;
- rafforzamento dell'importanza di una gestione integrata dei rischi;
- più enfasi alla necessità di una continua iterazione del processo di gestione del rischio quando emergono nuove informazioni che devono portare ad una rivisitazione dei processi, delle azioni e dei controlli;
- ottimizzazione dei contenuti per consentire una maggiore adattabilità dello standard a molteplici esigenze e contesti.

Il nuovo testo contiene un numero inferiore di pagine rispetto alla versione del 2009 ed è stato adottato dalla UNI (norma UNI ISO 31000:2018, entrata in vigore il 17 maggio 2018 - testo attualmente disponibile solo in lingua inglese).

La norma è destinata a coloro che creano e proteggono valore nelle organizzazioni avendo cura di gestire rischi, prendere decisioni, fissare e conseguire obiettivi e migliorare le prestazioni. Fornisce linee guida per gestire i rischi che le organizzazioni affrontano e può essere utilizzata durante tutta la vita dell'organizzazione, oltre a poter essere applicata a qualsiasi attività, compreso il processo decisionale a tutti i livelli.

Trattandosi di una linea guida, i suoi contenuti non costituiscono requisiti essenziali e, di conseguenza, lo standard non può essere assoggettato a certificazione. Si tratta di una precisa scelta finalizzata a consentire all'organizzazione la necessaria flessibilità nell'adozione della norma in funzione dei propri bisogni ed obiettivi.

L'approccio comune suggerito dal documento è idoneo a gestire qualsiasi tipo di rischio, non è dedicato ad un particolare settore o industria e può essere adattato a qualunque organizzazione e al suo contesto. I principi, la struttura di riferimento e il processo delineati nella ISO 31000 consentono di gestire il rischio in modo efficiente, efficace e sistematico.

1.1. Risk governance complessiva

La struttura e l'approccio complessivi della norma sono illustrati negli schemi che seguono.

Lo standard, innanzitutto, propone 8 principi che le organizzazioni dovrebbero tenere in considerazione nel definire la struttura di riferimento per la gestione dei rischi (*framework*) e l'implementazione del processo definitivo.

Alla base della scelta di adottare un sistema per la gestione del rischio vi è la convinzione che essa crei valore, aiutando l'organizzazione ad identificare non solo i potenziali rischi che possono costituire una minaccia, ma anche le opportunità che essi sottendono. Un sistema di *risk management* efficiente ha un impatto positivo sull'operatività dell'azienda, aiutando ad individuare ed eliminare le attività che non creano valore e le potenziali perdite derivanti da un incidente. Conseguentemente aumenterà il margine di profitto e può, di per sé stessa, generarne di nuovo (se si rileva, per esempio, che un'eccessiva assegnazione di responsabilità decisionali su un unico soggetto può rappresentare un rischio, l'organizzazione potrebbe propendere verso la creazione di un team che supporti il processo decisionale di costui. In questo modo, tra l'altro, migliorerà la condivisione delle conoscenze, gli scambi di informazione, si creeranno nuovi rapporti che possono generare nuove idee e opportunità).

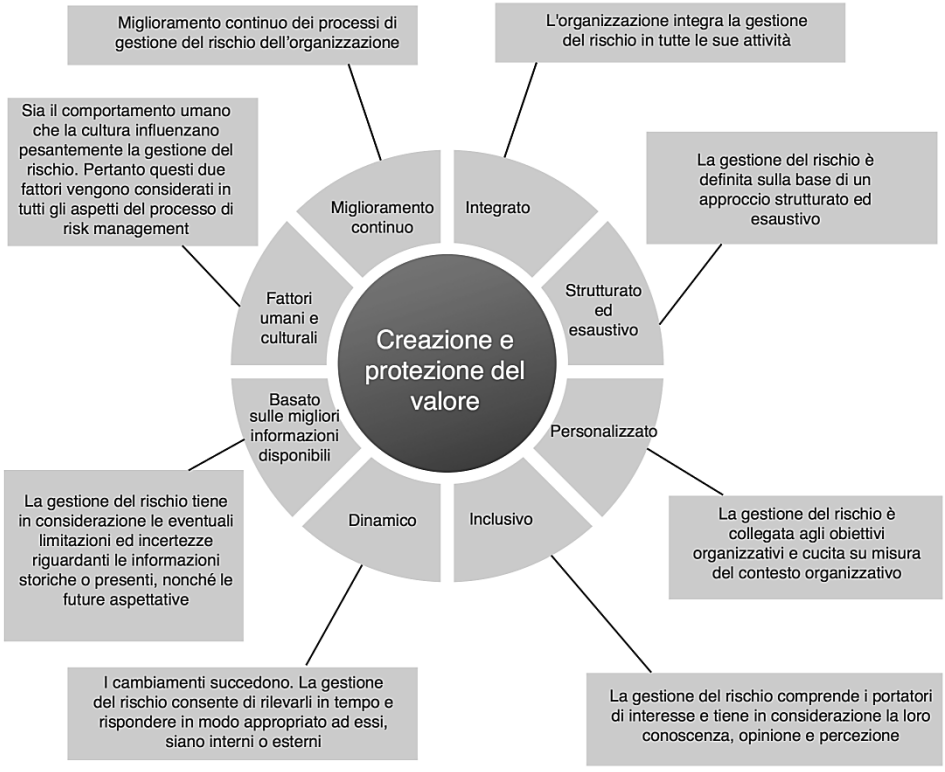

Figura 7

Il *framework* che indica all'organizzazione come integrare la gestione del

rischio in tutte le sue attività, è presentato come un processo iterativo che vede al centro la leadership e l'impegno del *board* al *risk management*.

Figura 8

Infine, il processo di *risk management* richiede l'applicazione sistematica di politiche, procedure e pratiche anche rivolte alle attività di comunicazione e consultazione, definendo il contesto e valutando, trattando, monitorando, riesaminando, registrando e segnalando i rischi.

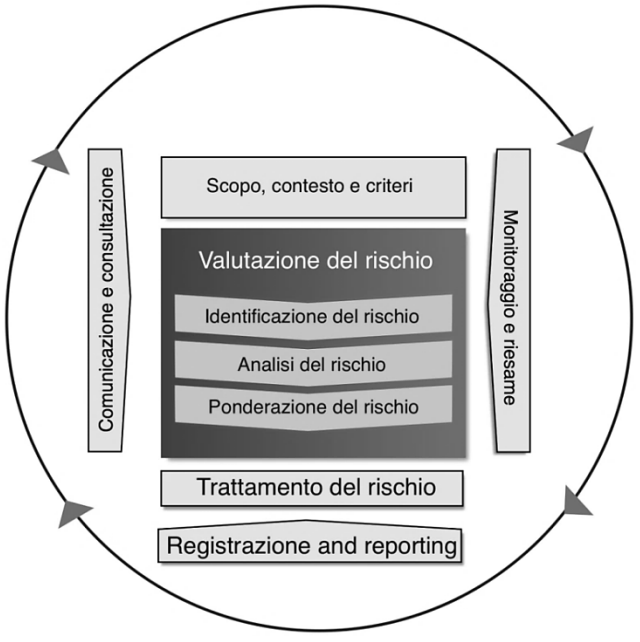

Figura 9

In sostanza, la *risk governance* dell'organizzazione, dovrebbe essere gestita secondo la seguente impostazione:

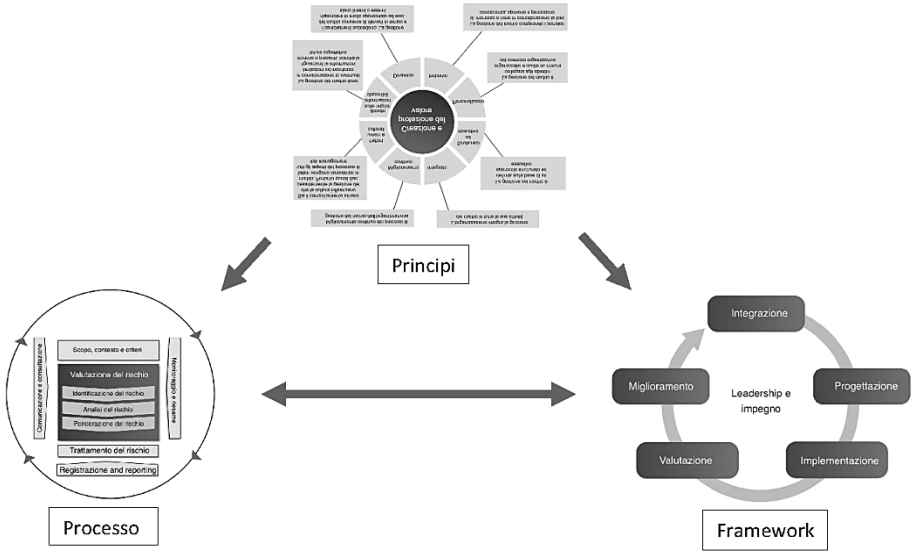

Figura 10

1.2. Il framework

Secondo la ISO 31000, i principi che si trovano alla base di un sistema di *risk management* efficace e il *framework* (cioè la struttura di riferimento, l'architettura complessiva per la gestione del rischio) che essa propone, sono strettamente correlati. Se uno dei principi alla base del governo del rischio è l'idea che la sua gestione debba essere "integrata", la trattazione nella ISO 31000 della componente "integrazione" del *framework* fornisce le informazioni necessarie per comprendere come ottenere il raggiungimento del risultato.

La base della struttura è il ben noto ciclo PDCA ("*Plan*", "*Do*", "*Check*", "*Act*") con al centro la *leadership* e l'impegno, poiché si rileva come un efficace sistema di *risk management* non possa essere estraneo e disallineato dai processi decisionali. Spetta alla leadership, sulla base dei bisogni dell'organizzazione, il compito di calare il *framework* all'interno di eventuali pratiche già esistenti, verificando se vi siano eventuali scostamenti rispetto a quanto stabilito dalla guida e colmando le differenze.

La definizione del contesto nel quale opera la strategia di *risk management* dell'organizzazione è parte integrante della fase di progettazione

("*Plan*", secondo il ciclo PDCA) e deve essere coerente con il contesto generale nel quale si svolgono le attività dell'organizzazione ed i suoi obiettivi, con riguardo a fattori sia interni che esterni. Ciò permetterà l'integrazione del *risk management* all'interno degli altri processi esistenti.

Elementi tipici da considerare nella definizione del contesto sono:

- cultura organizzativa e del rischio;
- politica;
- caratteristiche ambientali in cui opera l'organizzazione (culturali, legali, politici);
- prospettive ed evoluzioni dell'ambiente nel quale l'organizzazione opera;
- caratteristiche tecnologiche del proprio settore;
- normative di settore esistenti ed applicabili;
- concorrenza;
- obiettivi di business;
- propensione al rischio;
- attività operative;
- stakeholder interni ed esterni;
- complessità delle reti;
- interdipendenza e interconnessioni;
- risorse disponibili;
- organizzazione, responsabilità ed autorità assegnate;
- limiti o restrizioni temporali;
- dislocazione geografica delle attività e del business;
- attività di registrazione e reporting esistenti;
- flussi di comunicazione esistenti;
- …

Agli esiti di tale analisi, si procederà a definire l'impegno dell'alta direzione al *risk management*. L'importanza che la leadership riveste nel processo di *risk governance* generale è un elemento comune e condiviso con tutti gli altri standard ISO basati sull'*Annex SL* (vedi in seguito), poiché senza il suo contributo ed impegno verrebbe meno la possibilità di soddisfare alcuni requisiti essenziali per un'efficace gestione del rischio, per esempio:

- assicurare l'allineamento tra la cultura del rischio e della sicurezza dell'organizzazione con la gestione del rischio stesso. Si è già dato

conto dell'importanza di questo aspetto in precedenza e si ribadisce come esso sia strategico. La leadership ha il compito di comunicare e rappresentare la cultura a tutti i soggetti appartenenti all'organizzazione e alle parti interessate, in modo che non si creino contrasti tra i processi di *risk management* e gli obiettivi legati al business;

- allineare i processi di *risk management* alle strategie di business e gli obiettivi dell'organizzazione, in modo da poter valutare in modo accurato la sua propensione al rischio, definendo una strategia di gestione del rischio mirata e integrata;
- definire la politica di gestione del rischio ed assicurare che essa sia promossa e compresa da tutti i livelli dell'organizzazione;
- definire i criteri e i livelli di accettazione dei rischi;
- assegnare le risorse necessarie e sufficienti per la corretta gestione del rischio, conformemente agli esiti della valutazione ed all'esposizione dell'organizzazione ai rischi stessi;
- definire le responsabilità ed assegnare l'autorità necessaria a coloro i quali gestiscono le singole aree di rischio che, conformemente al punto precedente, devono essere in numero sufficiente alle esigenze;
- assicurare che le prestazioni dei processi di *risk management* siano rilevate e incluse tra gli altri indicatori delle prestazioni dell'organizzazione, al fine di evidenziare il loro andamento complessivo e per area di business;
- promuovere il monitoraggio sistematico dei rischi;
- riesame continuo dell'adeguatezza del *framework* e dei processi di *risk management*, man mano che emergono nuovi rischi o opportunità;
- assicurarsi che gli impegni volontari assunti dall'organizzazione, come anche le obbligazioni contrattuali nei confronti di altri soggetti esterni, rientrino nelle valutazioni del sistema di gestione del rischio.

I seguenti aspetti:

- assegnazione dei ruoli organizzativi, autorità e responsabilità;
- allocazione di risorse;
- comunicazione e consultazione;

sono elementi espressamente trattati all'interno della componente

"progettazione" del *framework* nel testo della ISO 31000.

Con riferimento alla "comunicazione e consultazione" è compito della *leadership* dare una risposta ai seguenti quesiti:

- chi sono gli *stakeholder* che devono essere coinvolti nel processo di gestione?
- cosa devono sapere e quali azioni devono intraprendere?
- quando devono essere coinvolti e quando devono attivarsi?
- come verrà comunicata la strategia di *risk management* a questi soggetti?

Vale la pena spendere qualche parola in più circa l'importanza della comunicazione. Si tratta di un elemento spesso sottovalutato, ma che in realtà, come può facilmente testimoniare l'esperienza di qualunque *risk manager*, è quello che ha il maggiore impatto sulle possibilità di successo del processo di gestione del rischio. Se vogliamo dirla tutta, la fase di rilevazione dei rischi, del contesto, la definizione delle misure, ecc. spesso catturano il massimo delle attenzioni e delle risorse. In fondo è per questo che ci prepariamo, è quanto abbiamo studiato, è quello che ci si aspetta da noi. Si svolgono con dinamiche e metodiche familiari a chi si occupa di gestione del rischio, ci permettono di dimostrare le nostre capacità di analisi e di apertura mentale nella ricerca delle soluzioni. E forse, la questione è tutta qui: lo sappiamo fare e, soprattutto, il buon esito della diagnosi e della definizione della cura dipende essenzialmente dalle nostre capacità[1].

Ma tutto cambia quando si tratterà di rendere operativo il lavoro svolto. In questa fase, il modello diventa ufficialmente di dominio pubblico, ma senza un'adeguata progettazione della comunicazione esso sarà destinato al fallimento per mancanza di partecipazione, per l'assenza dei necessari collegamenti e carenza di coinvolgimento.

Per evitare questa ovvia conclusione, devono essere individuati tutti gli *stakeholder*, quali siano le loro esigenze in termini di informazioni sui rischi che essi devono ricevere e fornire, in quali casi essi devono coinvolgere altri stakeholder, chi coinvolgere prioritariamente e in quale formato fornire le informazioni quando emerge un nuovo rischio o si pale-

[1] Il "noi" è riferito a tutti coloro i quali sono investiti della responsabilità di guidare praticamente e inizialmente il processo che porterà alla definizione del sistema nel suo complesso. Si tratta, generalmente, di un team di persone che devono interfacciarsi con le varie aree di rischio dell'organizzazione e qualificati come "esperti".

sano nuove opportunità (riunioni, mail, circolari, aggiornamento di procedure, ecc.).

In una riunione circa le fasi di avanzamento di un progetto di business, comunicare quale sia lo stato del rischio ad esso associato è altrettanto importante che definirne lo stadio raggiunto, in modo da poter assemblare le informazioni e verificare se la valutazione eseguita necessiti di aggiornamento, nonché controllare se le misure poste a prevenzione del rischio siano state effettivamente presidiate.

Un *risk manager* dovrebbe sempre operare sul campo, nella prima linea del rischio. Questo non significa necessariamente dover stare sempre a contatto con operatori *front-end*. Molti rischi e tutte le fasi iniziali di nuovi progetti nascono dalle decisioni prese da personale *back-end* ed, in queste circostanze, è lì che viene richiesta la sua presenza. E quando si parla di presenza, si intende principalmente presenza attiva: girare tra i reparti, parlare con le persone, informarsi con la dirigenza … Da queste attività non ufficiali possono emergere nuovi riscontri o elementi di dubbio, si scoprono i reali atteggiamenti nei confronti del rischio, si percepiscono gli umori, si colgono segnali deboli, si verifica la reale partecipazione.

Ciò detto, terminata la fase di progettazione, il successivo *step* del *framework* consiste nell'"implementazione" del piano per la gestione del rischio ("*Do*", secondo il ciclo PDCA), attraverso la sua comunicazione a tutte le parti interessate secondo le modalità definite dalla *leadership* ed in funzione dei singoli ruoli.

In questa fase si definiscono i criteri per la valutazione dei rischi e per la loro accettazione, un piano di implementazione, si definiscono le scadenze, si modificano i processi decisionali, se necessario.

Si procede, quindi, a dare seguito alla successiva componente del *framework*, ovvero la "valutazione" ("*Check*", secondo il ciclo PDCA) misurando le prestazioni dell'architettura progettata in rapporto ai suoi scopi, al livello di implementazione ed ai comportamenti e si verifica se essa è coerente con il raggiungimento degli obiettivi. Trattandosi di una linea guida, la ISO 31000 non contempla l'esecuzione di *audit* interni, ma evidentemente questo strumento costituisce uno dei mezzi privilegiati per monitorare il sistema, anche facendo riferimento alle indicazioni contenute in proposito nella norma dedicata ISO 19011. Le risultanze dei monitoraggi dovrebbero essere periodicamente sottoposti al riesame dell'alta direzione, al fine di verificare la necessità o l'opportunità di apportare modifiche o correzioni al *framework* definito.

Specificatamente a questo obiettivo è dedicata la componente "miglioramento" ("*Act*", secondo il ciclo PDCA) del *framework*, che spinge il sistema verso una maggiore efficienza, aumentando la resilienza del business in ragione dei cambiamenti del contesto che possono richiedere un aggiornamento dell'architettura di gestione.

1.3. Il processo di risk management

Quanto definito nel *framework* in termini di linee generali ed architettura per affrontare e gestire il rischio, trova specifica e pratica applicazione all'interno del processo di gestione del rischio vero e proprio che vede al suo centro le componenti di "valutazione del rischio" e "trattamento del rischio".

La IS0 31000 richiede che, innanzitutto, venga definito lo scopo, il contesto ed i criteri di valutazione dei rischi, al fine di adattare il processo di *risk management* alle effettive esigenze e stabilire i suoi confini. In linea di massima, si tratta di definire con maggior dettaglio quanto già sviluppato nella componente "progettazione" del *framework*, definendo strumenti pratici per la gestione di ciascun rischio e specifici per ciascuna area operativa o di business (non è detto che, ad esempio, i criteri di valutazione utilizzati per l'area *finance* siano i medesimi con i quali verrà analizzata l'area *IT*).

La definizione dei criteri di rischio consentirà all'organizzazione di portare avanti il processo in modo conciso, efficiente e standardizzato e, nella definizione di tali criteri, occorrerebbe tener presente:

- natura e tipo delle incertezze che possono avere impatto sugli esiti e obiettivi;
- impegni legali, contrattuali, normativi e volontari dell'organizzazione;
- la probabilità connessa ad un rischio e l'impatto delle sue conseguenze;
- fattori correlati al tempo;
- rischi multipli e connessi, con impatti a catena;
- come definire la severità di un rischio.

Definiti scopo, contesto e criteri di rischio, si può procedere alla "valutazione dei rischi" vera e propria del processo di *risk management*, che comprende le seguenti fasi:

- identificazione dei rischi;
- analisi dei rischi;
- ponderazione dei rischi.

L'intero processo è progettato per essere sistematico, iterativo e colla-

borativo e, dunque, in tutti questi stadi è vitale comunicare e coinvolgere qualunque soggetto interno ed esterno che possa portare informazioni, conoscenza, esperienza e competenza per il buon esito del processo.

1.3.1. Identificazione dei rischi

Questa fase comprende la ricerca, il riconoscimento e la descrizione dei rischi e, implicitamente, l'identificazione delle sorgenti di rischio, gli eventi che possono determinarne l'insorgenza e le loro potenziali conseguenze.

Nel suo sviluppo si può far ricorso all'esperienza, al parere di esperti, ad analisi teoriche, alla conoscenza di persone informate sull'argomento in analisi, ai bisogni delle parti interessate.

La visione di ciò che è da considerarsi *rischio* secondo la ISO 31000 è ben più ampia dell'analoga definizione contenuta nella normativa antinfortunistica[2] e, in questo senso, più aderente a una visione meno causale e deterministica degli incidenti.

La guida ISO 73, dalla quale è stata tratta la definizione di rischio riportata nella nuova ISO 31000, lo definisce, difatti, come:

> Rischio: l'effetto dell'incertezza sugli obiettivi.
>
> Nota 1: un effetto è uno scostamento da quanto atteso - positivo e/o negativo.
>
> Nota 2: gli obiettivi possono presentare aspetti differenti (come scopi finanziari, di salute e sicurezza, ambientali) e possono intervenire a livelli differenti (come progetti, prodotti e processi strategici, riguardanti l'intera organizzazione).
>
> Nota 3: il rischio è spesso caratterizzato dal riferimento a eventi potenziali e conseguenze, o una combinazione di questi.
>
> Nota 4: il rischio è spesso espresso in termini di combinazione delle conseguenze di un evento (compresi cambiamenti nelle circostanze) e della verosimiglianza del suo verificarsi.
>
> Nota 5: l'incertezza è lo stato, anche parziale, di assenza di informazioni relative alla comprensione o conoscenza di un evento, delle sue conseguenze o della loro verosimiglianza.

[2] Art. 2, comma 1, lett. s) del D.Lgs. n. 81/2008: "probabilità di raggiungimento del livello potenziale di danno nelle condizioni di impiego o di esposizione ad un determinato fattore o agente oppure alla loro combinazione".

Vale la pena soffermarsi per poche righe sul riferimento alla *verosimiglianza* nelle citate note 4 e 5[3].

Il termine rappresenta la trasposizione, magari non perfettamente riuscita, della parola "*likelihood*" ("*vraisemblance*" in francese), riportata nella versione inglese della norma, comunemente tradotta in italiano con "probabilità".

I paesi anglosassoni hanno due distinte parole per identificare la probabilità: *likelihood* e *probability*. Quest'ultima è comunemente associata al senso matematico del termine, mentre *likelihood* riveste un'accezione più ampia, un concetto non necessariamente quantificabile, misurabile o determinabile oggettivamente.

Il significato di *likelihood* deve essere inteso nel senso di "plausibilità di un accadimento ipotizzabile", così spingendo il valutatore ad analizzare anche rischi in quanto semplicemente "possibili", assegnando valore ai tentativi di registrare e accettare l'idea di analizzare anche gli scenari meno probabili, purché sufficientemente credibili.

Si ritiene interessante questo approccio perché spinge ad andare oltre le serie storiche di dati, le esperienze, l'induzione, rivolgendo la propria ricerca anche ai quadranti oltre i "fatti noti conosciuti e sconosciuti", promuovendo lo scetticismo.

La definizione e la natura stessa del rischio rendono impossibile fare un elenco *a priori* di quali essi siano. Tuttavia, a livello metodologico, aiuta avere una base di partenza o crearsi una strategia con la quale procedere per eseguire questa fase del processo.

Un primo tentativo, è quello di suddividere i rischi per categorie[4], un buon metodo anche per restringere il campo laddove alcune categorie di rischio fossero palesemente assenti o non rientranti nello scopo della *risk governance*. Anche in questo caso, l'elenco sarebbe inesauribile ed in letteratura esistono molteplici fonti alle quali attingere. Un esempio è riportato di seguito[5]:

[3] Entrambe le note non sono riportate nella ISO 31000:2018.

[4] Tipicamente, nel settore della sicurezza sul lavoro, molti ricorrono a questa strategia, suddividendo i rischi nelle categorie "sicurezza", "salute" e "trasversali".

[5] Tratto da: *A guide to the PMBOK*, 6th edition, 2017. L'elenco è specificatamente pensato per un'attività di *risk management* durante la realizzazione di un progetto.

Categoria	Descrizione
Interni	Rischi provenienti dall'interno dell'organizzazione.
Esterni	Rischi provenienti dall'esterno dell'organizzazione.
Finanziari	Rischi associati con profitti, ricavi, calcoli sul ritorno dell'investimento, budget di progetto, costi di progetto e simili.
Tecnici e prestazionali	Rischi associati agli aspetti tecnici del progetto. Potrebbe trattarsi di rischi correlati all'*information technology* o a rischi specifici di settore, come diagrammi ingegneristici, attrezzature meccaniche, impianti di supporto agli edifici e così via. Rischi prestazionali possono riguardare tecnologie in fase di sperimentazione o complesse o possono riguardare obiettivi o misure non realistici.
Business	Rischi associati al marketing o al tempo di rilascio dei prodotti, ritardi nelle vendite, problemi di gestione, informazioni sulla concorrenza, e così via.
Organizzativi	Rischi associati all'organizzazione in quanto tale.
Culturali	Rischi associati a problemi culturali o a differenze culturali (questo specialmente riguardo alle organizzazioni con presenza internazionale).
Security	Rischi associati alla sicurezza delle informazioni, del personale, della struttura e della proprietà intellettuale.
Project management	Rischi associati ai processi di *project management*, alla maturità organizzativa e all'abilità.
Legali	Rischi associati a problemi legali che potrebbero impattare l'organizzazione o il progetto.
Ambientali	Rischi associati con il progetto che potrebbero avere impatti ambientali, nonché rischi che l'ambiente può generare sul progetto.
Scopo	Rischi associati allo scopo del progetto.
Qualità	Rischi che impattano la qualità del progetto o del suo prodotto.

Programmazione	Rischi associati alle attività stimate e schedulate.
Processo	Rischi associati ai processi di business o altri processi che impattano sull'organizzazione, il consumatore o il progetto.
...	...

A loro volta, queste categorie, in particolare quelle molto ampie o complesse, possono essere suddivise in sottocategorie[6] per gestire meglio la fase di individuazione.

Sono altresì applicabili in questa fase alcune delle tecniche individuate dalla norma ISO 31010 "*Risk assessment techniques*" e che saranno elencate di seguito.

Indipendentemente dalle tecniche effettive che saranno impiegate, è importante che venga dato il dovuto riconoscimento ai fattori umani e organizzativi nell'identificazione del rischio.

1.3.2. Analisi dei rischi

Questa fase è quella attraverso la quale è possibile giungere alla comprensione dei rischi precedentemente individuati, fornendo l'*input* necessario ai processi decisionali. Nel condurre l'analisi ci si rifarà ai valori di probabilità, ove disponibili, piuttosto che assegnando in forma qualitativa un valore alla verosimiglianza di taluni eventi, nonché le conseguenze che essi possono comportare e quali siano le misure di controllo o mitigazione che possono ricondurre il rischio a valori di accettabilità.

I metodi di analisi possono essere:

- qualitativi: in generale essi assegnano alla probabilità ed alle conseguenze un livello di significatività (es. basso, medio, alto) sulla base di criteri qualitativi;
- semi-quantitativi: impiegati e ben noti nel settore della sicurezza sul lavoro sotto forma di matrici, permettono di ottenere il livello di rischio basandosi su assegnazioni numeriche ai valori di probabilità e conseguenza, a loro volta definiti sulla base di criteri qualitativi;
- quantitativi: utilizzano esclusivamente dati misurabili e oggettivi di probabilità e conseguenza.

[6] Ad esempio, nel settore della sicurezza sul lavoro, i "rischi per la salute" possono essere suddivisi in ulteriori categorie, quali "rischi chimici", "rischi fisici".