Università
Ca'Foscari
Venezia

Corso di Laurea magistrale

in Economia e finanza

Tesi di Laurea

La gestione del rischio nelle imprese di assicurazione: l'Enterprise Risk Management

Relatore
Ch. Prof. Antonio Proto

Laureando
Mattia Paquola
Matricola n. 847306

Anno Accademico
2017 / 2018

Università
Ca'Foscari
Venezia

INDICE

INTRODUZIONE

Il *risk management* assume importanza fondamentale sia nel settore bancario che in quello assicurativo: il rischio, se correttamente gestito, può rappresentare delle opportunità. L'attività delle imprese di assicurazione ha subito numerosi cambiamenti nel corso degli anni estendendosi anche sui mercati finanziari, accrescendo di conseguenza il grado di rischio complessivo dato da un maggior peso dei rischi finanziari accanto ai rischi tipici dell'attività di assicurazione.

Così come per il settore bancario attraverso Basilea II, la direttiva 2009/138/CE nota come *Solvency II* entrata in vigore nel gennaio 2016, intende regolamentare il settore assicurativo a livello Europeo: *Solvency II* prende il posto della precedente normativa nota come *Solvency I* sopperendo alle lacune a livello di armonizzazione tra gli stati membri soprattutto per quanto concerne i margini di solvibilità. *Solvency II* apporta perciò modifiche sostanziali sia per quanto riguarda i requisiti patrimoniali e le metodologie di calcolo, sia per quanto riguarda l'intero sistema di vigilanza prudenziale ponendo come finalità principali la tutela dei consumatori nonché un miglioramento della gestione rischio.

Solvency II ruota attorno a quelli che vengono definiti *tre pilastri*, ovvero requisiti finanziari minimi a copertura dei rischi, governance e risk management ed infine requisiti informativi. Si sottolinea inoltre come le maggiori innovazioni introdotte da Solvency II riguardino soprattutto il secondo pilastro.

L'elaborato intende riassumere le metodologie di gestione del rischio all'interno delle imprese di assicurazione attraverso l'uso dell'*Enterprise Risk Management* cercando di descrivere i rischi che l'impresa di assicurazione si trova a dover fronteggiare e come questi vengono da essere gestiti. Il presente elaborato è strutturato in tre capitoli: nel primo capitolo viene riassunta l'attività svolta da un'impresa di assicurazione indicandone le criticità, descrivendo i rischi nei quali essa incorre ed esplicitando le disposizioni normative per quanto concerne l'attività assicurativa e la gestione dei rischi. Nel secondo capitolo viene descritto il processo evolutivo che ha interessato le tecniche di *risk management* fino ad arrivare all'attuale *Enterprise Risk Management* (*ERM*), ovvero la metodologia più diffusa per la gestione del rischio. Ne viene quindi analizzato lo sviluppo a partire dagli anni Novanta, gli Standard di riferimento (*CoSO* e *ISO 31000*) e le fasi in cui esso si articola sottolineando inoltre l'importanza della connessione tra rischio e strategia nonché della costituzione di un'adeguata *risk aware culture*. Nel terzo capitolo viene infine esaminata la governance e la gestione del rischio di un'impresa di assicurazione studiando il processo di *Own Risk and Solvency Assessment* (*ORSA*)

disposto dall'art. 45 della direttiva *Solvency II*, il sistema dei controlli interni e approfondendo in ultima istanza il ruolo di due figure chiave per la gestione del rischio ovvero il *Chief Risk Officer* (*CRO*) e il CDA.

CAPITOLO 1

I RISCHI NELLE IMPRESE DI ASSICURAZIONE

1. L'ATTIVITÀ ASSICURATIVA

L'impresa di assicurazione svolge una funzione di fondamentale importanza all'interno del sistema economico, ovvero quella di assumere in modo sistematico i rischi che le vengono trasferiti dagli assicurati. Questi rischi sono definiti come *rischi puri* ovvero dei rischi che hanno solamente due possibilità di manifestazione: si verificano o non si verificano[1].

I rischi puri di cui l'impresa di assicurazione si fa carico afferiscono essenzialmente a due grandi aree a seconda di ciò che si vuole assicurare: *rami danni* se viene assicurato il patrimonio o un bene di proprietà dell'assicurando dal verificarsi di un sinistro, o *rami vita* se viene assicurato un evento attinente alla vita umana. Da questa distinzione è possibile cogliere come le assicurazioni dei rami danni siano una forma di tutela indennitaria e come invece le assicurazioni dei rami vita assolvano più ad una funzione previdenziale e/o di risparmio[2].

Le imprese di assicurazione non gestiscono questi rischi singolarmente, bensì in modo aggregato, rendendo possibile l'applicazione delle leggi statistiche e in particolare della *legge dei grandi numeri*[3]. Questa pratica di aggregazione dei rischi viene chiamata *risk pooling* e permette all'impresa di conoscere con precisione l'ammontare dei risarcimenti futuri facendo sì che il rischio medio assunto attraverso il *pool* di assicurati risulti inferiore al rischio individuale ceduto rendendo quindi conveniente assicurarsi[4].

È necessario però precisare che le leggi statistiche appena menzionate sono applicabili solamente nel caso in cui i rischi siano *omogenei* e *indipendenti* in quanto, suddividendoli in classi omogenee per probabilità di accadimento e per ammontare del danno, al tendere all'infinito della dimensione campionaria la legge dei grandi numeri fa sì che la frequenza di accadimento dei singoli

[1] Paci (2018).
[2] Le imprese di assicurazione che hanno ottenuto l'autorizzazione allo svolgimento dell'attività assicurativa di cui all'art. 13 del Codice delle Assicurazioni Private (CAP) se soddisfatte le condizioni previste all'art. 14, possono operare nei rami vita o nei rami danni così come classificati all'art. 2. L'impresa potrà svolgere la propria attività anche negli altri rami per i quali non ha già ottenuto l'autorizzazione se dimostra di disporre degli attivi a copertura delle riserve tecniche e dei fondi propri di base ammissibili necessari per coprire il Requisito Patrimoniale Minimo tenuto conto dei nuovi rami.
[3] La legge dei grandi numeri deriva da alcune diffuse constatazioni sperimentali: ripetendo nelle medesime condizioni un esperimento casuale, al crescere del numero delle prove, la frequenza relativa di un evento tende a stabilizzarsi. Inoltre, per variabili quantitative rilevate in più sottoprove ripetute, la media rilevata su un campione di osservazioni si stabilizza al crescere della dimensione campionaria convergendo verso il valore medio della popolazione (Piccolo 2010).
[4] Paci (2018).

sinistri e il loro ammontare venga a coincidere rispettivamente con la probabilità che il danno si verifichi e con il valore medio del risarcimento per quella categoria di assicurati[5]. Questa metodologia è quindi la base che permette alle imprese di assicurazione di calcolare un premio adeguato in relazione ai futuri impegni che si dovranno sostenere.

Dall'articolo 1882 del Codice civile, che definisce l'assicurazione come «…Il contratto con il quale l'assicuratore, verso pagamento di un premio, si obbliga a rivalere l'assicurato, entro i limiti convenuti, del danno ad esso prodotto da un sinistro ovvero a pagare un capitale o una rendita al verificarsi di un evento attinente alla vita umana»[6], è possibile ricavare che il premio è il prezzo che l'assicurato paga per poter accedere alle garanzie indicate nel contratto e, allo stesso tempo, è il corrispettivo che spetta all'assicuratore per i suoi impegni futuri[7].

Il concetto di premio non è però unico, bensì dev'essere declinato a seconda delle sue componenti: a livello teorico il premio dovrebbe uguagliare il valore attuale atteso dei risarcimenti futuri anche se, questo premio definito come *premio equo*, è solamente un concetto teorico in quanto l'aleatorietà che permea l'attività assicurativa, rende necessario aggiungere al premio un *caricamento di sicurezza* per sopperire ad errori nella sua determinazione[8]. Il premio così ottenuto viene definito *premio puro*, ma anche questo non è il prezzo ultimo che gli assicurati pagano. Infatti, il premio definitivo è il cosiddetto *premio di tariffa* ossia il premio che tiene conto dei costi che sostiene l'impresa di assicurazione nello svolgimento della propria attività[9] e che è ottenuto dalla somma tra premio puro e i cosiddetti *caricamenti*[10].

Se da un lato l'aspetto "matematico" è l'elemento cardine dell'attività assicurativa, d'altro lato il comportamento degli assicurati è una variabile difficilmente prevedibile che incide anch'essa sulle scelte di un'impresa di assicurazione, poiché il cliente cerca sempre di massimizzare il proprio profitto, anche a scapito dell'assicuratore. Così, dallo studio sull'osservazione dei comportamenti degli assicurati in sede di trattativa e stipula del contratto e dall'osservazione del loro comportamento

[5] Paci (2018); Cappiello (2018) specifica inoltre che l'omogeneità è intesa in senso sia *qualitativo* (ovvero di stessa probabilità che si verifichi il danno), sia *quantitativo* (ovvero stesso ammontare del danno).
[6] Art. 1882 Codice civile.
[7] Donati e Volpe (2019).
[8] Il premio infatti viene determinato sia attraverso le basi attuariali ovvero i dati statistici, sia attraverso le basi finanziarie (o tasso tecnico) ovvero il tasso utilizzato per l'attualizzazione. È chiaro quindi che una stima in difetto basata su errati dati statistici o un tasso tecnico troppo ottimista, possono comportare un errore nel calcolo del premio che viene così ad essere inferiore a quanto invece sarebbe necessario.
[9] L'impresa di assicurazione infatti sostiene dei costi che derivano dalla scelta del canale distributivo, dall'area di liquidazione sinistri, dagli altri oneri relativi alle altre aree gestionali diverse da distribuzione e liquidazione (come ad esempio marketing e sviluppo di nuovi prodotti) e dagli altri oneri relativi ai costi di supporto al business (come ad esempio gestione del personale, dei sistemi informatici e oneri legati all'amministrazione e contabilità).
[10] Cappiello (2019); Paci (2018). I caricamenti rappresentano la componente aggiuntiva di premio a carico degli assicurati al fine di coprire i costi acquisizione (ad esempio le provvigioni), i costi d'incasso (spese per emissione di quietanze ad esempio) e i costi di gestione.

dopo aver concluso il contratto, sono state individuate alcune condotte che possono causare serie difficoltà all'assicuratore, vale a dire la *Selezione avversa* e l'*Azzardo morale*.

Il concetto di *Selezione avversa*[11] (*Adverse Selection*) è strettamente collegato alla presenza di *asimmetrie informative* tra l'assicurato (*Agent*) e l'assicuratore (*Principal*). Il primo infatti, al fine di stipulare un contratto vantaggioso, potrebbe tacere alcune informazioni circa il rischio in oggetto (*hidden information*) con la conseguenza che l'assicuratore non sarà in grado di categorizzare adeguatamente la controparte e calcolerà un premio errato dato che nella maggioranza dei casi la verifica delle informazioni è molto costosa o addirittura impossibile[12].

La teoria economica, al fine di risolvere la questione della selezione avversa, suggerisce di suddividere i clienti in classi omogenee di rischio e di offrire ad ogni classe una polizza diversa[13], con una maggiore copertura e un premio più elevato, nel caso la controparte sia ad alto rischio e, viceversa, una copertura minore con un premio inferiore nel caso in cui la controparte abbia un basso rischio[14]. Questa soluzione non può tuttavia essere ritenuta soddisfacente in quanto altre imprese di assicurazione potrebbero proporre delle polizze che si collocano nel mezzo attirando entrambe le tipologie di clientela, vanificando così la segmentazione precedente. Le imprese di assicurazione realizzeranno sempre nuove polizze che si collocano nel mezzo rispetto alle precedenti variando livello di copertura e premio, con la diretta conseguenza che le precedenti polizze non risulteranno più competitive e verranno ritirate dal mercato. Si assisterà quindi ad una migrazione della clientela ad alto rischio che trova le nuove polizze più appetibili, mentre la clientela a basso rischio troverà sempre meno conveniente assicurarsi. Tutto questo potrebbe portare alla scomparsa del mercato assicurativo perché resterebbe nel mercato solamente la clientela ad alto rischio[15].

Se la teoria economica non riesce a dare una soluzione definitiva alla questione della selezione avversa, l'intervento legislativo permette di arginare tale situazione. La normativa vigente infatti disincentiva la reticenza o l'omissione dell'assicurato nel comunicare informazioni rilevanti circa il rischio oggetto di assicurazione, prevedendo nel caso di dolo o colpa grave l'annullamento del contratto e la perdita del diritto a ricevere l'indennizzo se si verifica un sinistro (art. 1892 c.c.) mentre, nel caso in cui non vi sia dolo o colpa grave, è prevista la possibilità di recesso da parte

[11] Sulla selezione avversa si veda: Akerlof (1970); Arrow (1969 e 1973)
[12] Donati e Volpe (2019); De Lorenzi (2008).
[13] La teoria suggerisce di ricercare un equilibrio di separazione (*separating equilibrium*) piuttosto che di aggregazione (*pooling equilibrium*) in modo tale che siano gli stessi individui a rivelarsi (*signalling*). De Lorenzi (2008).
[14] De Lorenzi (2008) sottolinea che in realtà nella prassi, le compagnie offrono la stessa polizza ma con premi differenti in relazione al rischio.
[15] De Lorenzi (2008).

dell'assicuratore o una riduzione dell'indennizzo se si verifica il sinistro prima che abbia luogo l'annullamento (art. 1893)[16].

Per quanto riguarda invece l'*Azzardo Morale* (*Moral Hazard*), esso fa riferimento al comportamento tenuto dagli assicurati successivamente alla stipula del contratto. L'assicurato, una volta trasferito il rischio, ha un interesse minore a prendere delle precauzioni in quanto il rischio è in capo all'assicuratore e i costi per le precauzioni porteranno una scarsa utilità all'assicurato[17]. Anche in questo caso ci troviamo di fronte alla presenza di *asimmetrie informative* in quanto, per l'assicuratore, risulta impossibile specificare nel contratto ogni singolo comportamento che l'assicurato dovrà tenere e pretendere che questo sia osservato, perché è molto difficile verificare il comportamento di quest'ultimo dopo la conclusione del contratto senza sostenere elevati costi[18].

Le soluzioni proposte dalla teoria economica suggeriscono all'assicuratore di predisporre un contratto che risulti appetibile per l'assicurato ma che al contempo lo sproni a prendere delle precauzioni allo scopo di evitare il verificarsi del danno. Si suggerisce infatti di predisporre dei contratti che prevedano un massimale (soprattutto nel caso di grandi danni) e/o scoperti e franchigie (soprattutto nel caso di piccoli danni), in modo tale che una parte del danno resti in capo all'assicurato così che il livello di scopertura venga a dipendere dai costi per le precauzioni[19]. Inoltre, in presenza di rapporti ripetuti tra assicurato e assicuratore il *moral hazard* si attenua, perché il premio viene aggiustato in base alla frequenza degli eventi dannosi verificatisi (*experience rating*)[20].

A differenza della selezione avversa, l'azzardo morale non è una circostanza così grave da richiedere un intervento normativo, in quanto generalmente attraverso gli accordi contrattuali si riesce a contenere il problema. L'intervento normativo risulta invece necessario nel momento in cui si generano delle esternalità negative dovute al comportamento degli assicurati che perseguono un mero scopo di lucro. Così infatti, per la validità del contratto di assicurazione, viene prevista la necessaria presenza di un interesse al risarcimento del danno, pena la nullità dello stesso (art. 1904 c.c.), viene stabilito che l'ammontare massimo del risarcimento non possa essere superiore al valore reale della cosa assicurata (art. 1908 c.c.), viene ammessa la sottoassicurazione (art. 1907 c.c.) e vietata la sovrassicurazione (art. 1909)[21].

[16] In merito si vedano anche artt. 1175, 1335, 1337, 1362, 1366 che dispongono quale debba essere il comportamento in sede precontrattuale, imponendo buona fede oggettiva, correttezza precontrattuale e ordinaria diligenza precontrattuale.
[17] De Lorenzi (2008).
[18] De Lorenzi (2008); Cappiello (2019).
[19] De Lorenzi (2008) suggerisce piena copertura ad un premio elevato nel caso in cui i costi delle precauzioni siano maggiori dei benefici derivanti dalle precauzioni stesse, mentre una copertura quasi piena se il costo delle precauzioni e basso (basterà infatti una piccola scopertura per far sì che l'assicurato prenda precauzioni).
[20] L'assicuratore in tali circostanze può concedere uno sconto o applicare una penalità in relazione al comportamento tenuto dall'assicurato durante il periodo contrattuale (*bonus/malus*).
[21] Donati e Volpe (2019); De Lorenzi (2008).

2. I RISCHI

Cercare di classificare ogni singolo rischio aziendale è un'operazione complessa in quanto le suddivisioni proposte risultano spesso differenti. Inoltre, si sottolinea come i confini tra le diverse tassonomie risultino spesso labili in quanto molti rischi in sede di classificazione possono rientrare in più categorie. In generale, i rischi di un'impresa di assicurazione afferiscono a due macroaree, l'area di gestione tecnico-assicurativa e l'area di gestione patrimoniale-finanziaria[22].

Con riferimento alla gestione tecnica ritroviamo quelli che sono definiti come *rischi attuariali* e che discendono da scostamenti tra le ipotesi statistiche di partenza usate come base di calcolo per il premio e l'effettiva frequenza dei rischi che si sono verificati. Essi vengono definiti *rischi di sottoscrizione* e si suddividono in *sottoscrizione vita* e *sottoscrizione non vita* (danni) a seconda del ramo considerato.

Accanto a questi rischi tipici che riguardano da vicino l'attività assicurativa, vi sono dei rischi comuni anche ad altre imprese e ad altri intermediari finanziari che fanno sostanzialmente riferimento alla gestione patrimoniale-finanziaria[23]. Generalmente si individuano le seguenti categorie di rischi[24]:

- *I rischi di mercato* sono i rischi tipici fronteggiati da chi effettua investimenti nel mercato finanziario e sono diretta conseguenza delle turbolenze che possono verificarsi a seguito di movimenti avversi di prezzo, interessi e valuta. Questi rischi sono tanto più intensi quanto maggiore è la volatilità del mercato di riferimento e riguardano:
    - *Il rischio tasso d'interesse*. Afferisce alla variazione della struttura a scadenza dei tassi e/o la volatilità degli stessi.
    - *Il rischio azionario*. Nasce dalla volatilità e dalle fluttuazioni dei prezzi di mercato dei titoli azionari e fa riferimento a tutte le attività e le passività il cui valore risulta sensibile alle variazioni dei prezzi azionari;

[22] Cappiello (2018); Paci (2018). Mentre *l'area tecnica-assicurativa* fa riferimento al core business della compagnia e quindi ad operazioni di assunzione dei rischi puri, di riassicurazione e di gestione dei risarcimenti da parte di queste, costituzione e gestione del portafoglio rischi, *l'area patrimoniale finanziaria*, oltre a ricercare l'equilibrio economico, è lo strumento che garantisce la solvibilità aziendale e che potenzia la struttura di impresa e che riguarda l'incasso di premi e altri ricavi, il pagamento dei risarcimenti, la gestione dei flussi in entrata e in uscita relativi alla gestione aziendale, l'investimento delle riserve tecniche e la gestione degli investimenti. De Lorenzi (2008) p. 49-50.

[23] Hajek (2018); Cappiello (2018); 10th Global Conference of Actuaries.

[24] La seguente classificazione si basa sull'opera di Prandi (2010). L'autore individua alcune macrocategorie quali *rischi imprenditoriali e associati* a seconda che esse facciano riferimento all'attività primaria dell'impresa o alle attività di supporto, *rischi puri e speculativi* la cui differenza consiste nella possibilità per i secondi di generare anche esiti positivi e se correttamente gestiti possono portare dei profitti per l'impresa, *rischi interni ed esterni* all'area dell'impresa e infine i *rischi sistematici e specifici* la cui discriminante consiste nell'impossibilità di diversificare i primi. Secondo prandi ogni rischio elencato di seguito potrebbe rientrare in una o più di queste macrocategorie.

- *Il rischio immobiliare* che riguarda la sensibilità di attività e passività, alla volatilità dei prezzi di mercato degli immobili;
- *Il rischio di cambio* (*o rischio valuta*), ovvero il rischio che si sostiene nel momento in cui si effettuano degli investimenti in strumenti finanziari in valuta estera e che dipende perciò da variazioni dalla volatilità dei tassi di cambio di valuta.
- *Il Rischio spread*, che discende da variazioni del livello o della volatilità degli spread di credito rispetto alla struttura per scadenze dei tassi d'interesse.
- *Il rischio di liquidità*[25] è il rischio che l'impresa non sia in grado a scadenza di assolvere ai propri obblighi in quanto non dispone delle risorse necessarie. Se l'impresa non dispone della liquidità necessaria è costretta a smobilizzare le proprie attività che rischiano quindi di essere svendute o a richiedere prestiti aumentando le proprie passività.

- *Il rischio di controparte* è il rischio di subire delle perdite derivanti dall'inadempimento imprevisto o dal deterioramento del merito di credito della controparte. L'impresa, per questo rischio, dovrà tenere in considerazione la *Probability of Default* (*PD*) la *Credit Exposure*, il *Recovery Rate* e la *Loss Given Default* (*LGD*)[26].
- *Il rischio di concentrazione* è il rischio che deriva dall'eccessiva concentrazione nei confronti di un unico emittente di titoli o di un gruppo di emittenti collegati dovuto ad una mancata diversificazione del proprio portafoglio.
- *I rischi operativi*. Si tratta di rischi che derivano dalle attività operative, che riguardano ogni fase del processo di business e al cui interno sono ricompresi una varietà di rischi. Fanno riferimento a eventi aleatori, interni o esterni, che determinano l'inefficacia o l'inefficienza dei processi aziendali[27]. Tra questi si ricordano i rischi che discendono dall'inadeguatezza o dalla mancanza di capacità del personale, i rischi connessi ai processi e ai sistemi utilizzati

[25] Gli studiosi sono soliti far rientrare il rischio di liquidità e il rischio di credito (o di controparte) all'interno della categoria *rischi finanziari* definita da Chapman (2006) come "*l'esposizione ad eventi avversi che intaccano la profittabilità e che in circostanze estreme possono portare al collasso l'impresa*", in modo tale da suddividere i rischi derivanti dalle scelte aziendali da quelli che invece dipendono esclusivamente dalle dinamiche di mercato. Si ricorda che, in merito alle classificazioni dei rischi, sussistono differenti opinioni spesso non condivise tra i diversi autori esaminati e così ad esempio Dowd (1998) individua separatamente il rischio di liquidità e il rischio di credito senza farli rientrare in una specifica categoria, mentre Prandi (2010) comprende all'interno dei rischi finanziari il rischio tasso e il rischio cambio.

[26] Queste sono le componenti del rischio di credito e riguardano la probabilità che la controparte sia inadempiente (*Probability of Default*), a quanto ammonta l'esposizione nei suoi confronti nel caso si verifichi il default (*Credit Exposure*), quanto potrò recuperare nel caso in cui il *default* si verifichi (*Recovery Rate*) e a quanto invece ammonterà la perdita in questa situazione (Loss Given Default); 10th Global Conference of Actuaries; Hajek (2011).

[27] Dowd (1998); Prandi (2010).

per produrre e supportare l'attività aziendale e i rischi che derivano da fattori esterni primo fra tutti la concorrenza[28].

- *I rischi di natura qualitativa* sono dei rischi difficili da quantificare in quanto non sono state sviluppate adeguate metodologie di calcolo:
    - *Il rischio strategico* che deriva dalle strategie utilizzate dall'impresa che col passare del tempo potrebbero rivelarsi errate;
    - il *rischio reputazionale* che impatta direttamente sull'immagine dell'azienda.

Nonostante sia stata effettuata una distinzione tra gestione tecnica-assicurativa e gestione patrimoniale-finanziaria, queste due aree non vanno osservate separatamente, bensì congiuntamente[29]. Infatti, se da un lato la gestione patrimoniale-finanziaria è diretta conseguenza della gestione tecnica-assicurativa, in quanto è necessario investire le risorse monetarie raccolte attraverso i premi, dall'altro lato essa risulta fondamentale per sopperire alla struttura deficitaria della gestione tecnica, causata dalle modalità di determinazione dei premi che scontano a favore dell'assicurato parte del rendimento atteso della gestione patrimoniale e anche per quanto riguarda l'imputazione dei costi di struttura, generali e amministrativi.

3. LA GESTIONE DEI RISCHI

Le imprese di assicurazione presentano una particolarità rispetto alle altre imprese, ovvero l'inversione del ciclo produttivo che vede prima l'ottenimento dei ricavi e successivamente (solo se si verifica l'evento assicurato) il sostenimento dei costi, con la diretta implicazione della necessità di accantonare una somma per far fronte agli impegni futuri. Queste somme prendono il nome di *riserve tecniche* e rappresentano il *debito* che l'assicuratore ha *nei confronti dell'insieme degli assicurati*[30]. Prescindendo dal fatto che il concetto di riserva tecnica debba essere declinato a seconda che si faccia riferimento ai rami danni o ai rami vita, esse presentano tre caratteristiche generali[31]:

[28] Chapman (2006) suddivide il rischio operativo in 4 categorie ovvero i rischi operativi connessi alle strategie, alle persone, ai processi e ai sistemi ed infine quelli connessi ad eventi esterni. Prandi (2010) p. 66-70, pur non suddividendo i rischi nelle quattro categorie appena presentate ne fornisce un elenco molto completo. Hajek (2011), evidenzia come questa classificazione nasca dalla necessità di classificare i rischi che non trovano collocazione nelle altre categorie e che riguardano essenzialmente la filiera dei processi aziendali; in essi inoltre viene ricompreso il rischio giuridico ma non i rischi reputazionali o strategici.
[29] Cappiello (2018).
[30] Questo perché sul singolo non è possibile applicare la legge dei grandi numeri non avendo la certezza che la frequenza degli eventi corrisponda alla probabilità che questo si verifichi.
[31] Paci (2018).

- Sono *strumentali e congiunte all'assunzione dei rischi*, perché esse sono collegate alla vendita del prodotto ma non sono il prodotto (nascono a causa dello sfasamento temporale degli impegni tra le controparti);
- Sono *aleatorie*, perché dipendono dalle stime sui flussi futuri in entrata e in uscita al momento in cui si effettua la rilevazione[32];
- Sono *non negoziabili* in quanto *non sono sistematicamente scambiate nei mercati organizzati*. Nonostante non vi sia un vero e proprio mercato per queste passività, perché sono dei contratti non standardizzabili e trasferibili in attività finanziarie che replichino fedelmente i flussi di cassa su cui basare gli scambi, esistono dei meccanismi che permettono di creare un mercato. Stiamo parlando della riassicurazione e della cartolarizzazione attraverso le quali si assiste all'episodico trasferimento di parte dei rischi, soprattutto quelli da cui possono discendere impegni di importo elevato (ad esempio rischi catastrofali)[33].

Come detto, il concetto di riserva va declinato a seconda che si faccia riferimento ai rami danni o ai rami vita. Tale distinzione discende dal fatto che nei rami vita, essendo i contratti legati alla vita umana, sono di lunga durata ed è perciò necessario considerare un periodo di tempo molto lungo nel momento in cui si calcolano gli impegni assunti, nonché un congruo tasso d'interesse per la valutazione. Inoltre, la durata pluriennale fa sorgere la convenienza alla corresponsione da parte degli assicurati di premi periodici, con la conseguenza che i flussi da considerare non saranno più solamente quelli relativi alle prestazioni dell'impresa di assicurazione, ma anche quelli che riguardano il pagamento dei premi futuri da parte degli assicurati. La stima circa la probabilità che gli assicurati continuino ad adempiere ai propri obblighi verrà a dipendere dalla sopravvivenza dell'assicurato e dalla sua volontà di mantenere in essere il contratto o di interromperlo[34].

Così nei rami danni vengono definiti il numero di sinistri che si verificheranno e il loro ammontare, accantonando la parte di premio che fa riferimento ai rischi ancora coperti contrattualmente[35]. Non è però sufficiente determinare esclusivamente la parte di premio da rinviare agli esercizi futuri, ma si rivela necessario accantonare ulteriori somme che tengano conto di un possibile peggioramento della sinistrosità (quindi di errori circa la determinazione del premio di tariffazione), degli eventi che si verificano raramente ma che possono determinare ingenti

[32] Dipende dal momento della rilevazione in quanto le riserve vengono calcolate al termine dell'esercizio e, a meno che non sia intercorso alcun cambiamento sociale, economico o giuridico all'interno dell'arco temporale di riferimento (ipotesi irrealistica), non è possibile utilizzare le stesse basi tecniche e finanziarie utilizzate per il calcolo del premio.
[33] Paci (2018).
[34] Paci (2018).
[35] È la cosiddetta *riserva per frazioni di premi*. Paci (2018); Cappiello (2018); Prosperetti e Colavolpe (2012).

risarcimenti, del progressivo invecchiamento della popolazione[36] e dei sinistri avvenuti durante l'anno[37].

Per i rami vita la questione si complica a causa delle peculiarità su esposte: le riserve per questi rami sono strettamente collegate al calcolo del premio, in quanto quest'ultimo viene determinato attualizzando il valore dei futuri risarcimenti (base attuariale) con un dato tasso di interesse (base finanziaria o tasso tecnico). Nel momento in cui stipulano il contratto, agli assicurati viene riconosciuto un rendimento pari al tasso tecnico (rendimento che serve quindi per ottenere il capitale). Successivamente, a seguito dell'investimento, il valore della riserva aumenta per un importo pari al tasso tecnico che è proprio il rendimento da raggiungere affinché l'assicuratore possa adempiere alle proprie prestazioni[38].

La riserva più importante nei rami vita è la riserva matematica poiché fronteggia proprio i rischi puri, esprimendo il valore delle obbligazioni potenziali dell'impresa di assicurazione verso gli assicurati. Essa è pari alla differenza tra il valore attuariale degli impegni dell'impresa di assicurazione (ovvero il pagamento del capitale) e quello degli assicurati (cioè il pagamento dei premi)[39].

Affinché vi sia un equilibrio fra le prestazioni, l'assicurato ogni anno dovrebbe pagare quelli che vengono definiti come *premi naturali*[40], che si sostanziano in premi variabili e commisurati all'aumentare o al diminuire della probabilità di morte/sopravvivenza lungo il periodo contrattuale[41]. Nella prassi gli assicuratori applicano generalmente dei premi periodici costanti, ricavati dall'uguaglianza tra il premio unico[42] e la somma dei singoli premi attualizzati e ponderati per la probabilità che si verifichi l'evento[43].

---

[36] Si tratta rispettivamente della riserva p*er rischi in corso, della riserva di perequazione* e *della riserva di* senescenza. Cappiello (2018); Prosperetti e Colavolpe (2012).

[37] Questa prende il nome di *riserva sinistri* e oltre a rappresentare un accantonamento per i sinistri denunciati e non ancora liquidati considera anche quelli che si sono verificati ma che non sono stati ancora denunciati, dei sinistri dei precedenti esercizi e degli oneri di liquidazione. Paci (2018); Cappiello (2018); Prosperetti e Colavolpe (2012).

[38] Paci (2018).

[39] Cappiello (2018).

[40] Il premio naturale è un premio con orizzonte temporale di un anno che va a coprire gli impegni dell'assicuratore esattamente in quell'anno. Ad esempio, il premio naturale pagato in t=0 copre esattamente gli impegni dell'assicuratore nel corso del primo anno e così ancora, il premio pagato in t=2 è il premio che copre gli impegni dell'assicuratore durante il terzo anno (cioè dall'inizio di t=2 fino alla fine di t=2). La somma (attuariale) dei premi naturali è pari al premio unico.

[41] Nel caso morte, utilizzando premi naturali, l'assicurato pagherebbe meno ad inizio contratto mentre pagherebbe di più verso la scadenza visto l'aumentare della probabilità di decesso (situazione in netto contrasto con la naturale diminuzione dei redditi all'avanzare dell'età).

[42] È il premio che l'assicurato dovrebbe pagare in un'unica soluzione ed è calcolato come capitale assicurato attualizzato, ponderato per la probabilità (nel caso morte la probabilità utilizzata è quella che l'assicurato di n anni al tempo t=0 muoia a n+x anni).

[43] Dell'uguaglianza si conosce il premio unico (in quanto calcolato con il metodo descritto nella nota precedente), i fattori di attualizzazione dei singoli premi e le loro probabilità mentre non si conoscono gli importi dei premi. Con dei semplici passaggi matematici è possibile esplicitare l'equazione per i premi e dalla sua risoluzione si trova l'importo dei premi costanti che soddisfa l'uguaglianza e che quindi è pari al premio puro.

È chiaro quindi che le riserve, oltre ad assolvere agli obblighi di rispetto delle leggi di bilancio e dei principi contabili (in particolare della competenza), rappresentano degli accantonamenti che coprono quella parte di "perdita attesa" rappresentata dagli impegni futuri verso gli assicurati. Se l'impresa di assicurazione si trovasse a dover fronteggiare solamente perdite attese le riserve sarebbero sufficienti, tuttavia possono verificarsi situazioni impreviste alle quali l'impresa di assicurazione risponde attingendo direttamente dal proprio patrimonio e non con le riserve.

Risulta quindi fondamentale sviluppare un adeguato sistema di gestione dei rischi che, al fine di dare attuazione alle decisioni dei vertici aziendali, monitori costantemente i rischi e intervenga nel modo più tempestivo possibile. Le imprese dovranno perseguire una "gestione attiva" dei rischi (che non lascia alcuno spazio ad interventi sporadici) e non semplicemente una "gestione passiva" attraverso il mero trasferimento a terzi dei rischi. Dev'essere inoltre una gestione integrata che consideri ogni profilo del rischio, quale sia la loro correlazione e che coinvolga tutte le unità aziendali e non solamente i vertici.

4. LA NORMATIVA: SOLVENCY 2

La direttiva 2009/138/CE nota come *Solvency II*, entrata in vigore nel gennaio 2016, prende il posto della precedente normativa *Solvency I* in quanto quest'ultima, mostrava delle lacune a livello di armonizzazione tra gli stati membri e soprattutto, per quanto riguarda i margini di solvibilità[44]. *Solvency II* apporta perciò modifiche sostanziali sia per quanto concerne i requisiti patrimoniali e le metodologie di calcolo, sia per quanto riguarda l'intero sistema di vigilanza prudenziale. Tra i suoi obiettivi principali essa pone la tutela dei consumatori, un miglioramento nella gestione del rischio, la ricerca della massima trasparenza di mercato e l'armonizzazione dell'attività assicurativa a livello europeo. In particolare, essa ruota attorno a tre punti fondamentali chiamati *pilastri* (vedi Fig. 1.1):

- *Requisiti finanziari minimi a copertura dei rischi* che riguardano:
  - *Misurazione attivi e passivi*
  - *Calcolo delle riserve tecniche*
  - *Fondi propri di base*
  - *SCR e MCR*
- *Governance e Risk Management*

[44] Prevedeva infatti che il margine di solvibilità fosse calcolato come una percentuale della riserva matematica (nei rami vita) e come percentuale dei premi annui (nei rami danni). Si trattava di una metodologia a "pesi fissi" che non era in grado di svolgere un'adeguata funzione segnaletica perché presentava il chiaro limite di non tener conto dei rischi finanziari che possono influenzare l'andamento della compagnia. Guida IVASS (2016).

- *Requisiti informativi*

Fig. 1.1 – I tre pilastri di Solvency 2

PRIMO PILASTRO	SECONDO PILASTRO	TERZO PILASTRO
Calcolo delle riserve tecniche	Presidi di governance	informativa periodica
Criteri di valutazione di attivi e passivi	Regolare Autovalutazione dei dei propri rischi e della propria posizione di solvibilità (Own Risk and Solvency Assessment, ORSA)	report alle autorità di vigilanza
Solvency Capital Requirement (SCR)	supervisory review process da parte delle autorità di vigilanza e imposizione di eventuali aumenti dei requisiti patrimoniali	report al mercato
Minimum Capital Requirement (MCR)		informativa non periodica in caso di eventi straordinari o durante le ispezioni di vigilanza

Fonte: Nostra elaborazione

È proprio il controllo e il governo del rischio l'aspetto che più di tutti caratterizza la normativa, introducendo modifiche sostanziali in tale ambito[45]. Così, l'art. 44.1 della direttiva *Solvency II* definisce il sistema di gestione dei rischi come, l'insieme di «…Strategie, processi e procedure di segnalazione per individuare, misurare, monitorare, gestire e segnalare su base continuativa i rischi a livello individuale e aggregato…»[46] e continua poi al comma 2, disponendo che esso è correttamente integrato nella struttura organizzativa e nei processi decisionali dell'impresa. La disciplina individua in modo preciso le diverse fasi in cui si articolano il controllo e la gestione dei rischi (individuazione, misurazione, controllo periodico e gestione) disponendo che tale attività sia effettuata in maniera continuativa e che vengano considerati non solo i rischi attuali, ma anche quelli prospettici, sia singolarmente che nel loro insieme. Inoltre, risulta fondamentale il raggiungimento del *data quality*, ovvero si richiede che i dati raccolti per attuare l'implementazione di tale sistema siano *accurati*, *completi* e *appropriati*[47].

Lo stesso art. 44 al paragrafo 2 richiede che siano considerate almeno le seguenti aree, per le quali il CAP richiede all'art. 30-bis comma 4 una politica scritta approvata dal consiglio di amministrazione[48]:

[45] Trombetti (2017).
[46] Art. 44.1 direttiva *Solvency II*.
[47] Paci (2018).
[48] Paci (2018), p. 102-104.

- *Sottoscrizione e costituzione delle riserve*. La prima concerne il rischio tariffario ed è previsto che per ogni nuova tariffa si valutino i rischi assicurabili, le ipotesi alla base del calcolo del premio e la redditività della stessa. Per quanto riguarda invece le riserve l'impresa è tenuta alla redazione annuale di una relazione sulle riserve a chiusura dell'esercizio che evidenzi valutazioni, procedimenti, controlli operati e ipotesi di calcolo utilizzate;
- *Gestione integrata di attività e passività (asset liability-management)*. Si analizza il disallineamento strutturale tra attività e passività calcolandone la durata analizzando eventuali correlazioni tra i rischi di diverse categorie di attività e passività e fra le diverse obbligazioni e l'effetto delle tecniche di attenuazione del rischio;
- *Investimenti*. Devono essere indicati i provvedimenti in base ai quali l'impresa controlla che gli investimenti tengano conto della natura dell'attività dell'impresa, dei limiti di tolleranza al rischio approvati, della sua posizione di solvibilità e della sua esposizione al rischio a lungo termine, della valutazione interna del rischio di credito delle controparti degli investimenti[49];
- *Gestione dei rischi di liquidità e di concentrazione*. Per quanto riguarda il primo è necessario indicare i provvedimenti che vengono adottati nei confronti del rischio di liquidità a breve e a lungo termine, mentre per il secondo devono essere indicati i provvedimenti che sono adottati per individuare le fonti di rischio di concentrazione e i provvedimenti per analizzare i rischi di contagio nel caso di concentrazione delle esposizioni;
- *Gestione dei rischi operativi*. Per la loro gestione risulta necessario indicare in modo chiaro le responsabilità spettanti ai soggetti incaricati dell'individuazione e del monitoraggio di tale rischio;
- *Riassicurazione e altre tecniche di mitigazione del rischio*. Dovrà essere indicato come si intende procedere per garantire la selezione di una riassicurazione adeguata e/o di altre tecniche per l'attenuazione del rischio.

4.1 Calcolo delle riserve, valutazione attività e passività

Nello svolgere la sua attività l'assicuratore deve innanzitutto detenere i mezzi necessari per far fronte agli impegni futuri accantonando alle già menzionate riserve le somme riscosse attraverso i premi. Queste risorse devono essere investite sia per garantire i rendimenti già concessi agli assicurati

[49] Paci (2018), p. 103.

sia per generare utili con cui remunerare la propria attività e, in tale circostanza, il rischio di un mancato assolvimento alle proprie obbligazioni, può riguardare tanto il fronte dell'insufficienza delle riserve quanto il fronte degli attivi a copertura delle stesse.

Si precisa poi come la regolamentazione parli in generale di investimenti, piuttosto che di attivi a copertura delle riserve tecniche, dal momento che il termine "investimenti" rappresenta una categoria generale al cui interno ritroviamo gli attivi a copertura. L'attuale normativa non fissa più dei vincoli quantitativi precisi all'attivo, bensì lascia all'impresa di assicurazione la possibilità di attuare le politiche di investimento che ritiene più consone ai propri obiettivi, stabilendo però che questi debbano essere effettuati secondo il *principio della persona prudente*.

Nell'art. 37-ter del CAP viene sancito tale principio per gli investimenti, poi ulteriormente ampliato dall'art. 38 con particolare riferimento agli attivi a copertura, mettendo in evidenza come sia necessario formalizzare una strategia di investimento commisurata alla natura dei rischi e delle obbligazioni assunte, privilegiando al contempo l'interesse degli assicurati (comma 1-bis), imponendo un'adeguata diversificazione (comma 3 art. 37-ter lettera c) e delineando le tre caratteristiche essenziali degli investimenti, vale a dire liquidità, redditività e sicurezza (comma 2 art. 37-ter lettera b)[50].

La regola di base richiede che gli attivi a copertura debbano essere almeno pari al valore delle riserve tecniche dal momento che essi rappresentano la garanzia della capacità dell'impresa di adempiere alle proprie obbligazioni verso gli assicurati. Ciò è perfettamente in linea con la definizione di prudenza e con finalità principale perseguita dalle autorità di vigilanza, ovvero quella di tutela degli assicurati.

In riferimento ai metodi di valutazione degli attivi *Solvency II* impone con l'art. 75, che «le attività siano valutate all'importo al quale potrebbero essere scambiate tra parti consapevoli e consenzienti in un'operazione svolta a normali condizioni di Mercato»[51]. Risulta quindi evidente che la normativa adotta un approccio *market consistent* valutando cioè attivi e passivi a valori di mercato e, laddove non risulta possibile individuare tali valori, ammette l'uso di tecniche di tipo *mark to model* basate su benchmark che si avvicinino agli input di mercato[52].

Regole puntuali vengono poi disposte per quanto concerne le riserve tecniche: viene stabilito all'art. 76 che il loro valore «…corrisponde all'importo attuale che le imprese di assicurazione e di riassicurazione dovrebbero pagare se dovessero trasferire immediatamente le loro obbligazioni… a

[50] Cappiello (2018) specifica che la *redditività* e la capacità di un determinato investimento patrimoniale di produrre adeguati flussi reddituali, la *sicurezza* riguarda l'attitudine dello stesso a conservare immutato il proprio valore economico nel tempo e infine la *liquidità* fa riferimento alla capacità dell'investimento di essere smobilizzato con facilità.
[51] Art. 75 *Solvency II*.
[52] Hajek (2011).

un'altra impresa di assicurazione o di riassicurazione»[53]. Il valore di mercato utilizzato è quindi il *current exit value* e si evince immediatamente come l'utilizzo di tale metodo comporti una non facile integrazione con i principi contabili internazionali, in quanto il *fair value* considerato da questi ultimi diverge da quello considerato da *Solvency II*[54].

La direttiva continua negli articoli seguenti specificando che le riserve tecniche sono date dalla somma della miglior stima e del margine di rischio (art. 77.1). Per quanto riguarda la *Best Estimate* si specifica nell'art. 77.2 che essa «…corrisponde alla media dei flussi di cassa futuri ponderata con la probabilità, tenendo conto del valore temporale del denaro (valore attuale atteso dei flussi di cassa futuri) sulla base della pertinente struttura per scadenza dei tassi di rischio»[55] mentre, nell'art.77.3 si dispone che il *Risk Margin* «…è tale da garantire che il valore delle riserve tecniche sia equivalente all'importo di cui le imprese di assicurazione e di riassicurazione avrebbero bisogno per assumersi e onorare le obbligazioni di assicurazione e di riassicurazione»[56].

Il margine di rischio rappresenta quindi il *surplus* che cautela e remunera il costo dell'incertezza e che previene un errore di calcolo della *best estimate* e inoltre, può essere definito come il costo sostenuto da un altro soggetto affinché questo decida di assumersi i rischi oggetto di cessione[57].

Tale osservazione trova conferma nell'art. 77.5 che dispone che «…il margine di rischio è calcolato determinando il costo della costituzione di un importo di fondi propri ammissibili pari al requisito patrimoniale di solvibilità necessario per far fronte alle obbligazioni di assicurazione e di riassicurazione per tutta la loro durata di vita»[58] da cui si evince inoltre come esso venga calcolato attraverso il criterio del *costo del capitale* ovvero del costo del capitale necessario per assolvere agli impegni futuri nei confronti degli assicurati.

Infine, la direttiva prevede all'art. 80 che «Quando calcolano le loro riserve tecniche, le imprese di assicurazione e di riassicurazione segmentano le loro obbligazioni di assicurazione e di riassicurazione in gruppi di rischi omogenei e quanto meno per aree di attività»[59] sancendo quindi il principio della segmentazione che prevede che il contratto sia scomposto al fine di evidenziare i rischi insiti nello stesso (*unbundling*) per poi aggregarli in gruppi omogenei di rischio secondo le *Line of Business* (*LoB*).

---

[53] Art. 76 *Solvency II*.
[54] Il principio contabile di riferimento per il fair value è l'IFRS 4. Lo IAS 39 paragrafo 9 definisce il fair value come "il corrispettivo al quale un'attività può essere ceduta o una passività può essere trasferita in una libera transazione fra parti consapevoli e disponibili".
[55] Art. 77.2 *Solvency II*.
[56] Art. 77.3 *Solvency II*.
[57] Cappiello (2018).
[58] Art. 77.5 *Solvency II*.
[59] Art. 80 *Solvency II*.

4.2 SCR, MCR e fondi propri ammissibili

La direttiva *Solvency II* prevede che l'impresa di assicurazione debba rispettare determinati requisiti patrimoniali durante lo svolgimento della sua attività. In particolare, prevede due requisiti di capitale, il *Solvency Capital Requirement* (*SCR*) e il *Minimum Capital Requirement* (*MCR*).

L'SCR rappresenta la parte di capitale che l'impresa deve detenere al fine di garantire la propria solvibilità ovverosia il capitale destinato alla copertura delle perdite inattese. Agli artt. 100 e 101 della direttiva recepiti dagli artt. 45-bis e 45-ter CAP, si dispone che esso venga calcolato in base al presupposto di continuità aziendale, che vengano presi in considerazione tutti i rischi quantificabili a cui l'impresa è esposta e che esso sia destinato a coprire l'attività esistente e le nuove attività con orizzonte temporale di dodici mesi. L'impresa di assicurazione dovrà quindi detenere fondi propri ammissibili sufficienti a coprire l'SCR ed è inoltre stabilito che quest'ultimo corrisponda «al valore a rischio dei fondi propri di base dell'impresa soggetto a un livello di confidenza del 99,5% su un periodo di un anno»[60].

Operativamente esso è determinato come differenza tra il patrimonio calcolato valutando attività e passività in base ai criteri di vigilanza (stato patrimoniale di vigilanza) e il patrimonio calcolato con la stessa metodologia ma ipotizzando una *condizione di stress*, ovvero un aumento istantaneo e permanente di uno dei rischi precedentemente elencati (ad esempio si ipotizza un aumento del 15% della mortalità)[61].

All'impresa di assicurazione viene poi data la possibilità di calcolare tale requisito mediante formula standard o attraverso dei modelli interni. Nello specifico, la *formula standard* stabilisce che l'SCR sia dato dalla somma di tre componenti:

- *SCR di Base* (*BSCR*)
- *Aggiustamento per la capacità di assorbimento delle perdite* (*ADJ*) che possono dipendere da:
    - *Assorbimenti delle perdite che derivano dalle partecipazioni agli utili* se ad esempio sono stati stipulati contratti che consentono di condividere con gli assicurati utili e perdite, perché in questo secondo caso sarà necessario detenere meno patrimonio;
    - *Assorbimenti che derivano dall'esistenza d'imposte differite* se ad esempio si vantano crediti d'imposta derivanti dagli esercizi precedenti è possibile ridurre le perdite;
- *Rischi operativi* (*SCR_{op}*)

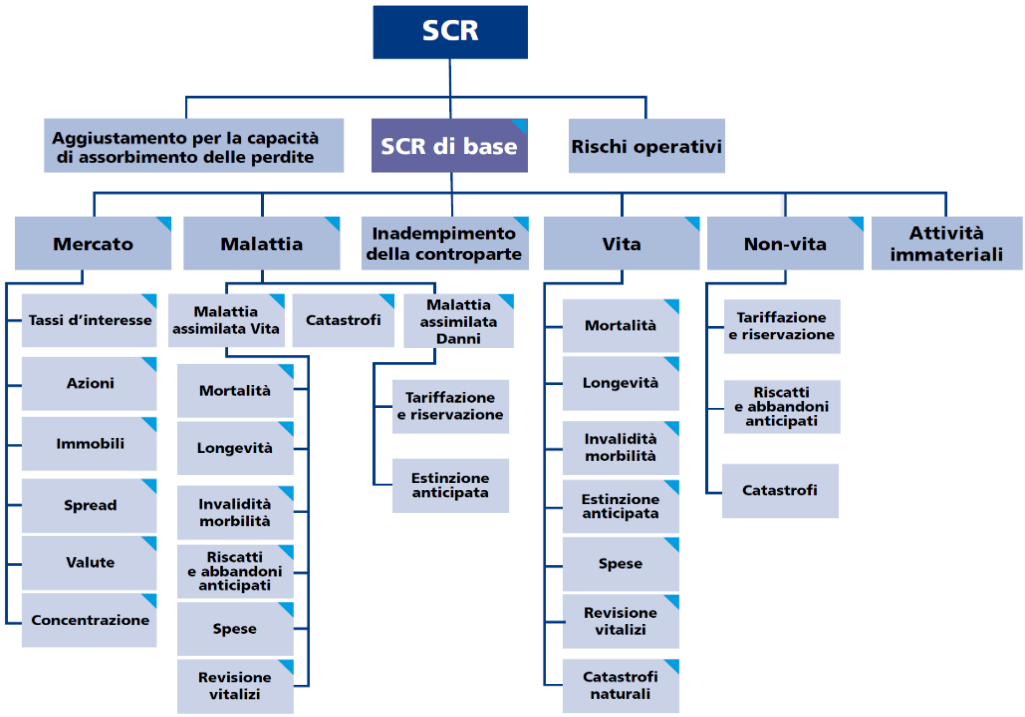
[60] Art. 45 CAP.
[61] Paci (2018).

La normativa classifica quindi i rischi in base a *moduli* e *sottomoduli*, in modo da determinare per ogni possibile rischio un requisito patrimoniale e tiene conto anche della correlazione tra i rischi i cui coefficienti sono determinati dalle *tabelle di correlazione*. La componente principale dell'SCR è il BSCR che è costituito dai seguenti moduli:

- $SCR_{mercato}$ che è il requisito patrimoniale per il rischio di mercato
- $SCR_{malattia}$ che è il requisito patrimoniale per il rischio malattia
- $SCR_{controparte}$ che è il requisito patrimoniale per il rischio di controparte
- SCR_{vita} che è il requisito patrimoniale per il rischio di sottoscrizione vita
- $SCR_{non\text{-}vita}$ che è il requisito patrimoniale per il rischio di sottoscrizione danni
- $SCR_{attività\ immateriali}$ che è il requisito patrimoniale per il rischio collegato alle attività immateriali

Si sottolinea che la disciplina tende a favorire l'uso di modelli interni piuttosto che il metodo standard, sia perché esso permette di costituire un patrimonio ottimale e potenzialmente inferiore a quello richiesto dal metodo standard (in quanto calcolato con una procedura ad hoc), sia perché spingono le imprese di assicurazione a ricercare una maggiore cultura nella gestione del rischio[62].

Fig. 1.2 – Moduli e sottomoduli SCR



Fonte: Guida semplificata IVASS (2016)

[62] Paci (2018), p. 83; Guida IVASS (2016).

Solvency II predispone quindi un elenco dei rischi che devono essere tenuti in considerazione da parte delle imprese di assicurazione in sede di calcolo dell'SCR (vedi Fig. 1.2):

- *Rischi di sottoscrizione vita*, dipendono da:
  - *Rischio di mortalità*, ovvero il rischio che le previsioni statistiche circa la mortalità siano errate;
  - *Rischio di longevità*, ovvero il rischio che le previsioni statistiche circa la sopravvivenza degli assicurati siano errate;
  - *Rischio di invalidità e morbilità*, ovvero che aumentino gli infortuni e/o che sorgano nuove malattie;
  - *Rischio di spesa*, ovvero il rischio di sostenere costi di gestione delle polizze non previsti;
  - *Rischio di revisione*, ovvero il rischio che cambiamenti normativi impongano obblighi contrattuali aggiuntivi a favore dell'assicurato;
  - *Rischio di estinzione anticipata*, che discende dalla possibilità che l'assicurato estingua la polizza anticipatamente;
  - *Rischio catastrofale ramo vita*, ovvero il rischio che una catastrofe quale ad esempio terremoto o alluvione produca danni alle persone;
- *Rischi di sottoscrizione rami danni*, che derivano dall'assunzione da parte della compagnia di rischi in tale ambito:
  - *Rischio di tariffazione*, ovvero il rischio di sbagliare la determinazione dei premi a causa di una sottotariffazione[63];
  - *Rischio di riservazione*, ovvero il rischio di sbagliare la stima dei sinistri che dovrò pagare a causa di una sovrasinistrosità;
  - *Rischio che le riserve tecniche siano insufficienti*, è un rischio che discende direttamente dai precedenti due e in particolare, dal rischio di tariffazione, deriva la possibilità di sbagliare il calcolo della riserva premi mentre, dal rischio di riservazione, deriva la possibilità di sbagliare il calcolo della riserva sinistri;
  - *Rischio catastrofale rami danni* che, come nel caso del ramo vita, si tratta di un evento catastrofale che comporta elevate richieste di risarcimento;
- *Rischio operativo*;

[63] A. Cappiello (2018), fa riferimento ad una sottotariffazione *volontaria* nel caso in cui la compagnia applichi consapevolmente un premio di tariffa non in linea con le ipotesi attuariali o *involontaria*, nel caso in cui questo derivi esclusivamente da uno scostamento tra statistiche e risultati effettivi e/o tra rendimenti attesi ed effettivi.

- *Rischio di mercato* e i suoi sottomoduli:
    - *Rischio di tasso d'interesse*. Si tratta di un rischio che assume maggiore importanza nelle assicurazioni vita e di capitalizzazione piuttosto che nelle assicurazioni danni, visto che per queste ultime non è riconosciuto contrattualmente un interesse.
    - *Rischio azionario*;
    - *Rischio immobiliare*;
    - *Rischio di cambio* (o *rischio valuta*);
    - *Rischio spread*;
- *Rischio di concentrazione del rischio di mercato*, si tratta del rischio che si sostiene se non si diversifica adeguatamente il proprio portafoglio in quanto, così facendo, si avrebbe un'unica grande esposizione nei confronti di un unico emittente di titoli o di un gruppo di titoli. Esso discende ovviamente dal rischio di mercato;
- *Rischio di liquidità*, il rischio che l'impresa di assicurazione o di riassicurazione non sia in grado di liquidare investimenti ed altre attività per regolare le proprie obbligazioni finanziarie quando queste ultime scadono[64];
- *Rischio di controparte*, che nel campo assicurativo, assume importanza soprattutto in riferimento agli accordi di riassicurazione. l'EIOPA attua una distinzione tra due tipi di esposizioni ovvero, quelle diversificabili e per le quali è possibile attribuire alla controparte un rating (chiamate di tipo 1) e quelle invece non diversificabili per le quali invece non è possibile attribuire un rating alla controparte (chiamate di tipo 2)[65].

Per quanto riguarda invece l'MCR, viene stabilito all'art. 47-ter del CAP che esso rappresenta il capitale minimo «…al di sotto del quale I contraenti, i beneficiari, gli assicurati e gli altri aventi diritto alle prestazioni assicurative sarebbero esposti a un livello di rischio inaccettabile qualora all'impresa assicurativa fosse consentito di continuare la propria attività»[66]. Lo stesso articolo stabilisce poi che esso dev'essere compreso tra il 25% e il 45% dell'SCR e, all'interno di questo intervallo, l'MCR viene calcolato «…utilizzando una funzione lineare calibrata sul valore a rischio

[64] Art. 13, comma 34, direttiva 2009/138/CE.
[65] Si specifica che al primo tipo di esposizioni appartengono ad esempio le modalità di riassicurazione, la cartolarizzazione e i derivati, gli averi in banca e ogni altro contratto per l'attenuazione dei rischi mentre, per la seconda categoria di esposizioni, ci si riferisce ad esempio ai crediti da riscuotere da parte degli intermediari e ai debitori in possesso di una polizza. Hajek (2011).
[66] Art. 47-ter CAP.

dei fondi propri di base dell'impresa con un intervallo di confidenza dell'85% su un periodo di un anno»[67]. Sono inoltre previsti dei minimi assoluti[68]:

- 2,5 milioni per le imprese che operano esclusivamente nei rami danni;
- 3,7 milioni per le imprese che operano esclusivamente nei rami vita;
- 6,2 per le imprese che operano in entrambi i rami.

Si ricorda inoltre che non tutti i fondi sono adatti alla costituzione dei requisiti patrimoniali e la disciplina indica espressamente quali di questi possono essere utilizzati. In particolare, si individuano due tipologie di fondi propri ammissibili[69]:

- *Fondi propri di base* costituiti dalla differenza fra attività e passività, con l'aggiunta delle passività subordinate;
- *Fondi propri accessori*, ovvero ulteriori elementi che possono assorbire perdite.

I fondi propri vengono classificati in 3 livelli (*tier*) a seconda della loro capacità di assorbimento delle perdite[70]:

- *Disponibilità permanente*, se la posta è in grado di essere sempre disponibile per coprire le perdite;
- *Subordinazione* se, nel caso in cui la posta debba essere rimborsata, lo sarà dopo tutte le altre;
- *Assenza di obblighi, incentivi al rimborso e gravami*, significa cioè che questa posta deve essere libera da qualsiasi vincolo che ne possa compromettere l'utilizzo per la copertura di perdite.

I fondi propri accessori possono appartenere solamente al *tier 2* e al *tier 3* mentre, i fondi propri di base, possono appartenere ad uno qualsiasi dei tre *tier*: infatti, se dispongono di tutte e tre le caratteristiche apparterranno al tier 1 se ne presentano solamente due al *tier 2* mentre il resto finisce invece nel *tier 3*. Si specifica che il *tier 1* si suddivide in due classi a seconda che si parli di elementi di migliore qualità o di minor qualità:

- *Fondi utilizzabili senza restrizioni* (*unrestricted tier 1*) che comprendono il capitale sociale versato, le riserve utili e la riserva di riconciliazione;

[67] Art. 47-ter CAP.
[68] Paci (2018), p. 121.
[69] Paci (2018).
[70] Paci, (2018); Cappiello (2018).

- *Fondi utilizzabili con restrizioni* (*restricted tier 1*) nei quali vi rientrano gli altri fondi propri di base come le azioni privilegiate e le passività subordinate.

La normativa disciplina in modo puntuale la composizione sia dell'SCR che dell'MCR, indicando chiaramente le percentuali dei fondi propri di base e dei fondi accessori, poiché non si vuole correre il rischio che le imprese di assicurazione abbiano un patrimonio che sia quantitativamente ma non qualitativamente adeguato.

CAPITOLO 2
L'ENTERPRISE RISK MANAGEMENT

1. SVILUPPO DEL RISK MANAGEMENT: DALL'INSURANCE RISK MANAGEMENT ALL'ERM

La propensione alla mitigazione dei rischi ha subito attraverso i secoli innumerevoli cambiamenti: dalla semplice mutualità ad accordi di assicurazione, fino ad approdare al risk management e alla sua forma odierna più evoluta chiamata Enterprise Risk Management[71].

Storicamente l'assicurazione e le sue continue evoluzioni hanno caratterizzato le tecniche di gestione del rischio addirittura dall'VIII secolo a.C. a partire dai Fenici: questi infatti utilizzavano una forma di copertura che prevedeva che il debitore rendesse l'importo preso a prestito al creditore se e solo se la merce oggetto dell'accordo avesse raggiunto intatta il porto di destinazione. Le prime vere e proprie polizze assicurative nacquero però a metà del XIV secolo nelle repubbliche marinare e riguardavano sostanzialmente i trasporti marittimi. Fu solo a seguito del grande incendio di Londra del 1666 che esse furono allargate anche alla copertura di danni derivanti da catastrofi individuali e collettive e grazie allo sviluppo delle tecniche di calcolo probabilistico del XVII secolo, videro la luce le prime assicurazioni vita. Di un vero e proprio risk management si iniziò però a parlarne solamente a partire dal secondo dopoguerra, in particolare nel 1956 quando venne pubblicato il primo articolo scientifico in cui si utilizzava espressamente il termine "risk management"[72], ma si sottolinea che i primi veri tentativi di realizzare operativamente una gestione dei rischi, videro gli albori solamente negli anni Settanta quando si cominciò a ritenere che l'assicurazione non fosse più l'unico strumento per assolvere a tale scopo[73].

L'elemento che ha permesso la continua evoluzione di tale sistema è rappresentato dal crescente interesse verso il calcolo statistico che, come afferma Peter Bernstein (1998), ha permesso di «scritturare il passato per prevedere possibili futuri»[74]. L'idea di gestire il rischio assume quindi un carattere logico e coerente all'incertezza del futuro, che consente di vivere in modo più prudente e produttivo, evitando inutili sprechi di risorse e che va oltre la fortuna perché, continua Bernstein, «se tutto è una questione di fortuna allora la gestione del rischio è un esercizio insignificante. Invocare la

[71] Prandi (2010).
[72] L'opera a cui si fa riferimento è quella di Gallagher Russel, *Risk Management: A New phase of Cost Control*, Harvard Business Review 1956.
[73] Prandi (2010).
[74] Peter Bernstein (1998).

fortuna oscura la verità, perché separa un evento dalla sua causa»[75]. Al di là del calcolo statistico, ogni decisione riguardante il rischio è composta da due elementi inseparabili ovvero l'aspettativa soggettiva circa il guadagno o la perdita e il fatto oggettivo che si verificherà e quindi, l'essenza del risk management si sostanzia nella massimizzazione delle aree in cui si ha un controllo e nella minimizzazione delle aree in cui non si ha alcun controllo, in modo tale che le aspettative convergano all'evento che si verificherà[76].

Da questo breve excursus storico possiamo notare come inizialmente i modelli di gestione del rischio fossero essenzialmente volti alla prevenzione e alla mitigazione (si parla infatti di *Insurance Risk Management*) piuttosto che ad una proattività nei confronti del rischio (*Risk Management*) e che il cambiamento di *mindset* rispetto al rischio (da evento esclusivamente negativo a opportunità) sia l'elemento chiave per una svolta verso una gestione attiva.

Analizzando i primi processi di risk management degli anni Settanta, si nota immediatamente come il processo di gestione sia stato tradizionalmente segmentato e affidato ad ogni singola *business unit*, in un'attività che potremmo definire *silos by silos*, un'immagine che ben rappresenta la concezione di gestione del rischio di quegli anni[77]. Questo impianto a compartimenti discende da precisi aspetti comportamentali e dalla prassi organizzativa aziendale. La nostra mente infatti, si approccia al *problem solving* suddividendo il problema in sottogruppi e risolvendoli uno alla volta[78] e allo stesso modo, per gestire un'attività imprenditoriale, si attua una suddivisione in aree di gestione: emerge la tendenza a voler dividere i rischi in categorie distinte, reciprocamente esclusive, perché questo sembrerebbe essere il risultato del modo in cui suddividiamo i problemi per gestirli. Tutto ciò ha spinto le imprese ad allocare compiti specifici all'interno di ogni singola *business unit* con l'assunto sottostante che le conseguenze di un evento imprevisto sarebbero state più o meno limitate a una determinata area[79].

Ciò che mancava per procedere allo step successivo era capire che il rischio doveva essere percepito non più come un qualcosa da cui proteggersi (*down-side risk*), ma piuttosto come un'opportunità (*up-side risk*), perché solamente assumendo rischi maggiori è possibile migliorare le proprie performance. È perciò necessario che le imprese capiscano quali rischi stiano correndo, come questi siano correlati tra loro e come il sorgere di un rischio in un'area di business possa pregiudicarne

[75] Bernstein (1998).
[76] Bernstein (1998). Si veda anche Fraser e Simkins (2010), p. 20.
[77] Prandi (2010).
[78] Come afferma Thaler (1985 e 1999) gli individui organizzano, valutano e tengono il conto delle operazioni economico finanziarie in un processo chiamato *mental accounting* (termine coniato da Kahneman e Tversky nel 1984). In questo modo, per risolvere il problema di come allocare le risorse a disposizione lo si segmenta e lo si divide in conti mentali ognuno dei quali preposto ad un preciso scopo. Gardenal e Rigoni (2016), p. 56-65.
[79] Chapman (2006).

la redditività nelle altre[80]. in conclusione, non ci si dovrebbe preoccupare del down-side risk (minaccia) quanto piuttosto dell'up-side risk (opportunità), perché l'assunzione di rischi "corretti" comporta un maggior valore per l'impresa. Rischio e opportunità devono ricevere perciò la stessa attenzione e il consiglio di amministrazione deve ricercarne il corretto bilanciamento[81].

Come afferma il National Audit Office infatti, «un approccio di business risk management offre la possibilità di raggiungere un equilibrio ragionevole e sistematicamente sostenuto tra rischi e opportunità sotto forma di pressioni contraddittorie, per una maggiore imprenditorialità da un lato e per una limitazione dei rischi a ribasso dall'altro»[82]. Anche Knight e Petty (2001) sottolineano che la gestione dei rischi riguarda l'up-side risk e le opportunità che esso comporta, enfatizzando il fatto che sbarazzarsi del rischio soffocherebbe la fonte della creazione di valore e del potenziale positivo. Di conseguenza un comportamento che cerca di evitare il rischio porterà alla decisione meno razionale di tutte, ovvero non fare nulla e perciò il rischio diventerebbe non un motivo di azione, bensì una restrizione all'azione. Il risk management riguarderebbe quindi il controllo del rischio al fine di massimizzarne l'opportunità[83].

È proprio da queste considerazioni e dall'inefficienza del processo *silos by silos*, che possiamo far risalire la nascita dell'Enterprise Risk Management: così il *Committee of Sponsoring Organizations of the Treadway Commission* (*CoSO*) nel 1992 ha pubblicato il proprio studio in merito, dal titolo *Internal Control - Integrated Framework* con lo scopo di fornire delle linee guida comuni per tutte imprese. È proprio la parola "*integrato*" che rappresenta la chiave di lettura di questa metodologia di gestione che comporta un approccio sistematico, che guarda il rischio dall'alto e che considera anche e soprattutto le relazioni esistenti tra i vari rischi. Non si tratta più di demandare la valutazione e la gestione dei rischi ad ogni singola unità organizzativa, ma si tratta altresì di un processo che coinvolge tutta l'azienda e che si pone l'obiettivo di creare una vera e propria cultura del rischio (si parla infatti di *risk awareness*, di *consapevolezza del rischio*) in modo tale che tutte le funzioni e le aree aziendali ne siano pervase.

[80] Chapman (2006); Prandi (2010).
[81] Chapman (2006).
[82] National Audit Office (2000).
[83] Knight e Petty (2001); Chapman (2006).

2. STANDARD DI RIFERIMENTO: LINEE GUIDA

2.1. *Committee of Sponsoring Organizations of the Treadway Commission* (*CoSO*)

Grazie al *Committee of Sponsoring Organizations of the Treadway Commission* (*CoSO*) nel 1992, è stato fatto un primo passo per la definizione di uno standard che potesse essere seguito da qualsiasi impresa per quanto riguarda la gestione integrata del rischio. Nato dalla *Treadway commission* (il cui nome completo è *National Commission on Fraudolent Financial Reporting*), il CoSo ha assolto fin da subito al delicato compito di «realizzare uno studio teorico basato sulla dottrina esistente in tema di controlli interni»[84]. Il Report del 1992 *Internal Control - Integrated Framework*, per la prima volta evidenzia gli elementi cardine su cui il sistema di controllo interno deve poggiare.

«Il controllo interno, in base alla definizione proposta dal CoSO, è un processo, svolto dal consiglio di amministrazione, dai dirigenti e da altri operatori della struttura aziendale, che si prefigge lo scopo di fornire una ragionevole sicurezza sulla realizzazione di efficacia ed efficienza delle attività operative (*operations*); attendibilità delle informazioni di bilancio (*financial reporting*); conformità alle leggi e ai regolamenti in vigore (*compliance*)»[85].

Il Report mostrava però dei limiti perché se da un lato riduceva i rischi di comportamenti fraudolenti e permetteva una maggiore conformità alla normativa, dall'altro non identificava e tantomeno valutava quali fossero i rischi che le imprese dovevano sottoporre a controllo: infatti, lo standard iniziale pose l'accento sull'*Audit* come forza motrice del *risk management*[86].

Così nel 2004 il CoSO ha pubblicato un nuovo elaborato dal titolo *Enterprise Risk Management – Integrated Framework* nel quale il concetto di "controllo" è stato inglobato nel più grande concetto di "gestione dei rischi". L'ERM viene così definito

«…un processo, posto in essere dal consiglio di amministrazione, dal management e da altri operatori della struttura aziendale; utilizzato per la formulazione delle strategie in tutta l'organizzazione; progettato per individuare eventi potenziali che possono influire sull'attività

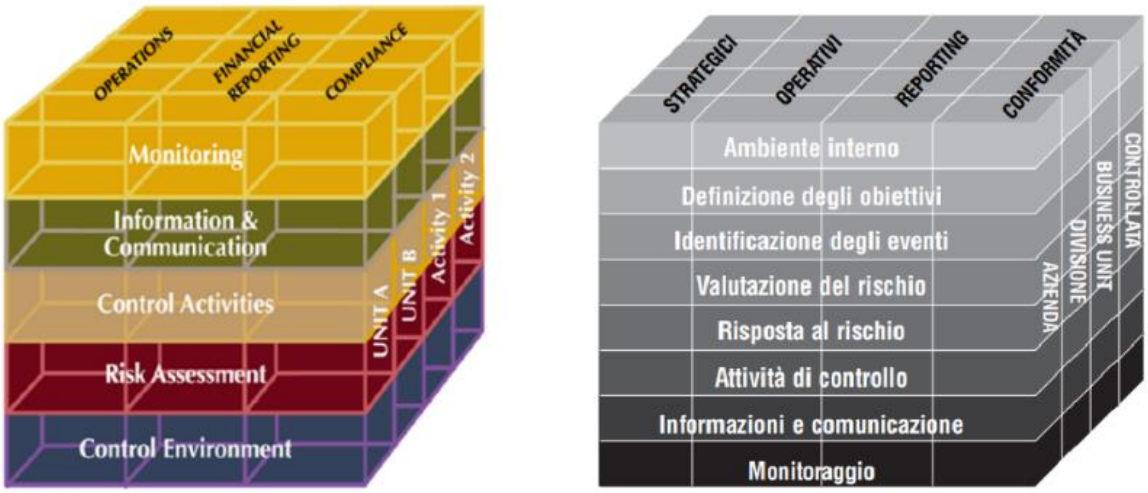
[84] Gasparri (2013).
[85] Gasparri (2013).
[86] Williams (marzo 2019).

aziendale, per gestire il rischio entro i limiti del rischio accettabile e per fornire una ragionevole sicurezza sul conseguimento degli obiettivi aziendali»[87].

Da questa definizione è possibile estrapolare i concetti fondamentali che tale approccio propone[88]: È un processo continuo che riguarda tutta l'organizzazione; è svolto da individui che occupano posizioni in tutti i livelli aziendali; è utilizzato per la formulazione di strategie; Racchiude una visione del rischio che riguarda l'azienda nel complesso; Identifica i rischi e li gestisce entro i limiti del rischio accettabile; Fornisce sicurezza al *management*.

Per meglio comprendere come obiettivi, struttura organizzativa e attività siano collegati in un'ottica di ERM il CoSo utilizza una matrice tridimensionale che prende il nome di *CoSo Cube* (vedi Fig. 2.1).

Fig. 2.1 – CoSO Cube 1992 e CoSO Cube 2004



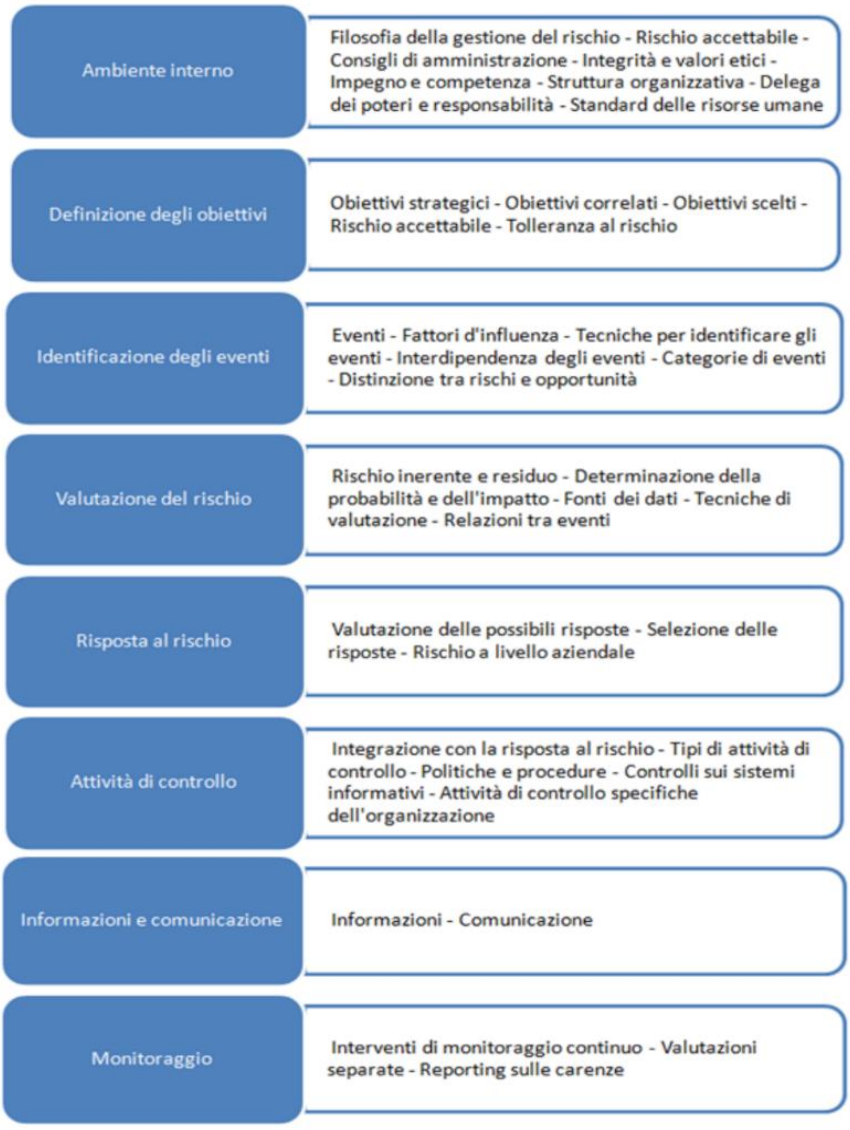
Fonte: rielaborazione grafica PWC (2013); CoSO 2004, Associazione Italiana Internal Auditors e PWC (2006)

Dall'immagine si può notare chiaramente come il *CoSO Cube* del 2004 (a destra) intenda dare una svolta strategica alla gestione del rischio anche se, resta comunque un framework che si adatta meglio alle imprese in cui il rischio è guidato dall'*audit*, in quanto è proprio su questo aspetto che continua a focalizzarsi: l'inserimento della "strategia" fra gli obiettivi serviva solo a garantire che le strategie aziendali si allineassero alle attività operative, alle attendibilità delle informazioni di bilancio e alla conformità a leggi e regolamenti[89].

[87] Associazione Italiana Internal Auditors e PricewaterhouseCoopers (2006), Il Sole 24 ore.
[88] Elenco tratto da Associazione Italiana Internal Auditors e PricewaterhouseCoopers (2006), Il Sole 24 ore.
[89] Williams (marzo 2019).

Rispetto al precedente Report, i nuovi elementi che vengono considerati sono (vedi Fig. 2.2): la *definizione degli obiettivi* (obiettivi aziendali e definizione del rischio sopportabile); l'*identificazione degli eventi*, ovvero si riferisce alla rilevazione dei rischi derivanti da eventi interni o esterni all'impresa; ed infine la *risposta al rischio* che indica le modalità con cui il management intente procedere e gli strumenti che utilizzerà per mantenere il rischio ad un livello "accettabile".

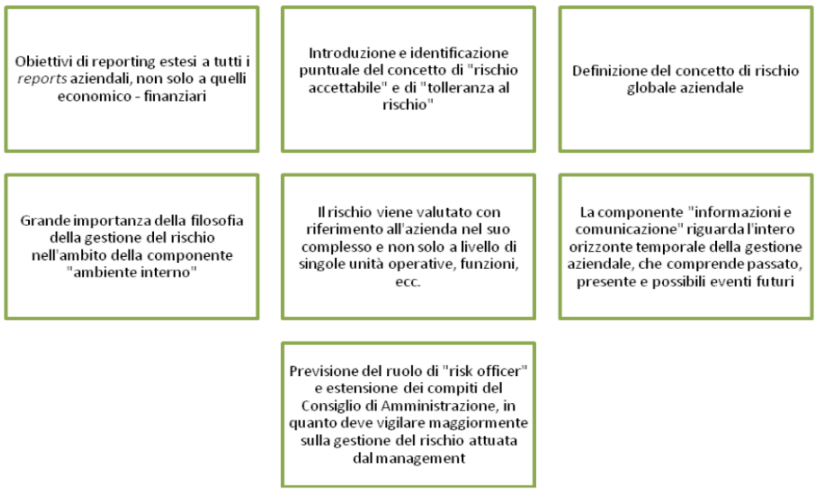
Fig. 2.2 – Dettaglio delle componenti dell'ERM



Fonte: CoSO 2004, Ass. It. Internal Auditors e PWC (2006)

Nonostante l'idea di fondo sia rimasta la stessa, il nuovo Report introduce nuovi aspetti circa l'ERM che ne migliorano la completezza in quanto si pone maggiore enfasi sul tema del rischio piuttosto che sui controlli interni. Questi contenuti sono riassunti in Figura 2.3:

Fig. 2.3 – Novità introdotte dal CoSO 2004



Fonte: Venturelli (2007)

Nel 2013 viene pubblicato un aggiornamento al CoSO Report del 2004 in risposta ai cambiamenti intervenuti nel *business environment* nei 20 anni successivi alla pubblicazione del primo Report. Questo aggiornamento rappresenta uno strumento per la gestione del rischio sia per imprese private che per quelle pubbliche e in generale per ogni impresa che intenda migliorare il proprio sistema di controllo interno. Il cambiamento più significativo riguarda la codificazione dei 17 principi a supporto delle 5 componenti che nel Report del 1992 erano considerate implicite. Affinché vi sia un efficace sistema dei controlli interni il framework richiede che *ciascuna delle 5 componenti e dei 17 principi siano presenti e funzionanti e che le 5 componenti debbano funzionare insieme in modo integrato*. *Presente* significa che componenti e principi esistono e che essi sono inseriti nella progettazione e nell'attuazione del sistema di controllo interno, mentre *funzionante* significa che le componenti e i principi pertinenti continuano ad esistere nel sistema di controllo interno[90] (vedi Fig. 2.3).

Fig. 2.3 – CoSO Cube 2013

Fonte: Sox-online.com, the original CoSO Cube

[90] KPMG (2013).

Il Framework del 2013 ricorda che comunque vi possono essere dei limiti nell'applicazione di tale modello perché gli obiettivi potrebbero non essere adeguati, l'uomo può commettere errori che possono portare all'insuccesso e i controlli interni potrebbero essere elusi[91] (vedi Fig. 2.4).

Fig. 2.4 – I principi del CoSO Report 2013

COMPONENTI DEL CONTROLLO INTERNO	PRINCIPI
AMBIENTE DI CONTROLLO INTERNO	1. L'organizzazione deve dimostrare l'impegno nell'integrità e nei valori etici. 2. Il Cda deve dimostrare indipendenza dal management ed esercitare la propria supervisione. 3. Il management, con la supervisione del Cda, deve stabilire le linee di reporting e le responsabilità in linea con gli obiettivi aziendali. 4. L'organizzazione deve attrarre, far crescere e trattenere personale competente. 5. L'organizzazione stabilisce e definisce le responsabilità.
VALUTAZIONE DI CONTROLLO	6. L'organizzazione deve determinare gli obiettivi con chiarezza, al fine di rendere possibile l'identificazione dei rischi ad esse correlati. 7. L'organizzazione deve identificare e valutare i rischi. 8. La valutazione dei rischi deve tenere in considerazione le potenziali frodi aziendali. 9. L'organizzazione deve identificare e valutare i cambiamenti significativi che potrebbero influire sul sistema di controllo interno.
ATTIVITÀ DI CONTROLLO	10. L'organizzazione deve sviluppare e implementare attività di controllo che contribuiscano a mitigare i rischi. 11. L'organizzazione deve sviluppare e implementare controlli di alto livello sulle tecnologie di supporto al raggiungimento degli obiettivi. 12. L'organizzazione deve definire le attività di controllo tramite politiche che ne stabiliscano le aspettative e procedure che definiscano il piano operativo delle politiche
INFORMAZIONE E COMUNICAZIONE	13. L'organizzazione deve ottenere o generare informazioni di qualità e che siano rilevanti per il raggiungimento degli obiettivi. 14. L'organizzazione deve comunicare efficacemente internamente. 15. L'organizzazione deve comunicare efficacemente esternamente.
MONITORAGGIO DELLE ATTIVITÀ	16. L'organizzazione deve sviluppare e attuare valutazioni e attività di monitoraggio. 17. L'organizzazione deve valutare e comunicare le carenze organizzative.

Fonte: Nostra elaborazione dei principi elencati su CoSO Report 2013

L'ultima modifica apportata al CoSO risale al 2017 e prende il nome di *Enterprise Risk Management – Aligning Risk with Strategy and Performance*. Il nuovo Report pone maggiore enfasi sull'integrazione dei rischi nella strategia per il raggiungimento degli obiettivi, in quanto ci si accorse che nella pratica i processi furono spesso ignorati o non sempre compresi (*mancanza di integrazione*), venivano applicati a livello di singoli processi e non a livello strategico (*mancata implementazione*)

[91] KPMG (2013).

e il management non è stato coinvolto nella sua realizzazione (*mancanza di coinvolgimento*)[92]. Il nuovo Report pone un'attenzione maggiore alla ricerca di un adeguato sistema di gestione dei rischi, dove i rischi sono considerati come opportunità per la creazione di valore: creare valore è infatti l'obiettivo di ogni impresa ed è necessario dare più importanza alla relazione "*rischio - strategia - Performance*"[93].

Sin dalla nuova rappresentazione grafica si comprende come l'ERM debba essere considerato uno strumento per la creazione di valore da rappresentare non più come un cubo, ma come una spirale dove si intrecciano due flussi. Quest'ultimi, contenenti le cinque componenti dell'ERM, si organizzano in (vedi Fig. 2.5):

- *"Flusso dei processi comuni"*, al cui interno sono ricomprese le seguenti componenti:
    - *Strategia e definizione degli obiettivi*. Questa componente si concentra sulla pianificazione strategica e su come l'organizzazione possa conoscere l'effetto dei fattori interni ed esterni sul rischio;
    - *Performance*. Dopo che un'organizzazione ha sviluppato la sua strategia, passa quindi a identificare e valutare i rischi che potrebbero influire sulla sua capacità di raggiungere questi obiettivi;
    - *Riesame e revisione*. Si dovrà quindi valutare e riesaminare i cambiamenti in atto e gli eventuali rischi correlati, rimodulare le iniziative se vi sono stati degli scostamenti di performance ed eventualmente revisionare le strategie intraprese. Inoltre, questa è anche l'occasione per capire come migliorare il processo nel suo complesso[94].
- "*Flusso dei meccanismi di supporto dell'ERM*" composto da:
    - *Governance e cultura*. La *governance* determina l'impostazione dell'organizzazione definendo strutture, responsabilità e sistemi di supervisione, mentre la *cultura* rappresenta la base per valori etici, integrità e trasparenza[95];
    - *Informazione, comunicazione e reporting*. Riguarda la condivisione di informazioni provenienti da fonti interne ed esterne a tutta l'impresa. I sistemi e le tecnologie vengono utilizzati non solo per comunicare i rischi ma anche per acquisire, elaborare, gestire e produrre report.

[92] Associazione Nazionale dei Risk Manager e Responsabili Assicurazioni Aziendali, ANRA (2018).
[93] ANRA (2018).
[94] Attisano (ottobre 2019).
[95] Attisano (ottobre 2019).

Fig. 2.5 – Rappresentazione grafica CoSO Report 2017

Fonte: CoSO Report 2017

L'obiettivo del Report è quello di far sì che le imprese prendano decisioni consapevoli al fine di raggiungere gli obiettivi strategici e di performance. La rappresentazione a spirale vuole indicare come il *risk management* sia intrecciato in ogni fase di un piano strategico e come esso sia un modello che presenta una grande adattabilità (Fig. 2.6).

Fig. 2.6 – I principi del CoSO Report 2017

Governance & Culture	Strategy & Objective-Setting	Performance	Review & Revision	Information, Communication, & Reporting
1. Esercitare l'attività di supervisione dei rischi	6. Analizzare il contesto di Business	10. Identificare i rischi	15. Valutare modifiche sostanziali	18. Sfruttare informazioni e tecnologie
2. Costituire delle strutture operative	7. Definire l'appetito per il rischio	11. Valutare la gravità del rischio	16. Riesaminare rischi e performance	19. Comunicare le informazioni riguardanti il rischio
3. Definire la cultura desiderata	8. Valutare strategie alternative	12. Costruire una scala di priorità dei rischi	17. Perseguire miglioramenti del sistema di ERM	20. Redigere Reports su rischi, cultura e performance
4. Dimostrare impegno verso i valori fondamentali	9. Formulare obiettivi di Business	13. Implementare procedure di risposta al rischio		
5. Attrarre, Formare e trattenere Individui capaci		14. Sviluppare una Portfolio View		

Fonte: Personale rielaborazione CoSO Report 2017

2.2. International Organisation for Standardization (ISO) 31000

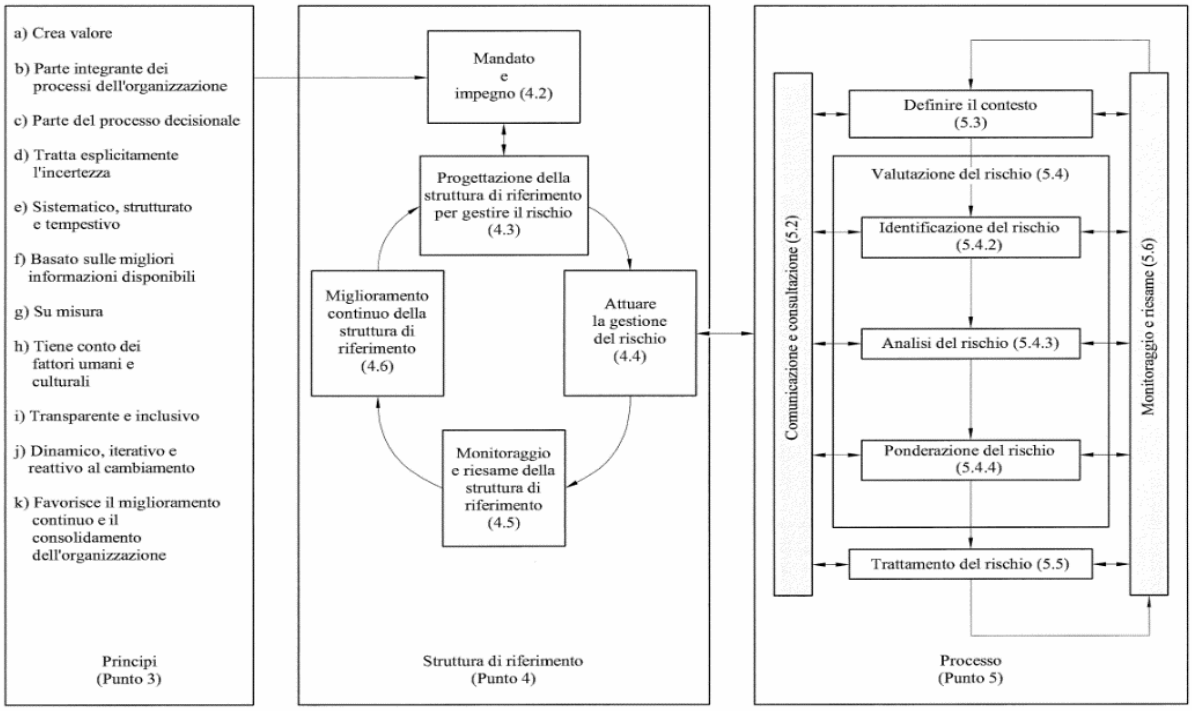
Il secondo Standard di riferimento per l'ERM è l'ISO 31000 "*Risk Management - Principles and Guidelines*". Nonostante affondi le sue radici già nel 1995[96] il primo vero Report risale al 2009 (recepito in Italia con lo standard *UNI ISO 31000:2010 "Gestione del rischio"*) ed è stato fin da subito accettato da aziende private, pubbliche e organizzazioni non-profit in quanto lo scopo di questo Standard è di «rendere disponibile a tutti i principi e le linee guida generali sulla gestione del rischio e di renderla adattabile a qualsiasi tipo di organizzazione (impresa pubblica, privata, o sociale, associazione, gruppo o individuo) e di settore lungo l'intera vita dell'organizzazione medesima»[97].

[96] Si veda in merito lo Standard AS/NZS 1995.
[97] Dittmeier (2015).

I benefici che possono derivare dall'implementazione di un processo di risk management secondo lo standard ISO 31000 sono[98]: l'aumento della probabilità di raggiungimento degli obiettivi; incoraggiare una gestione proattiva, volta a favorire le opportunità, a migliorare la prevenzione delle minacce e la gestione degli incidenti e della minimizzazione dei danni; migliorare l'identificazione delle opportunità e delle minacce; promuovere la consapevolezza della necessità di identificare e trattare i rischi nell'intera organizzazione; migliorare il reporting, della governance, dell'efficacia e dell'efficienza operativa, dei controlli dell'assegnazione delle risorse per il trattamento dei rischi; costituire una base affidabile per il processo decisionale e di pianificazione; incrementare la fiducia degli stakeholder; sviluppare la resilienza organizzativa, intesa come capacità di sopportare le avversità e a reagire prontamente alle stesse; ed infine di migliorare l'apprendimento organizzativo.

Lo standard ISO del 2009 ruota attorno a 3 punti essenziali, ovvero *Principi*, *Framework* (*Struttura di riferimento*), *Processo* (vedi Fig. 2.7).

Fig. 2.7 – Relazione tra Princi di Risk Management Framework e Processi



Fonte: Cybersecurity360.it, Il risk Management e la nuova ISO 31000:2018: le linee guida

L'obiettivo principale di un impianto di *risk management* secondo i dettami di questo standard sarebbe quello di creare valore attraverso un sistema che diviene parte integrante dei processi dell'organizzazione e del processo decisionale. L'incertezza assume un ruolo molto importante in

[98] Dittmeier (2015).

questo ambito e le metodologie per gestirla vengono elencati nei principi successivi (dal punto "e" al punto "j"), favorendo in conclusione un continuo miglioramento e un consolidamento dell'organizzazione.

Il *Framework* individua il quadro di riferimento, indicando le modalità di progettazione della struttura, di attuazione della gestione dei rischi, di monitoraggio e di continuo miglioramento della struttura di riferimento[99], sostenendo inoltre che tale successione di fasi debba essere preceduta dalla fase denominata "*mandato e impegno*", il primo da parte dei vertici dell'impresa, mentre il secondo da parte di tutti i livelli aziendali.

La prima fase è quella di *progettazione della struttura di gestione dei rischi* (punto 4.3) e riguarda lo studio dell'ambiente interno ed esterno; l'elaborazione della *Policy* di gestione del rischio; l'*Accountability*, individuando le responsabilità di ogni soggetto aziendale; l'inserimento della gestione del rischio in tutti i processi aziendali; la previsione delle modalità di comunicazione interna ed esterna[100]. La seconda fase è quella di *attuazione della gestione del rischio* (punto 4.4) nella quale si valuta come, in che modo e con quali tempistiche sarà implementata la procedura, se sono rispettate le disposizioni normative e se vi è un adeguato sistema di comunicazione. La terza fase riguarda il *monitoraggio e il riesame del framework* che comporta la necessità di attuare un controllo delle performance in relazione al processo di rischio e nel caso in cui esso si riveli deficitario procedere con un aggiornamento dello stesso. La quarta fase riguarda il *continuo miglioramento*, perché è fondamentale che il *framework* si adatti ai cambiamenti che potranno intervenire così da non cogliere impreparata l'impresa ed evitando di pregiudicare la redditività della stessa.

Per quanto concerne il terzo elemento, "il processo", si rimanda ai capitoli successivi, dove verrà trattato in dettaglio.

Data la continua evoluzione delle pratiche di *risk management* appare immediatamente chiaro come questo Standard sia incompleto poiché non fornisce sufficienti spiegazioni in merito al *risk appetite*, all'integrazione del *risk management* negli altri processi e non dava istruzioni circa la sua implementazione[101].

Nel 2018 l'ISO 31000 è stato aggiornato «ponendo una maggiore attenzione alla creazione di valore come fattore chiave per il *risk management*»[102]: infatti, lo scopo del *risk management* non è di proteggere, bensì di creare e accrescere il valore dell'impresa.

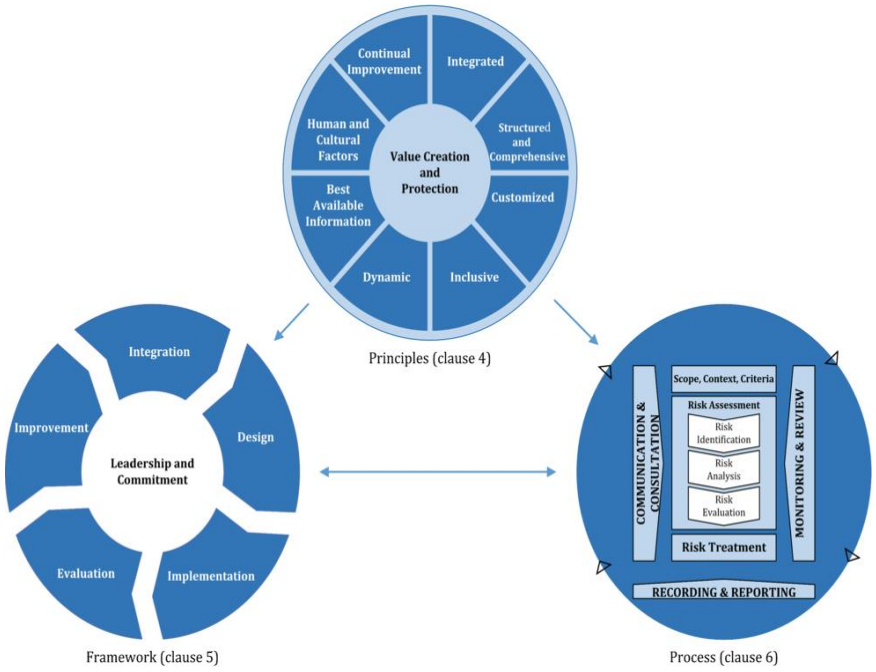
[99] Dittmeier (2015) definisce questa successione di fasi come Plan, Do, Check and Act (PDCA), il cui obiettivo è quello di promuovere un continuo sviluppo dei processi e un efficiente consumo delle risorse.
[100] Dittmeier (2015).
[101] Williams (Febbraio 2019).
[102] Williams (Febbraio 2019).

Le principali modifiche riguardano innanzitutto la revisione e l'aggiornamento dei principi che da undici passano a otto; in seconda istanza lo snellimento dei contenuti per renderne più fruibile la lettura; ed infine viene data una maggiore attenzione alla *leadership* e all'integrazione della gestione del rischio, nonché all'iteratività nella medesima, nell'ambito del governo dell'impresa.

Il vero valore aggiunto di questa modifica consiste nella semplicità di lettura dello Standard poiché semplifica ulteriormente quanto già esposto nella versione del 2009, senza però snaturarne i concetti chiave. Dalla nuova rappresentazione grafica si evince chiaramente una maggiore attenzione per il *rischio inteso come opportunità* in quanto i principi ruotano attorno alla *creazione di valore* che è il vero obiettivo di ogni impresa. È cambiato il modo di pensare, creazione e protezione di valore non devono essere perseguiti per raggiungere un'efficace gestione del modello di *risk management*, ma al contrario, per permettere di creare e proteggere il valore.

Il concetto di "*integrazione*" accresce la sua importanza tanto da essere inserito sia fra i principi che nel *framework*. Per quest'ultimo viene poi specificato (ponendo al centro dello schema "*leadership e impegno"*) che spetta proprio ai vertici realizzare la struttura di riferimento per la gestione dei rischi. *Principi e Framework seguono un metodo iterativo* che potremo definire come «la ripetizione di una serie di analisi o di cicli di operazioni per arrivare al risultato desiderato»[103] (vedi Fig. 2.8).

Fig. 2.8 – Relazione tra principi, framework e processi nell'ISO 31000: 2018



Fonte: iso.org, ISO 31000:2018

[103] Williams (Febbraio 2019).

A conclusione dell'esame sugli Standard di riferimento, si riassumono gli aspetti comuni e le diversità fra lo Standard ISO 3100 del 2018 e lo Standard CoSO del 2017 (vedi Fig. 2.9).

Fig. 2.8 – Differenze e similitudini tra gli Standard ISO 31000 e CoSO 2017

SIMILITUDINI	DIFFERENZE
Entrambi gli Standard hanno l'obiettivo di espandere il risk management, incorraggiando l'assunzione dei rischi	L'ISO 31000 risulta più standardizzato rispetto alla versione proposta dal CoSO 2017
Entrambi gli Standard si pongono come linee guida che dovranno poi essere adattate alle caratteristiche dell'impresa	Mentre lo standard ISO 31000 è stato adottato come standard di Risk Management ufficiale dalle Organizzazioni di standard nazionali in circa 57 Paesi già alla fine del 2015, l'aggiornamento del 2017 dello standard CoSO ha ricevuto contributi per la sua stesura soprattutto da studiosi ed esperti provenienti dagli Stati Uniti
Entrambi gli Standard incorporano il Risk Management nel processo di decisione e ciò garantisce che l'impresa stia assumendo i giusti rischi nella giusta quantità	Lo Standard CoSO ha sempre fatto riferimento ai bisogni degli Auditors confermando tale impostanzione anche nell'aggiornamento del 2017 nonostante sia possibile notare una maggiore enfasi nella strategia, mentre lo Standard ISO 31000 intende fornire una linea quida a chiunque sia interessato all'implementazione di un sistema di Risk Management
	Lo Standard CoSO si concentra maggiormente su come i vertici dovrebbero sorvegliare l'intera organizzazione piuttosto che fare direttamente riferimento al rischio, mentre lo Standard ISO 31000 si concentra invece quasi esclusivamente sul rischio e su come incorporarlo nel processo di pianificazione strategica
	Mentre lo Standard ISO 31000 fornisce una chiara distinzione tra framework e processi, lo Standard CoSO mescola questi due concetti e infatti solamente una componente su cinque del framework, menziona l'attuale processo di risk management
	Mentre lo Standard CoSO del 2017 discute approfonditamente del risk appetite fornendo esempi in merito a concetti quali risk appetite, risk tolerance e risk capacity, lo Standard ISO 31000 si limita semplicemente a menzionare l'argomento sotto l'etichetta di "risk criteria"
	Sebbene lo Standard CoSO 2017 si concentri di più sul raggiungimento degli obiettivi rispetto alle versioni precedenti esso continua ad incoraggiare la "caccia" al rischio, rimanendo quindi rischio-centrico. Lo Standard ISO 31000 pone invece una maggiore enfasi sul raggiungimento degli obiettivi, piuttosto che sull'evitare le conseguenze negative del rischio con una visione che possiamo definire come successo-centrica

Fonte: Nostra elaborazione su erminsightsbycarol.com

3. ERM E PIANIFICAZIONE STRATEGICA: LO STRATEGIC RISK MANAGEMENT

Come ha dimostrato la crisi del 2008, ignorare il connubio rischio-strategia può portare a risultati disastrosi e perciò adottare un processo di ERM diventa una priorità per il *top management*. Come indicato nelle linee guida proposte dagli Standard, lo scopo ultimo dell'ERM è quello di creare valore per l'impresa e per questo dev'essere inserito nella pianificazione strategica perché non integrare le attività di *risk management* nella pianificazione strategica significa sottovalutare il rischio strategico[104].

Implementare un sistema di supervisione basato sull'ERM non è una sfida semplice: Il numero e la complessità dei rischi in cui incorre l'impresa cresce molto velocemente a causa dei sempre più rapidi cambiamenti tecnologici, delle sempre più sofisticate operazioni di business e dalla sempre maggiore competizione che rende difficile prevedere l'evoluzione del portafoglio rischi. Un altro aspetto che complica la gestione del rischio, discende dalla constatazione che spesso le tecniche utilizzate dal *board* e dai *senior executives* sono datate, poco sofisticate e spesso ad hoc. L'ERM rappresenta quindi una soluzione che enfatizza un approccio di *risk management* olistico e *top-down*, in quanto il suo scopo è quello di aumentare la probabilità che l'impresa raggiunga i propri obiettivi compatibilmente all'appetito per il rischio degli *stakeholders*[105].

Affinché lo sviluppo di un sistema di ERM all'interno del piano strategico abbia successo, è necessario bilanciare gli obiettivi di performance e i relativi rischi. Il *management* valuta quindi le diverse alternative strategiche disegnate per raggiungere gli obiettivi di performance, tenendo in considerazione i rischi che ciascuna alternativa comporta. Lo scopo è quello di determinare se i potenziali benefici sono commisurati ai rischi associati ad ogni alternativa e quali iniziative strategiche saranno invece controproducenti. L'ERM permette quindi di rivelare le aree in cui l'impresa è avversa al rischio o le aree in cui sta rispondendo in modo inefficace a rischi simili esistenti in altre aree dell'impresa[106].

Per implementare un adeguato sistema di *Strategic Risk Management* è necessario adottare una metodologia che permetta di valutare sistematicamente il rischio strategico. Generalmente, le strategie attuate dalle imprese perseguono l'obiettivo di aumentare il valore per gli azionisti, ad esempio attraverso un aumento dei ricavi o una riduzione dei costi, risultando quindi fondamentale l'approfondita conoscenza dei *drivers* che generano tale valore e dei rischi ad essi legati. Parafrasando la definizione di "rischio" proposta da Michael Porter (1985), esso rappresenterebbe «la funzione che

[104] Fraser e Simkins (2010).
[105] Fraser e Simkins (2010).
[106] Fraser e Simkins (2010).

indica quanto una strategia è sottoperformante nel caso in cui si verifichi lo scenario sbagliato»[107]: il primo passo per un processo di *Strategic Risk Management*, consiste quindi nell'identificazione e nella valutazione di tutti gli eventi e dei possibili scenari che si possono verificare nel caso in cui la strategia scelta venga messa in atto. Questa fase deve però essere preceduta dalla definizione dell'obiettivo del *risk appetite*, in modo tale che *board* e *management* possano comprendere quali rischi strategici si intenda assumere[108].

Un efficace strumento per integrare obiettivi strategici e obiettivi di *risk management* è rappresentato dal *Return Driven Strategy framework*, che permette di stabilire una gerarchia delle attività strategiche. La *Return Driven Strategy* si compone di dieci principi e tre punti cardine (chiamati *fundamentals*), formando una gerarchia di attività correlate che l'impresa deve svolgere se intende migliorare le proprie performance. I dieci principi sono[109]:

- *Il principio dell'impegno*. Il management deve riuscire a creare valore per gli azionisti rispettando l'etica:
    1. *Massimizzare il benessere in modo etico*;
- *I due principi degli obiettivi*. L'impresa dev'essere in grado di soddisfare le esigenze dei clienti che non sono ancora pienamente soddisfatti e deve allo stesso tempo formare un gruppo di clienti che sia redditizio e che abbia possibilità di crescita:
    2. *Soddisfare le esigenze dei clienti che ancora non sono state soddisfatte*;
    3. *Individuare gruppi di clienti ritenuti appropriati* (*target and dominate*);
- *I tre principi della competenza*. L'impresa dev'essere in grado di sviluppare delle offerte che rispettino i tre principi elencati precedentemente, innovando le offerte in modo da soddisfare i clienti ancora insoddisfatti, attrarne di nuovi e infine apporre il proprio *brand* così da fidelizzare il cliente
    4. *Sviluppare offerte*;
    5. *Innovare le offerte*;
    6. *Appore il proprio brand alle offerte*;
- *I quattro principi di supporto*. Le attività di supporto vengono svolte per raggiungere gli obiettivi indicati dai "*principi di alto livello*"
    7. *Ricerca di Partners*;
    8. *Mappare e ridefinire i processi*;

[107] Porter (1985).
[108] Fraser e Simkins (2010).
[109] Frigo e Litman (2002, 2003, 2004, 2008).

9. *Coinvolgere i dipendenti*;
10. *Comunicare in modo olistico*.

Vi sono poi tre punti cardine (*fundamentals*) per il perseguimento di una *Return Driven Strategy*[110]: il primo è rappresentato dai *Genuine Assets* che possono essere definiti come «l'insieme delle risorse tangibili e intangibili e delle capacità che permettono all'impresa di raggiungere i propri obiettivi»[111] e sono gli strumenti attraverso i quali l'impresa potrà ottenere un vantaggio competitivo sostenibile. Le attività possono essere copiate dai *competitor* e perciò solamente facendo leva su *assets* unici è possibile creare un'offerta che sia unica e che non potrà essere copiata (un esempio di *genuine asset* è il *brand*); il secondo riguarda la *Vigilanza sulle forze del cambiamento* in quanto l'impresa dev'essere abile e agire velocemente per sfruttare le opportunità ed evitare le minacce; il terzo consiste nel *disciplinare la misurazione e la valutazione delle performance* in quanto è necessario creare un sistema che sia in grado di collegare la strategia ai risultati finali al fine di verificare il raggiungimento degli obiettivi. Le misure di performance fungono da strumento di supporto per il raggiungimento degli obiettivi strategici e per la creazione di valore.

Questo *framework* descrive quindi come allineare la strategia di un'azienda all'obiettivo finale di "*massimizzare eticamente la ricchezza degli azionisti*". Il management deve quindi comprendere, definire e allineare le attività di *risk management* con l'obiettivo di creare valore per gli azionisti in modo etico.

Per essere efficace, il *framework* di uno *Strategic Risk Management* necessita di queste caratteristiche: primo fra tutte, esso richiede un *allineamento con l'impegno alla creazione di valore in modo etico per gli azionisti* in quanto è fondamentale che il *risk management* persegua l'obiettivo di proteggere e creare nuovo valore per gli azionisti, concentrandosi quindi sui rischi intesi come opportunità (*up-side risk*) e che tutto ciò sia fatto rispettando i parametri etici[112]. Secondariamente dev'essere un *approccio olistico*, in quanto il *framework* per uno *Strategic Risk Management* necessita di una visione a 360 gradi all'interno dell'impresa perché solamente essendo integrato con tutte le attività dell'impresa può permettere a questa di raggiungere i propri obiettivi. Un approccio di tipo ERM risponde adeguatamente alla necessità di una visione olistica e *top-down* del rischio, collegando le diverse *business unit* per raggiungere l'obiettivo dell'impresa e allo stesso tempo massimizzando l'obiettivo degli azionisti[113]. Infine, deve possedere la *capacità di identificare e*

[110] Frigo e Litman (2002, 2003, 2004, 2008).
[111] Frigo (febbraio 2014).
[112] Fraser e Simkins (2010).
[113] Fraser e Simkins (2010).

valutare le forze del cambiamento perché lo *Strategic Risk Management* non deve essere un processo occasionale, bensì un processo continuo perché i rischi sono in costante evoluzione e di conseguenza le strategie delle imprese devono necessariamente evolversi se vogliono stare al passo. Lo *Strategic Risk Management* deve essere quindi capace di identificare e valutare regolarmente eventi, scenari e forze del cambiamento, che impattano sulle strategie di business e sulle performance[114].

Per collegare l'ERM alla pianificazione strategica e realizzare un efficace sistema di *Strategic Risk Management* si possono adottare due approcci[115]: Un primo approccio riguarda *l'implementazione di un processo di valutazione del rischio strategico* che comporta la necessità di:

- *Valutare il rischio dei piani strategici*. La valutazione strategica del rischio può iniziare conducendo una valutazione globale del rischio dei piani strategici. Questa valutazione include l'analisi dello scenario a seguito dei diversi cambiamenti nelle modifiche delle ipotesi che circondano i drivers della strategia
- *Identificare gli scenari di rischio critico*. Il passo successivo è quello di identificare e descrivere gli "scenari di rischio critico" considerando gravità e probabilità che eventi e scenari si verifichino.
- *Identificare le contromisure*. dopo avere identificato gli scenari di rischio critico è necessario definire delle contromisure se tali scenari si verificano.
- *Realizzare un processo di un monitoraggio continuo*.

Un secondo approccio concerne invece *l'implementazione di un processo che identifichi i Genuine Assets a rischio*. Come detto, i *Genuine Assets* rappresentano le capacità e le risorse (tangibili e intangibili) che rendono uniche le offerte dell'impresa e che permettono di creare un vantaggio competitivo sostenibile e solo attraverso questi vantaggi è possibile realizzare una strategia che sia in grado di aumentare il valore.

Un efficace processo di *Strategic Risk Management* è quindi in grado di determinare la sopravvivenza di un'impresa oppure no. Se progettata in modo corretto, la connessione tra ERM e strategia dovrebbe essere in grado di creare nuovo valore per l'impresa, rendendola più proattiva e flessibile nella gestione dei rischi. La chiave per uno *Strategic Risk Management* di successo è rappresentata dalla capacità di identificare i rischi insiti nella strategia aziendale in grado di attivare una reazione a catena potenzialmente dannosa per l'impresa.

[114] Fraser e Simkins (2010).
[115] Fraser e Simkins (2010).

4. RISK-AWARE CULTURE E L'AMBIENTE DI RISK CHALLENGE CULTURE

Nonostante l'ERM sia un valido strumento per la gestione del rischio in quanto crea valore, riduce la volatilità e conduce ad un miglior processo decisionale, è comunque necessario che esso sia supportato da un'ambiente di *risk challenge culture*. La *risk challenge culture* viene definita dall'*Association of Accountants and Financial Professionals in Business* (*ACCA-IMA*) come «un ambiente che incoraggia, esige e premia la messa in discussione delle condizioni esistenti»[116] e continua poi attraverso degli esempi che chiariscono ciò che non permette la creazione di un ambiente in tal senso:

«Se un subordinato ha paura di chiedere al *senior management* quali siano i rischi percepiti, non ci troviamo in un ambiente di *challenge culture*. Quando un membro del consiglio di amministrazione è soddisfatto da una fugace risposta del CEO in merito ad una particolare problematica riguardante il rischio, non è un ambiente di *challenge culture*. Quando i membri del *board* liquidano velocemente particolari aspetti critici della gestione del *management* senza affrontarle attraverso un serio dibattito, non hanno agito a beneficio della *challenge culture*»[117].

Dopo aver dato una definizione di *risk challenge culture*, vengono individuati otto aspetti che determinano l'esistenza di un ambiente di risk challenge culture[118]: il primo aspetto riguarda lo *scetticismo professionale e la supervisione del rischio da parte del board* evidenziando come l'approccio alla supervisione del rischio debba avvenire in modo interrogativo attraverso valutazioni critiche dell'efficacia del proprio processo di *risk management*. Ogni possibile scenario di rischio dovrebbe includere una serie di "*what if*", guardando anche oltre la situazione attuale; un secondo aspetto riguarda la *Diversità del Board e sviluppo delle esperienze di ERM* e infatti, affinché un ambiente di *risk challenge culture* possa essere presente in ogni livello aziendale e affinché il *board* possa svolgere il proprio compito di supervisione del rischio, è necessario che i membri di quest'ultimo apportino le loro diverse esperienze e competenze e che siano consci della necessità di un approccio di gestione del rischio olistico, quale l'ERM. Se così non fosse, potrebbe essere il *board* stesso un fattore di rischio; il terzo aspetto concerne la *Discussione e definizione dei ruoli* indicando che i ruoli necessari per guidare e sostenere un ambiente di *risk challenge culture* includono il *board* e i suoi comitati, il CEO e gli *executives*. Il consiglio dovrebbe promuovere un elevato livello di

[116] Association of Accountants and Financial Professionals in Business (2013).
[117] Association of Accountants and Financial Professionals in Business (2013).
[118] Walker, Shenkir e Barton (aprile 2015).

apertura nelle discussioni circa la gestione dei rischi perché sarà poi dalle decisioni prese in tale sede che si avranno ripercussioni in tutta l'impresa[119]; il quarto aspetto fa riferimento all'*Asimmetria informativa e ai report sul rischio* sottolineando che tra *board* e *management* sussiste una asimmetria informativa che si verifica nel momento in cui il *management*, a seguito di rallentamenti nella gestione, fa pervenire al *board* le informazioni in ritardo. Senza tali informazioni è difficile per i membri del *board* adempiere alle proprie responsabilità circa il controllo e la gestione del rischio, anche perché alcuni rischi possono concretizzarsi talmente rapidamente che ogni ritardo può essere fatale per la sopravvivenza dell'impresa[120]; il quinto aspetto concerne il *Processo decisionale e i Bias cognitivi* [121] ricordando che un grave impedimento per il successo di una *risk challenge culture* è rappresentato proprio dai *bias* cognitivi che affliggono il processo decisionale; il sesto aspetto attiene al *rischio e alla strategia* mettendo in luce come in un ambiente di *risk challenge culture* tutti gli *stakeholders* debbano richiedere un collegamento continuo tra rischio e opportunità nel perseguimento della strategia; il settimo aspetto riguarda il collegamento tra *incentivi e rischio* in quanto, affinché via sia un atteggiamento proattivo nei confronti dell'assunzione del rischio in linea con il *tone at the top,* è necessario motivare tali comportamenti attraverso una serie di incentivi; l'ultimo aspetto che garantisce la presenza di un ambiente di *risk challenge culture* è il *risk appetite* in quanto è necessario che *board* e *management* definiscano e comunichino all'intera impresa, il livello di rischio che si intende accettare (*appetite*)[122].

La presenza di un'adeguata cultura, in un contesto di ERM, può essere valutata attraverso l'impatto che essa ha sulle decisioni: *vi sarà una forte cultura se le decisioni vengono prese, ad ogni livello aziendale, in modo disciplinato*[123]. Un elemento cruciale nel momento in cui si effettua una decisione circa l'assunzione di un rischio, riguarda il *trade-off* tra *guadagni a breve termine* o *valore risk-adjusted di lungo termine*: i guadagni a breve termine fanno riferimento al raggiungimento o al superamento dei *target* di vendita o agli incentivi collegati al raggiungimento di determinati *target* personali. Di conseguenza, perseguire tali obiettivi può comportare l'assunzione di rischi considerati "non buoni" per l'impresa, al solo scopo di ottenere vantaggi dal raggiungimento di tali *target*. Adottare invece decisioni che possono portare ad un valore *risk-adjusted,* implica la necessaria

[119] Walker, Shenkir e Barton (aprile 2015) sottolineano come i professionisti del rischio, quale ad esempio il Chief Risk Officer (CRO), debbano partecipare attivamente per frenare l'assunzione di rischi quando ritenuto appropriato e disporre delle capacità di leadership per gestire la discussione.
[120] Walker, Shenkir e Barton (aprile 2015).
[121] Un bias cognitivo è un costrutto mentale basato su un pregiudizio che porta ad una distorsione della realtà. Alcuni esempi possono essere overconfidence (eccessiva fiducia in sé stesso), confirmation bias (la tendenza a trovare prove a conferma della decisione iniziale), ancoraggio (la tendenza ad attribuire eccessiva importanza ad un punto di riferimento) e avversione alle perdite. Gardenal e Rigoni (2016).
[122] Walker, Shenkir e Barton (aprile 2015).
[123] Fraser e Simkins (2010).

presenza di una forte *risk culture* all'interno dell'impresa, che aumenti la consapevolezza ad ogni livello aziendale, di quali rischi sono considerati "buoni" e che vanno perciò assunti[124].

L'obiettivo di una *cultura consapevole del rischio* (*risk-aware culture*) è quello di assicurare che tutti i soggetti che prendono delle decisioni, riconoscano l'importanza di identificare e inserire il rischio all'interno delle attività aziendali, di comunicare la presenza di rischi attuali e futuri e che siano consapevoli dell'importanza della dinamica *risk and reward*. la *risk-aware culture* non deve restare appannaggio solamente dei soggetti responsabili delle decisioni ma deve essere estesa a tutta l'impresa[125]. Affinché vi sia una *risk-aware* culture in ogni livello aziendale, risulta necessario incoraggiare determinati comportamenti e premiarli attraverso adeguati processi che contribuiscano al loro rafforzamento. Fraser e Simkins (2010) sottolineano come le procedure decisionali che "restano sulla carta senza essere applicate in modo effettivo", siano viste come prive di importanza e di conseguenza non attuate. È perciò necessario creare dei processi che incoraggino i comportamenti ritenuti corretti nei confronti del rischio attraverso misurazioni, monitoraggio, reporting e un'adeguata governance[126]. In Fig. 2.10 vengono indicate le caratteristiche di cui un sistema di *risk-aware culture* deve disporre[127]:

Fig. 2.10 – Le caratteristiche di un sistema di risk aware culture

Caratteristiche
1. Forte Leadership che renda chiaro quali rischi debbano essere assunti e quali invece debbano essere evitati
2. Una visione olistica
3. Attiva partecipazione del management
4. Sfruttare le conoscenze di tutto lo staff e dei membri del team
5. Incoraggiare lo staff a rendere conto delle proprie azioni
6. Fare in modo che le attività di risk-taking avvengano ad ogni livello dell'organizzazione
7. Fare in modo che i sistemi di controllo agiscano prima che si verifichino i rischi
8. Migliorare comunicazione e lavoro di squadra
9. Incoraggiare la consapevolezza del rischio in tutta l'organizzazione
10. Rendere chiaro in tutta l'impresa l'importanza di un continuo processo di risk management
11. Premiare i comportamenti di risk-taking ritenuti ottimali e sanzionare i comportamenti inappropriati

Fonte: nostra elaborazione su Fraser e Simkins (2010) e Wood (2019)

[124] Fraser e Simkins (2010).
[125] Fraser e Simkins (2010).
[126] Fraser e Simkins (2010).
[127] Fraser e Simkins (2010); Wood (2019).

Sebbene nella prassi la *risk culture* risulti ancora un ambito fortemente inesplorato, essa si rivela in grado di contribuire al successo o al fallimento di un programma di ERM. Un processo di ERM efficiente in teoria ma non nella pratica, può essere peggiore di una totale assenza di un processo di *risk management*, perché dà alle persone un falso senso di sicurezza e non consente alcun sviluppo di una struttura efficace. L'obiettivo della *risk culture* è perciò quello di incentivare l'assunzione dei rischi in modo responsabile, premiando e incoraggiando i comportamenti in tal senso[128].

5. IL RISK APPETITE

Nonostante non vi sia una definizione univoca del concetto di *risk appetite*, vi è concordanza circa la sua importanza strategica: diverse strategie comportano svariati livelli di rischio e di conseguenza si rivela necessario optare per quella che comporta un livello di rischio in linea con il *risk appetite* dell'impresa[129].

Il *risk appetite* viene definito dallo *Standard ISO (2009)* come «l'ammontare e la tipologia di rischi che un'impresa è disposta a perseguire o trattenere»[130], *PWC* lo definisce come «l'insieme dei rischi che un'organizzazione accetta deliberatamente al fine di perseguire i propri obiettivi strategici»[131], secondo il *Financial Stability Board* rappresenta «il livello aggregato e le tipologie di rischio che un istituto finanziario è disposto ad assumersi conformemente alla sua capacità di rischio per raggiungere i propri obiettivi strategici e di business plan»[132] e infine secondo il *CoSO* sarebbe «la quantità di rischio che, a livello generale, un'impresa sarebbe disposta ad accettare»"[133].

Prima di poter dare una definizione di *risk appetite* è necessario analizzare alcuni concetti strettamente collegati ad esso: il primo concetto che ci apprestiamo ad esaminare è la *tolleranza al rischio* che viene definita da Fraser e Simkins come «l'esposizione al rischio che un'impresa ritiene appropriata perseguire o evitare»[134], da PWC come «il livello accettabile di variabilità al fine di raggiungere i propri obiettivi strategici»[135], dall'Institute of Risk Management come «i confini che delimitano il *risk-taking*, al di fuori dei quali l'impresa non è disposta ad avventurarsi nel

[128] Walker, Shenkir e Barton (aprile 2015)
[129] Beretta (2019)
[130] ISO/Guide 73:2009 Risk management – Vocabulary.
[131] PWC (2014).
[132] Financial Stability Board (2013).
[133] Dr. Curtis P., Carey M, Deloitte & Touche LLP, ricerca commissionata da CoSO, (2012).
[134] Fraser e Simkins (2010).
[135] PWC (2014).

perseguimento dei suoi obiettivi di lungo termine»[136]. Il rischio è ancora una volta inteso come probabilità, risultato incerto e/o conseguenza.

Un altro aspetto comune alle definizioni prese in esame è rappresentato dal concetto di *appropriato* o, in modo analogo, di *accettabile*: definire ciò che è appropriato richiede di considerare individualmente e collettivamente, una serie di aspetti quali attitudini al rischio, obiettivi, capacità in termini di struttura (*capabilities*) e di risorse monetarie (*capacity*) al fine dell'assunzione dei rischi e in ultima istanza di effettuare un'analisi costi benefici della gestione del rischio[137]. Strettamente collegato alla definizione di *risk tolerance* è il concetto di *esposizione al rischio*, ovvero la misura che determina l'impatto di un evento rischioso[138].

Sebbene non vi sia una formula che possa essere applicata in modo puntuale per determinare quale sia la *risk tollerance* di un'impresa, è possibile porsi delle domande che aiutano a tracciarne i confini[139]:

- *Qual è l'attitudine al rischio dell'impresa*? si tratta di capire se l'impresa è *risk-taker*, *risk-averse* o *risk-neutral*.
- *Quali sono gli obiettivi dell'impresa*? gli obiettivi indicano come l'impresa distribuirà le proprie risorse ed è molto importante considerarli perché, diversi obiettivi incentivino diversi comportamenti di *risk-taking* che portano di conseguenza a diversi livelli di *risk tollerance*.
- *Quali sono le capacità dell'impresa di gestire il rischio (risk capabilities)*? Sebbene la traduzione di "*capabilities*" e "*capacity*" possa essere fuorviante in quanto entrambe vogliono dire "capacità", *capabilities* rappresenta l'abilità dell'impresa di gestire l'esposizione al rischio e ciò dipende: dalla comprensione del proprio rischio (quali sono gli eventi che possono verificarsi? Che impatto potrebbero avere e con che probabilità?); dalla capacità di misurazione del rischio; dalle capacità delle risorse umane; dall'adeguatezza o meno delle pratiche di *risk management*; dal controllo e dalla supervisione del processo di *risk management*;
- *L'impresa è in grado di assorbire, attraverso le proprie risorse a disposizione, le perdite che possono derivare dai rischi assunti?* Questa è la *capacity*, ovvero la capacità dell'impresa di essere in grado, se si verificano gli eventi rischiosi, di coprire le perdite (*loss assorbing capacity*). In questo caso l'impresa dovrà valutare: la capacità finanziaria di cui dispone per assorbire le perdite nel caso si verifichi l'evento rischioso; il potenziale impatto

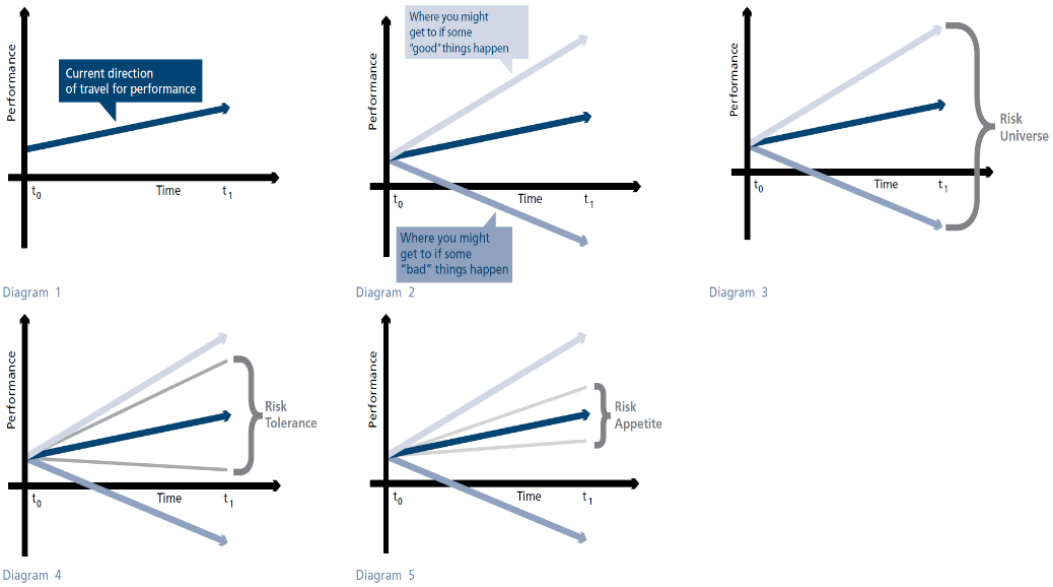
[136] Institute of Risk Management (2011).
[137] Fraser e Simkins (2010).
[138] Fraser e Simkins (2010).
[139] Il seguente elenco muove dalla trattazione di Fraser e Simkins (2010).

che un evento rischioso potrà avere sul raggiungimento degli obiettivi; l'impatto che potrà avere l'evento rischioso sulla reputazione dell'impresa;

- *Quali sono i costi e i benefici che derivano dalla gestione del rischio?*

Per un'adeguata definizione della tolleranza al rischio, è opportuno che il *board* rediga una *policy* formalizzando le aspettative per ogni categoria di rischio[140]. Nella pratica *risk appetite* e *risk tollerance* vengono spesso confusi e utilizzati come sinonimi quando invece così non è, perché mentre il *risk appetite* ha una chiara definizione e riguarda l'insieme dei rischi che l'intera impresa è disposta ad accettare, la *risk tollerance* riguarda invece i rischi a livello individuale e non ha una vera e propria definizione[141].

Fig. 2.11 – Relazione performance - risk appetite - risk tollerance



Fonte: Institute of Risk Management, risk appetite and risk tollerance guidance paper 2011

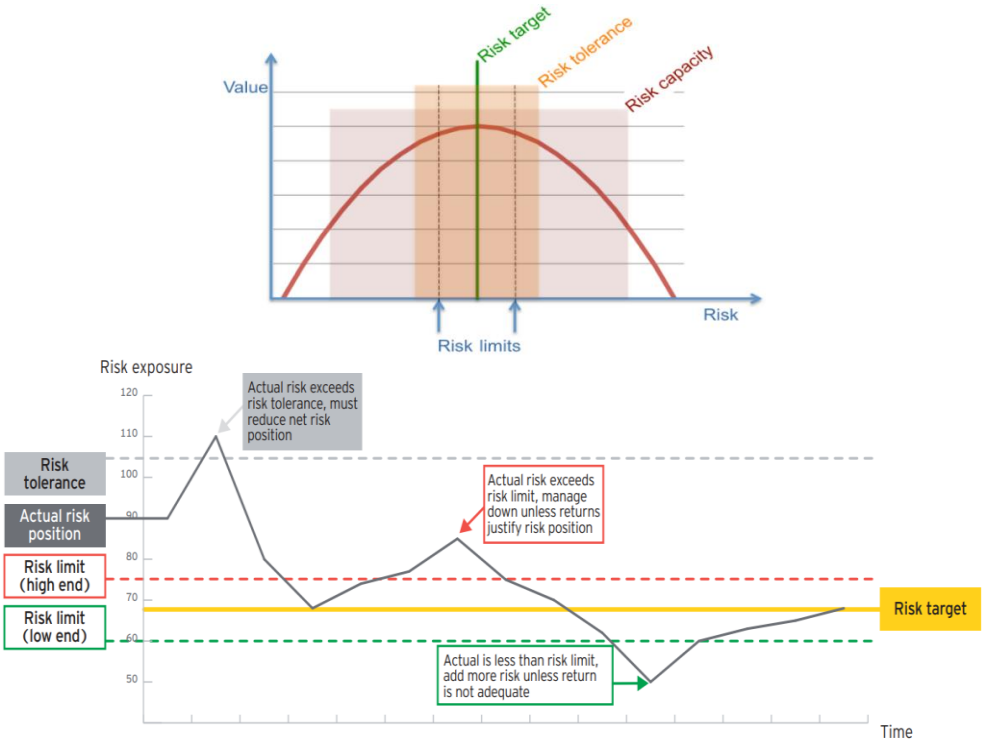
La fig. 2.11 evidenzia come il *risk appetite* rappresenti quanto rischio a livello globale un'impresa sia disposta ad accettare, indicando come esso debba restare all'interno della *risk tollerance* che invece misura il livello di rischio tollerabile per ogni singolo rischio: le parole chiave che chiariscono la differenza tra queste due definizioni sono perseguire (*risk appetite*) e permettere (*risk-tollerance*)[142].

Le imprese definiscono poi un *risk target*, ovvero il livello ottimale di rischio che un'impresa è disposta a sopportare nel perseguimento di uno specifico obiettivo di business e dei *risk limits*,

[140] Fraser e Simkins (2010).
[141] Manoukian (settembre 2016).
[142] Institute of Risk Management (2011).

ovvero delle soglie poste per monitorare che l'attuale esposizione non si discosti troppo dal *risk target* e rimanga al contempo all'interno della *risk tollerance* e del *risk appetite*: al superamento di tale soglia il *management* deve attivarsi per riportare il rischio all'interno delle soglie prestabilite (vedi Fig. 2.12).

Fig. 2.12 – Relazione risk target - risk limit - risk tollerance e risk capacity



Fonte: rielaborazione personale "Risk appetite and ISO 31000" su jeges.com e "Risk appetite the strategic balancing act" Ernst & Young

Altri due concetti da prendere in considerazione nella definizione del risk appetite sono i *risk criteria* e il *risk profile*. I *risk criteria* rappresentano uno degli elementi del *context statement*: si tratta dei termini di riferimento su cui si basa la valutazione del rischio e dipendono dagli obiettivi dell'impresa nonché dal contesto interno ed esterno e possono derivare da standard, leggi e *policies*[143].

Il *profilo di rischio* rappresenta l'esito del processo di valutazione attuato dall'impresa in merito ai propri rischi: esso delinea il numero, il tipo e il potenziale effetto dei rischi. L'impresa dovrà valutare il proprio profilo di rischio il più spesso possibile in quanto deve sempre essere rispettata la seguente relazione: *risk profile* ≤ *risk appetite* ≤ *risk capacity* (vedi Fig. 2.13).

[143] Risk Management LTD (settembre 2015)

Fig. 2.13 – relazione risk profile - risk appetite - risk capacity

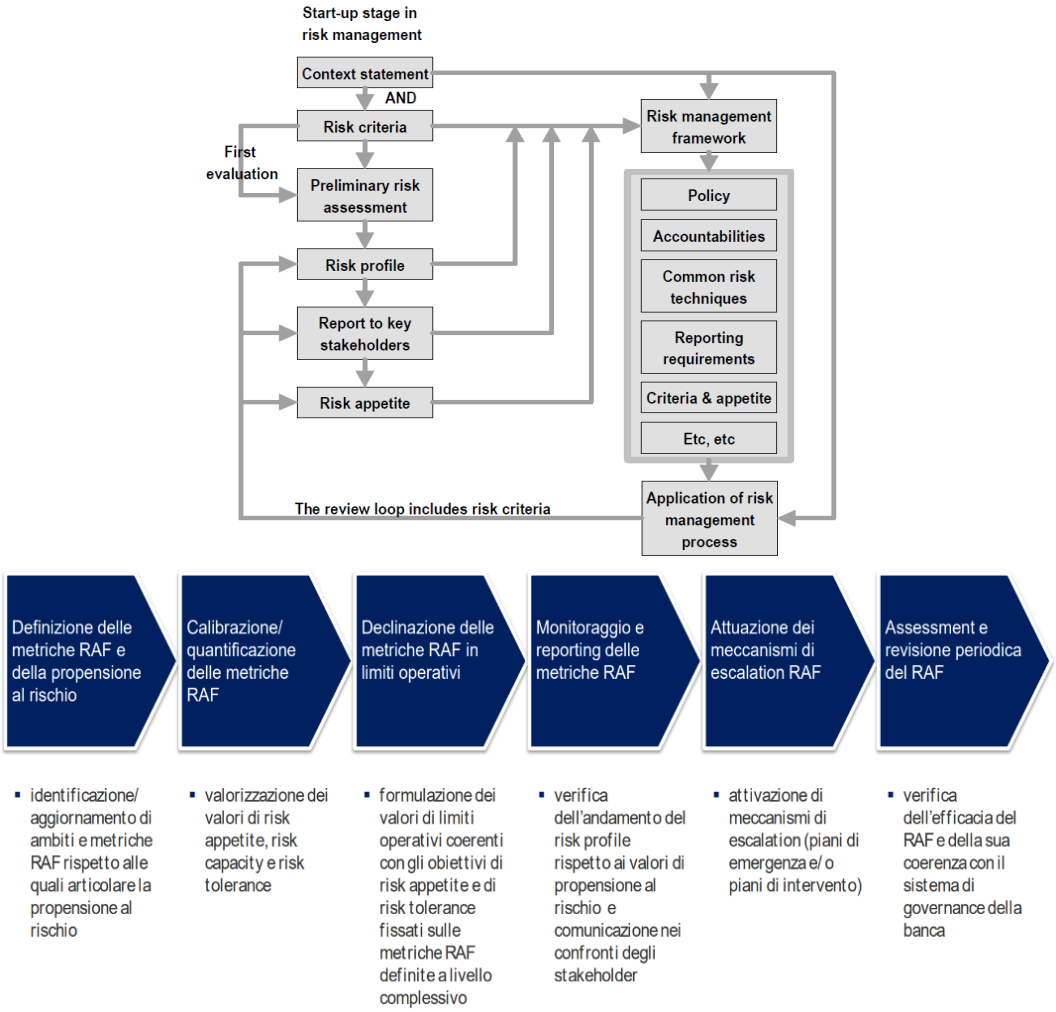
Fonte: nostra elaborazione

Tale relazione deve essere rispettata costantemente altrimenti è necessario un tempestivo intervento da parte del *board* nel tentativo di arrestare la crescita negativa e/o la distruzione del valore. Il primo passo per definire il *risk appetite* consiste nell'individuazione del *contesto* (*context statement*), ovvero «i parametri interni ed esterni che devono essere presi in considerazione in sede di gestione del rischio, nonché la determinazione dello scopo nella definizione di una policy di risk management»[144] e nell'individuazione dei *risk criteria*, ovvero delle metriche e degli indicatori per esprimere il proprio livello di propensione al rischio[145]. A questo punto viene effettuata una valutazione preliminare che conduce ad un profilo di rischio che indica le classi/categorie di rischio che possono influenzare gli obiettivi dell'impresa. Il profilo di rischio individuato in questo stadio iniziale viene comunicato agli *stakeholders* e potranno seguire nuove calibrazioni. Verranno inoltre quantificate le metriche del *Risk Appetite Framework* (*RAF*) che porteranno all'individuazione dei limiti di *risk capacity* e *risk tollerance* generando il *Risk Appetite Statement*[146], il quale sarà poi parte integrante del *Risk Management Framework.*

Il *risk appetite* è continuamente monitorato, verificando il rispetto dei limiti imposti dalla *risk capacity* e dalla *risk tollerance*, nonché dalle altre metriche del RAF per valutare una sua revisione nel caso in cui vi siano cambiamenti nel *risk appetite* degli *stakeholder* e nel caso in cui dovesse eccedere i limiti imposti, si renderà necessario l'intervento del *board* per sanare la situazione (vedi Fig. 2.14).

[144] Risk Management LTD (settembre 2015).
[145] Risk Management LTD (settembre 2015); Associazione Italiana Financial Industry Risk Management (AIFIRM) (aprile 2017).
[146] Risk Management LTD (settembre 2015); AIFIRM (aprile 2017).
Il Risk Apppetite Framework fornisce un approccio strutturato per la gestione, misurazione e controllo del rischio e garantisce che il rischio assunto sia coerente col risk appetite. *Il Risk Appetite Statement* indica invece l'ammontare e la tipologia di rischi che un'impresa assume consapevolmente al fine di perseguire i propri obiettivi. The Risk Management Association (2013)

Fig. 2.14 – Il processo di definizione del Risk Appetite

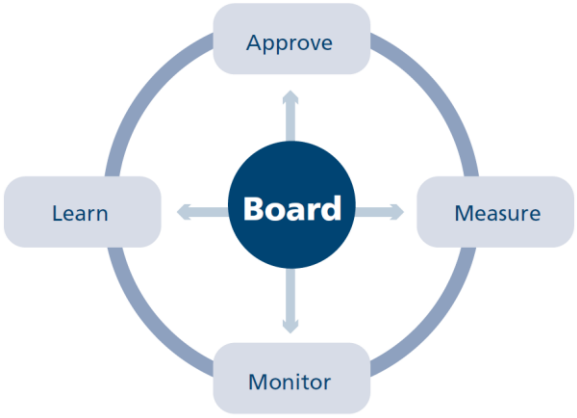


Fonte: rielaborazione personale Risk Management LTD publication del settembre 2015; AIFIRM (aprile 2017).

La *governance* da parte del *board* circa il *risk appetite statement* ruota intorno a questi quattro punti (vedi Fig. 2.15): il primo passo consiste nell'*approvazione* del *risk appetite statement*, alla quale seguono una *misurazione* e un *monitoraggio* continuo, verificando la presenza di tensioni e/o violazioni per poi intervenire. Il *board* verifica infine che l'intera impresa *apprenda* dall'implementazione del RAF, perché solo in questo modo esso viene ad essere inglobato all'interno del contesto aziendale[147].

[147] AIFIRM (aprile 2017).

Fig. 2.15 – Governance del risk appetite



Fonte: AIFIRM (aprile 2017).

6. LE FASI DEL PROCESSO ERM

6.1. Risk Management Policy

Affinché il processo di ERM possa essere conosciuto da tutti i soggetti operanti nell'impresa ed essere efficacemente attuato, è necessario che l'impresa lo formalizzi in un documento che viene chiamato *Risk Management Policy*. Vengono individuate tre tipi di *policies*[148]: una prima tipologia di *policies* riguarda le *policies per il framework dell'ERM, i suoi processi e le sue procedure*, ovvero i documenti in cui viene indicato il quadro di riferimento del processo di *risk management* comprendendo l'approccio al rischio dell'impresa, la terminologia utilizzata nella descrizione dei rischi, nonché i processi e le procedure da seguire per un continuo miglioramento del *framework*, le responsabilità dei soggetti per quanto riguarda la gestione del rischio, come si intende attuare le procedure di monitoraggio, revisione e di controllo[149]. Una seconda tipologia di *policies* fa riferimento alle *policies che riguardano l'impegno, le responsabilità, le modalità di monitoraggio e di revisione*[150]. Infine, l'ultima tipologia di *policies* individuata riguarda le *policies per le decisioni di Risk Management*, ovvero documenti nei quali vengono definite le politiche generali da applicare al processo di ERM. queste fanno riferimento:

- all'indicazione del *risk appetite* nelle sue due dimensioni, ovvero i risultati attesi e quelli inattesi derivanti dagli eventi rischiosi. Generalmente i risultati attesi vengono stimati

[148] Il seguente elenco muove dalla trattazione di Fraser e Simkins (2010).
[149] Fraser e Simkins (2010).
[150] Fraser e Simkins (2010).

attraverso una simulazione Monte Carlo che ne determina la dimensione media, mentre la dimensione inattesa viene stimata considerando la massima perdita che può essere tollerata;

- Il *risk appetite* viene diffuso in tutta l'impresa attraverso i *risk criteria*, che forniscono per ogni decisione delle linee guida circa il livello di tollerabilità del rischio. Questi si basano oltre che sul *risk appetite*, anche sugli obiettivi dell'organizzazione per i quali verrà fissato un livello minimo da superare e generalmente si tratta di policies che riguardano come questi obiettivi saranno monitorati, quali saranno le azioni da intraprendere e se si debba attuare una revisione. I *risk criteria* dovrebbero perciò includere tutto ciò che riguarda gli obiettivi e può trattarsi di limiti, criteri di ottimizzazione o altro;
- Un ultimo aspetto per queste tipologie di *policies* riguarda il *risk reporting* per il quale si richiede che i rischi vengano aggregati sia orizzontalmente che verticalmente

Il *Risk Management Policy* è quindi un documento che definisce quale sia lo scopo del sistema di *risk management*, chiarisce ruoli e responsabilità, indica quale sia il *risk appetite*, quali siano le categorie di rischio e come si articoli il processo di *risk management*. In generale formalizza il *framework* di riferimento per un adeguato processo di *risk management*.

6.2. FASE 1: Definire il contesto

Senza definire il contesto in cui l'impresa si trova ad operare, il processo di ERM non potrebbe aver luogo: lo scopo di questa fase è quello di ricercare dati puntuali circa la propria attività e più dati vengono individuati più il restante processo di gestione del rischio risulterà efficiente[151]. Lo Standard ISO 31000 definisce questo step nel modo seguente «definendo il contesto, l'impresa specifica i propri obiettivi, i parametri interni ed esterni che devono essere presi in considerazione nella gestione del rischio e definisce lo scopo e i criteri per la parte restante del processo»[152].

Definire il contesto chiarisce la portata del processo di *risk management* e stabilisce i criteri in base ai quali i rischi verranno valutati. È inoltre necessario fare riferimento agli obiettivi dell'impresa, in quanto i rischi incidono sul raggiungimento degli stessi e di conseguenza, non potranno essere identificati completamente se obiettivi e strategie non sono resi chiari[153]. In questa fase si cerca di comprendere quali siano le caratteristiche dell'impresa e si approfondisce la specifica attività, lo specifico processo o progetto che si sottopongono alla gestione del rischio. La fase di definizione del

[151] Chapman (2006).
[152] ISO/Guide 73:2009 Risk management – Vocabulary.
[153] Charted Accountants Australia and New Zeland.

contesto può essere ritenuta sufficiente nel momento in cui vengono definiti gli obiettivi, l'organigramma della struttura dell'impresa, il sistema dei controlli interni e il *risk appetite*, vengono esaminate tutte le funzioni primarie dell'impresa e infine quando il processo di *risk management* è stato revisionato[154].

Questa fase si sostanzia nella definizione del contesto interno e ed esterno all'impresa in quanto i rischi possono provenire da entrambe le direzioni: il *contesto esterno* rappresenta l'ambiente in cui l'impresa opera e per una sua analisi è necessario che vengano presi in considerazione i seguenti input, ovvero il contesto economico, sociale, regolamentare, legislativo, culturale, competitivo, finanziario e politico. Il *contesto interno* fa riferimento invece all'ambiente interno all'impresa in cui essa svolge la propria attività e riguarda la definizione di obiettivi, strategie, tolleranza al rischio e *risk appetite*, *governance*, struttura, ruoli, responsabilità e infine le capacità del personale, dei sistemi e dei processi[155]. I meccanismi che permettono di definire il contesto sono[156]:

- *Financial analysis tool*. In questa categoria sono compresi i *ratios* di profittabilità, liquidità ed efficienza in quanto possono essere utilizzati per esaminare la posizione finanziaria e le performance nonché per pianificazione, controllo e valutazione. I *financial ratios* rappresentano quindi uno strumento rapido e relativamente semplice per esaminare le condizioni finanziarie di un'azienda.
- *Diagnostica del processo di risk management*. Risulta fondamentale per l'impresa determinare il grado di sviluppo del proprio processo di *risk management* e determinare quanto esso sia inserito nell'organizzazione[157].
- *SWOT analysis*. Con questo metodo vengono analizzati i punti di forza e di debolezza, le opportunità e le minacce che riguardano l'impresa e ciò permette di valutare i dati raccolti in modo oggettivo, fornendo uno strumento che aiuta a capire, presentare, discutere e a prendere decisioni.
- *PEST analysis*. È l'analisi dei fattori politici, economici, sociali e tecnologici che viene utilizzata per analizzare i fattori che influenzano il mercato cercando poi di anticiparne i cambiamenti.

[154] Chapman (2006).
[155] Charted Accountants Australia and New Zeland.
[156] Chapman (2006).
[157] Chapman (2006). L'autore, ai fini di un'adeguata diagnostica del processo, sottolinea che è necessario esaminare se: sono stati individuati in modo chiaro i responsabili del processo di risk management; le policies e gli effettivi benefici del risk management sono stati comunicati a tutta l'impresa; il framework utilizzato è trasparente e ripetibile, è stata diffusa una risk culture adeguata; se la gestione del rischio risulta integrata nel processo di gestione e se essa è strettamente collegata al raggiungimento degli obiettivi; infine se i rischi sono costantemente monitorati e sottoposti a revisione.

Questa prima fase risulta fondamentale per un processo di ERM che permetta di individuare un gran numero di informazioni pertinenti, fornendo suggerimenti circa la necessità di ulteriori approfondimenti sui rischi, individuando i soggetti che possono contribuire maggiormente durante questa fase.

6.3. FASE 2: Risk Assessment

Dopo aver definito il contesto, la fase successiva è rappresentata dal *risk assessment*, ovvero la fase in cui i rischi vengono identificati (*risk identification*), analizzati (*risk analysis*) e infine valutati (*risk evaluation*)[158]. Se nella fase di identificazione i rischi vengono individuati e iscritti in una lista (*risk register*), nella fase di analisi si definiscono invece le probabilità e le conseguenze che tali rischi possono comportare, lasciando alla fase di valutazione dei rischi il compito di valutarli confrontandoli con i *risk criteria*. La fase di *risk assessment* permette quindi di trasformare i rischi individuati in strumenti utili per la creazione e la protezione di valore: La fase di *risk assessment* viene definita come un «Accurato costrutto, costantemente in evoluzione e regolarmente eseguito dall'impresa per esaminare i rischi, sia positivi che negativi, attribuendo loro un grado di priorità usando e combinando metodologie quantitative e qualitative per comprendere l'influenza che un rischio ha sull'impresa»[159].

1) La prima fase del *risk assessment* consiste nella *Risk Identification*: dopo aver definito il contesto in cui l'impresa opera è necessario identificare i rischi che saranno fronteggiati in quanto, se essi non vengono individuati, risulta impossibile procedere ad una gestione degli stessi. Ogni processo di *risk management* richiede perciò che vengano identificati gli eventi rischiosi intesi sia come opportunità che come esiti negativi, cercando di comprendere anche quale sia la fonte che li genera. È un'attività che necessita di essere svolta periodicamente su base continua in quanto «un rischio individuato la settimana scorsa, non sarà lo stesso rischio che verrà identificato la settimana successiva»[160].

Lo Standard ISO 31000 definisce la fase di *risk identification* nel modo seguente

«l'impresa dovrebbe identificare le fonti di rischio, le aree d'impatto, gli eventi (compresi i cambiamenti di circostanze), le cause scatenanti tali eventi e le potenziali conseguenze. Lo scopo di questa fase è quello di generare un elenco completo di rischi basato sugli eventi che potrebbero

[158] Lo Standard ISO 31000 definisce la fase di risk assessment come "*Il processo generale di identificazione, analisi e valutazione del rischio*".
[159] Williams (aprile 2018).
[160] Chapman (2006).

migliorare o pregiudicare, accelerando o ritardando, il raggiungimento degli obiettivi. È importante identificare i rischi che non sono associati al perseguimento di un'opportunità. Un'identificazione completa è cruciale in quanto un rischio che non è identificato in questa fase, non sarà incluso in un'analisi futura»[161].

Lo Standard CoSO fa riferimento a questa fase come la fase di "*identificazione degli eventi*" e la definisce nel modo seguente

«Il management identifica gli eventi potenziali che, nel caso in cui si verifichino, colpiranno l'intera impresa e determina se essi rappresentano un'opportunità o una minaccia alla capacità dell'impresa di implementare strategie e raggiungere gli obiettivi. Eventi con un impatto negativo rappresentano rischi per i quali è richiesta una responsabilità e una valutazione da parte del management, mentre gli eventi con un impatto positivo rappresentano opportunità che il management deve inglobare nel processo di definizione di obiettivi e strategie. Nel processo di identificazione degli eventi il management considera una varietà di fattori interni ed esterni che possono far sorgere rischi e opportunità»[162]

L'elemento comune alle definizioni proposte dai due Standard consiste nel fatto che entrambi fanno riferimento ai rischi in senso sia negativo che positivo[163]. L'obiettivo del processo di *risk identification* dovrebbe quindi essere quello di produrre una lista di rischi, chiamata *risk register*, che possono colpire l'impresa sia in modo positivo che negativo in modo tale da comprendere il contributo che può derivarne dall'assunzione[164].

Vengono individuati alcuni errori concettuali che tipicamente vengono commessi in questa fase: un primo errore riguarda la *Reattività al problema* in quanto spesso le imprese evitano di occuparsi di una determinata questione semplicemente perché essa non viene considerata urgente, ma attendere finché questa non sia diventata un problema può pregiudicare il raggiungimento degli obiettivi. un secondo problema discende dall'*assenza di un approccio metodologico per identificare i rischi* perché non si tratta solo di redigere una lista dei rischi ma è necessario applicare un processo metodologico che può variare ad esempio a seconda dei soggetti destinatari o dello scopo (l'intera impresa, il progetto, la *business unit*, ecc.). avere un metodo di lavorazione permette di identificare

[161] ISO/Guide 73:2009 Risk management – Vocabulary
[162] CoSO (2017).
[163] Williams (2018).
[164] Williams (2018); Chapman (2006).

tutte le più importanti attività nonché i possibili rischi e conseguenze ad esse collegate. Un terzo problema concerne il n*on vedere il rischio nel più generale contesto d'impresa* in quanto uno degli errori più comuni nel processo di identificazione del rischio consiste nell'osservare i rischi attraverso la "lente di una particolare *business unit*" contraddicendo lo scopo principale dell'ERM[165].

Identificare il rischio non significa semplicemente indirizzarlo ad una specifica *business unit* ma piuttosto esaminare il suo impatto su tutta l'impresa, sulla strategia, ecc. un quarto problema è strettamente collegato all'*identificazione di un rischio senza però averne capito lo scopo* e infatti molto spesso *managers* e *directors* di una specifica *business unit*, una volta individuato un rischio significativo per la loro area di competenza, tendono a farlo rientrare esclusivamente nella propria *business unit*. È invece necessario che essi lavorino congiuntamente con tutte le altre aree di business, affinché quel rischio individuato venga esplicitato nella sua interezza considerando anche gli impatti che potrebbe avere non solo nella principale area di competenza ma anche in quelle pertinenti. Un quinto problema riguarda la *mancata costituzione di un processo di risk identification su misura* perché molte imprese tendono a fare semplicemente un copia e incolla degli stessi approcci applicandoli a tutta l'impresa. È invece fondamentale adottare un processo su misura che si adatti all'impresa e alla sua cultura per evitare che il processo sia fallimentare. Un sesto problema fa riferimento *all'utilizzo di un singolo metodo di identificazione del rischio* con la diretta conseguenza che il metodo di individuazione utilizzato ai livelli inferiori dell'impresa potrebbe non essere adatto per il processo di individuazione; infine un ultimo problema riguarda la *convinzione che l'attività di risk identification sia un'attività da svolgere una tantum*. È fondamentale ricordare che i rischi sono sempre in continuo cambiamento e di conseguenza non è sufficiente identificarli una sola volta ma è necessario procedere ad un processo di revisione periodico.

Chiariti i principali errori che possono essere commessi in questa fase, il primo passo consiste nella determinazione del contesto così come descritto nel capitolo precedente e successivamente si dovrà determinare l'approccio e la metodologia che verrà utilizzata. Per quanto riguarda l'approccio questo può essere[166]:

- *Top-Down*. È un approccio che viene utilizzato dai componenti del consiglio di amministrazione e dai dirigenti di alto livello che definiscono le strategie avendo riguardo dell'impresa nel suo complesso e diffonderanno poi delle informazioni raccolte a tutti i livelli dell'impresa fino a quelli più bassi.

[165] Williams (2018).
[166] Williams (2018).

- *Bottom-Up*. Questo approccio affonda invece le radici direttamente nel progetto, nella funzione o nel processo a cui si riferisce andando molto più nel dettaglio. Saranno quindi i soggetti che svolgono l'attività in queste singole aree a fornire indicazioni circa i rischi riscontrati attraverso un reporting per i vertici.

Per quanto riguarda invece le metodologie di identificazione si rilevano le seguenti tipologie[167], le cui caratteristiche chiave sono sintetizzate nella Fig. 2.16:

Fig. 2.16 – Principali metodologie per un processo di risk identificatione

	Best Use	Approccio	Audience	Contesto	Benefici	Difficoltà
Workshop	Identificare tutti i rischi dell'impresa con l'ausilio di un piccolo gruppo di executives	Top-Down	Un piccolo gruppo di membri del Cda, top executives o dirigenti di alto livello	I principali rischi di tutta l'impresa	Individuare i collegamenti tra i rischi e assegnarli ai rispettivi risk owners	Sintetizzare i risultati in una lista di "rischi di alto livello"
Interviste	Identificare i principali rischi dell'impresa così come visti dagli executives	Top-Down	Incontri one-on-one con gli executives o il top management	I principali rischi di tutta l'impresa	I partecipanti sono più propensi alla condivisione in questo tipo di ambiente	Comprenderendere le preoccupazioni e classificare i rischi
Scenario Analysis	Identificare i rischi che hanno una bassa probabilità di verificarsi ma che possono avere un grande impatto nel processo decisionale	Entrambi	Top managemen o midlle management	Rischi strategici e fatal risks; identificare l'impatto dei possibili cambiamenti	Stimolare i partecipanti ad individuare nuovi fattori, interdipendenze, punti cechi e bias	Porre delle domande che siano adeguate
Sondaggi	Identificare i rischi all'interno dell'organizzazione	Bottom-Up	Middle management e lo staff di supporto	Business level o a livello di singole operazioni	Dà allo staff la possibilità di partecipare al processo; identifica i rischi visibili solo dallo staff	Maneggiare un gran numero di informazioni richiede processi e strumenti adeguati
Root Cause Analysis	Comprendere la causa principale di una situazione che si conosce e utilizzarla per identificare i rischi ad essa collegati	Bottom-Up	Middle management e lo staff di supporto	Progetti specifici o specifiche operazioni	Permette di scoprire nuovi rischi che altrimenti sarebbero rimasti nascosti	le discussioni possono essere molto dettagliate

Fonte: Rielaborazione personale Carol Williams, 5 effective methods to identify risks in your organization, 2018

Vengono poi annoverati tra i meccanismi di *risk identification* anche[168]:

- L'*analisi SWOT*;
- L'*analisi PEST* (Political, Economic, Social e Technological);
- La *Risk Checklist*, nella quale vengono indicati alcuni dei rischi precedentemente individuati (ad esempio in altri progetti);
- *Risk List*, è un elenco di tutti i rischi suddivisi per tipologia o area di riferimento.

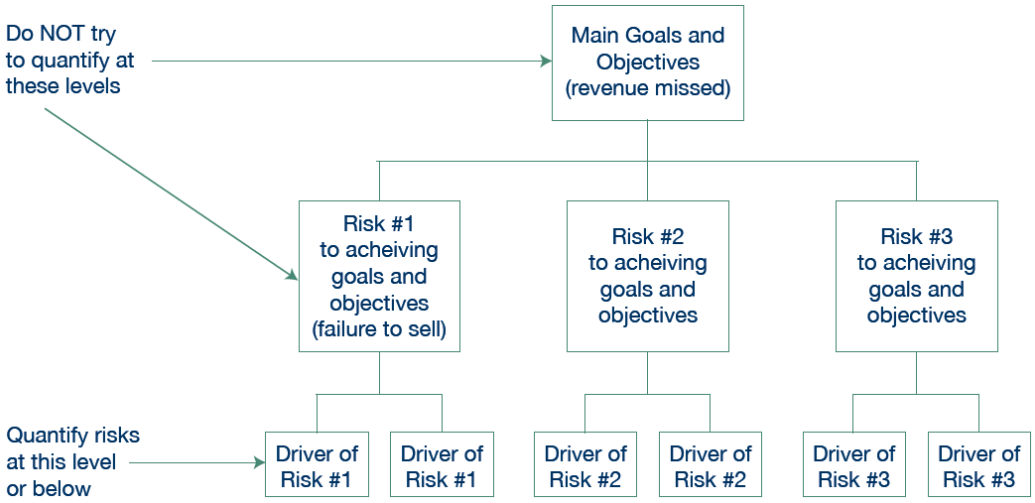
[167] Williams (2018).
[168] Chapman (2006).

L'attività di identificazione dei rischi permette quindi di chiarire gli obiettivi dell'impresa in relazione ai rischi individuati, di revisionare l'analisi di business alla luce dei nuovi rischi emersi descritta nel precedente capitolo, identificare i rischi e le opportunità nonché individuare le possibili interdipendenze al fine di ottenere una loro descrizione accurata.

2) la seconda fase di *risk assessment* è la *Risk Analysis*. In questa fase i rischi identificati vengono analizzati per stabilire la probabilità che si verifichino e quali siano le relative conseguenze così da poterne determinare il livello di rischio[169]. Al termine di questa fase il registro rischi redatto nella fase di identificazione verrà ampliato tenendo conto delle probabilità di ciascun rischio in esso indicato e l'impatto che questo potrà generare in termini sia positivi che negativi[170].

Prima di quantificare un rischio sarà necessario comprenderne le cause individuando i potenziali *risk drivers* (ad esempio attraverso una *root cause analysis* o una *scenario analysis*) in modo tale da ottenere ulteriori informazioni[171] perché, quantificare un rischio ad un livello troppo alto potrebbe rendere difficoltoso individuare cause e soluzioni, mentre analizzandolo in dettaglio, sarà possibile suddividere problemi complessi in problemi più semplici[172] (vedi Fig. 2.17).

Fig. 2.17 – Quando quantificare, l'importanza dei risk drivers



Fonte: IMA, Enterprise Risk Management: Tools and Techniques for Effective Implementation, 2007

[169] Lo Standard ISO 31000 definisce *likelihood* come le probabilità che si verifichi un evento, sottolineando che questo può essere definito, determinato, misurato soggettivamente e oggettivamente e infine può essere espresso sia qualitativamente che quantitativamente. Lo Standard definisce poi *consequence* come il risultato di un evento e l'effetto che esso ha sugli obiettivi una singolo evento può generare un range di conseguenze che possono avere effetti sia positivi che negativi sull'obiettivo. Lo Standard definisce infine il *level of risk* come la magnitudo di un rischio considerando in modo combinato probabilità e conseguenze e può essere assegnato ad un singolo rischio o ad un gruppo di rischi.
[170] Chapman (2006).
[171] The Association of Accountants and Financial Professionals in Business (IMA), 2007
[172] Williams (aprile 2018); IMA (2007).

Le analisi che possono essere svolte in questa fase, rientrano in tre categorie[173]:

- *Analisi qualitative*. Questo tipo di analisi utilizza elementi descrittivi per rappresentare effetti e probabilità
- *Analisi semi-quantitative*. Alle categorie che sono state individuate tramite l'analisi qualitativa viene attribuito un numero che non quantifica la probabilità o gli effetti in senso stretto, bensì permette di ordinare le diverse tipologie per importanza
- *Analisi quantitative*. Queste determinano in maniera analitica la distribuzione di probabilità associata ad un determinato evento rischioso.

Le analisi qualitative e semi-quantitative sono più semplici e meno costose rispetto a quelle quantitative anche se un'analisi accurata può essere effettuata solo attraverso queste ultime. Nella prassi le tecniche qualitative e semi-quantitative vengono utilizzate come primo *step* di una preliminare selezione delle principali categorie di rischio, per poi procedere ad una più accurata analisi qualitativa. La discriminante nella scelta delle tecniche di analisi riguarda il confronto tra costi e benefici in termini di conoscenza dei fenomeni analizzati e le informazioni che si hanno a disposizione (serie storiche, modelli teorici e sperimentali, esperienza dei soggetti coinvolti)[174].

Alcuni esempi di *analisi qualitative* possono essere: il giudizio degli esperti, *surveys, risk maps, risk ranking o workshop*. La tecnica più diffusa è quella della *risk map* nota anche come *risk matrix*, *heat map* o *matrice probabilità-impatto*, la quale considera cinque classi di probabilità, cinque classi di impatto e quattro classi di *risk rating* per ciascuna delle quali corrisponde una valutazione del rischio[175] (vedi Fig. 2.18 e Fig. 2.19).

[173] Floreani (2004)
[174] Floreani (2004). Lo stesso autore ricorda inoltre che l'informazione circa gli eventi aleatori determina incertezza sulle stime e continua poi sottolineando che i rischi finanziari vengono stimati quantitativamente in quanto si dispone di dati osservabili sul mercato, i rischi puri sono stimati quantitativamente solo se si dispone di serie storiche sufficientemente ampie, mentre i rischi strategici e operativi sono i rischi col più alto livello d'incertezza in quanto modifiche nell'ambiente rendono di difficile utilizzo le serie storiche di cui si dispone. Conclude poi evidenziando che le tecniche quantitative sono sempre utilizzabili per stimare la distribuzione di qualsiasi variabile aleatoria fornendo, almeno a livello teorico, la migliore conoscenza del fenomeno, ma la scelta di utilizzare tali tecniche a discapito di quelle qualitative avverrà solamente se i benefici incrementali saranno maggiori dei costi incrementali.
[175] Floreani (2004); Williams (aprile 2018); IMA (2007).

Fig. 2.18 – Esempio di risk map, analisi qualitativa

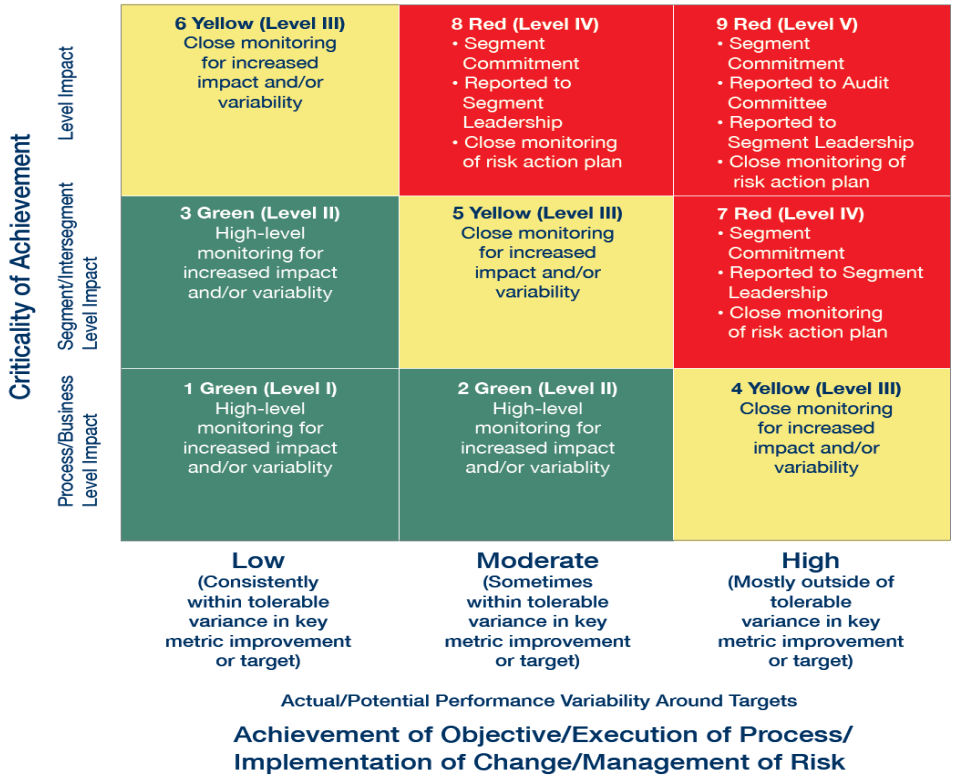
	Impatto				
Probabilità	**Insignificante**	**Basso**	**Moderato**	**Elevato**	**Catastrofico**
Quasi certo	Alto	Alto	Estremo	Estremo	Estremo
Probabile	Moderato	Alto	Alto	Estremo	Estremo
Moderata	Basso	Moderato	Alto	Estremo	Estremo
Improbabile	Basso	Basso	Moderato	Alto	Estremo
Rara	Basso	Basso	Moderato	Alto	Alto

Legenda (descrizione qualitativa del significato assunto dalle diverse classi di probabilità e impatto e del risk rating)

Probabilità	
Quasi certo	Avviene nella maggior parte dei casi (probabili maggiore del 50%)
Probabile	Avviene in una buona parte dei casi (probabilità tra 20% e 50%)
Moderata	Può accadere in un certo numero di casi (probabilità tra 5% e 20%)
Improbabile	E' improbabile che accada (probabilità tra 1% e 5%)
Rara	Accade solo in circostanze eccezionali (probabilità inferiore a 1%)
Impatto	
Catastrofico	Effetti economici disastrosi per l'azienda considerata
Elevato	Effetti economici molto elevati per l'azienda considerata
Moderato	Effetti economici moderatamente elevati per l'azienda considerata
Basso	Effetti economici piuttosto bassi per l'azienda considerata
Insignificante	Effetti economici trascurabili per l'azienda considerata
Risk Rating	
Estremo	Si richiede un immediato intervento per il trattamento del rischio
Alto	Si richiede una attenta valutazione del rischio da parte del responsabile di più elevato livello (individuato a seconda delle circostanze)
Moderato	Si richiede di individuare il responsabile per la sua gestione
Basso	Gestione attraverso procedure di routine

Fonte: Floreani, Enterprise Risk Management: I rischi aziendali e il processo di risk management, 2004

Fig. 2.19 – Esempio 2 di risk map (heat map)



Fonte: IMA, Enterprise Risk Management: Tools and Techniques for Effective Implementation, 2007

Utilizzare questa metodologia richiede però alcune cautele in quanto il processo potrebbe essere molto soggettivo dato che non tutti vedono il rischio allo stesso modo, potrebbero esserci degli interessi da parte di alcuni soggetti nell'indirizzare le risorse dell'impresa verso particolari rischi e infine possono essere commessi due tipi di errori, ovvero classificare un rischio non importante come rilevante (maggiore utilizzo di risorse in termini di tempo e costi quando invece non sarebbe necessario) e considerare un rischio importante come non rilevante (il rischio viene sottovalutato e può portare anche a gravi conseguenze)[176].

Le analisi semi-quantitative come detto, prendono come punto di riferimento le classificazioni ottenute attraverso l'analisi qualitativa assegnando dei numeri che permettono di valutare i rischi tramite un punteggio (*risk score*), rendendo quindi possibile ordinare i rischi per poi confrontarli. Basterà attribuire un punteggio alle probabilità e agli impatti indicati nella matrice probabilità-impatto per essere in grado di ordinare i rischi grazie al *risk score* dato dal prodotto tra i due[177] (vedi Fig. 2.20).

Fig. 2.20 – Esempio di risk map, analisi semi-quantitativa

	Impatto				
Probabilità	**Insignificante**	**Basso**	**Moderato**	**Elevato**	**Catastrofico**
Quasi certo	100	1.000	5.000	20.000	100.000
Probabile	50	500	1.250	10.000	50.000
Moderata	25	250	1.250	5.000	25.000
Improbabile	5	50	250	1.000	5.000
Rara	1	10	50	200	1.000

Probabilità	**Score**
Quasi certo	100
Probabile	50
Moderata	25
Improbabile	5
Rara	1
Impatto	**Score**
Catastrofico	1 000
Elevato	200
Moderato	50
Basso	10
Insignificante	1
Risk Score	Ottenuto dal prodotto tra score di probabilità e impatto
Estremo	Pari o superiore a 5 000
Alto	Pari o superiore a 500
Moderato	Pari o superiore a 50
Basso	Inferiore a 50

Fonte: Rielaborazione personale tabella di Floreani (2004)

[176] Floreani (2004); Williams (aprile 2018).
[177] Floreani (2004).

Infine, le *analisi quantitative* permettono di stimare la distribuzione di una variabile aleatoria rappresentando la *distribuzione dei risultati possibili*, ovvero l'impatto dei rischi sulla variabile obiettivo (ad esempio il patrimonio) oppure la *distribuzione delle perdite possibili*, ovvero la variazione negativa che il rischio può portare alla variabile obiettivo. Grazie alla stima della distribuzione dei risultati sarà possibile misurare i risultati utilizzando i principali indicatori statistici (ad esempio valore atteso, varianza, *value at risk*)[178].

Il metodo più diffuso per risolvere problemi riguardanti le variabile aleatori è rappresentato dalla simulazione *Monte Carlo* che determina la variabile aleatoria obiettivo simulandone un elevato numero di realizzazioni in diversi scenari così da determinarne la distribuzione di frequenza[179].
Il risultato della *risk analys* permette quindi di generare un profilo di rischio che possa essere uno strumento per attribuire un grado di probabilità a ciascun rischio in modo tale da rendere chiaro su quali rischi concentrare maggiormente gli sforzi di *risk treatment* e infatti lo Standard ISO 31000 afferma che «la *risk analysis* riguarda la comprensione del rischio […] e fornisce un *input* al processo decisionale nelle situazioni in cui le decisioni riguardano differenti tipi e livelli di rischio»[180].

3) La valutazione del rischio rappresenta l'ultima fase del processo di *risk assessment* e segue immediatamente la fase di analisi: lo Standard ISO 31000 sostiene infatti che «la *risk analysis* fornisce un input al processo di *risk evaluation*»[181]. Data la criticità di questa fase, un primo passo consiste nell'esaminare i risultati ottenuti dalla precedente analisi per essere sicuri che ad ogni rischio sia assegnato un corretto livello di rischio (*consolidamento dei risultati prodotti dalla risk analysis*). Questa è una fase molto importante perché in base al livello di rischio viene decisa l'intensità del processo di trattamento e perciò sarà necessario domandarsi, non se il rischio è stato stimato correttamente, bensì se il livello di rischio è corretto[182].

Vengono quindi valutati gli *inherent risks* (letteralmente: rischi inerenti) dell'impresa ovvero i rischi ai quali l'impresa è esposta prima di una qualsiasi operazione di trattamento che ne possa quindi alterare la probabilità o l'impatto[183]. Così facendo l'impresa valuta i rischi non solo singolarmente, ma anche a livello aggregato, classificandoli e attribuendo loro determinate priorità: non si tratta semplicemente di sommare tutti i rischi esistenti, bensì di considerare anche le possibili relazioni

[178] Floreani (2004). Si ricorda inoltre che il Value at risk (VaR) è un metodo statistico di misurazione del rischio di un portafoglio in risposta alle variazioni del mercato, che riassume la massima perdita attesa, su un dato orizzonte temporale, nei limiti di un intervallo di confidenza predefinito.
[179] Floreani (2004).
[180] Standard ISO 31000 (2018).
[181] Standard ISO 31000 (2018).
[182] Refsdal et al. (2015).
[183] Ricerca commissionata da CoSO (2012).

esistenti tra di essi in quanto alcuni rischi che singolarmente possono non essere considerati critici lo potrebbero diventare nel momento in cui vanno ad interagire con gli altri rischi.

La valutazione deve tenere in considerazione anche il livello di tolleranza al rischio stabilito nelle fasi iniziali del processo di ERM in quanto nessun rischio può eccedere tale livello e dovrà considerare poi anche la quantità di risorse da dedicare alla gestione dei rischi, singolarmente e a livello aggregato, per evitare sprechi.

6.4. FASE 3: Risk Treatment

La fase di *risk treatment* è la vera è propria fase di gestione del rischio e fa riferimento alle attività volte a ridurre, eliminare o a modificare il profilo di rischio individuato nella fase di *risk assessment*[184]. La fase di risk treatment consiste nelle seguenti attività[185]:

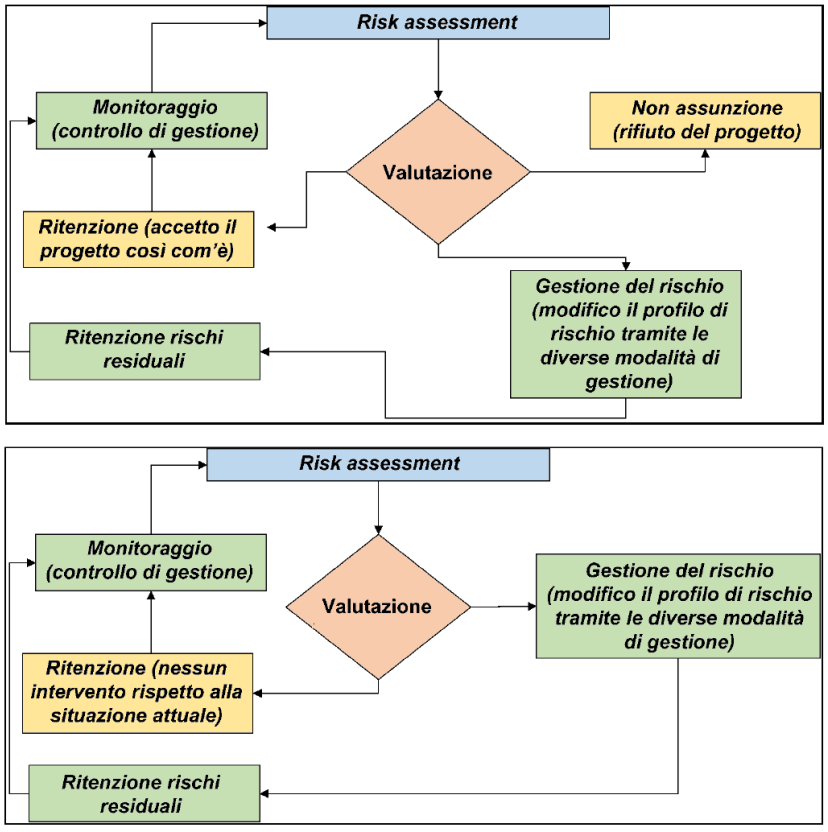
- *Avoid*. Attraverso la non assunzione, l'impresa decide di non intraprendere l'attività che introdurrebbe un rischio considerato inaccettabile. Optare per tale scelta implica che le misure di gestione del rischio attualmente in atto non sono adatte al trattamento di questo rischio o che i costi derivanti da una gestione dello stesso superano i benefici che sarebbero ottenuti o ancora, può implicare la presenza di attività alternative che comportano un rischio accettabile.
- *Accept*. Se nella fase di *risk assessment* viene rilevato che il rischio in esame è ritenuto accettabile o che i costi del trattamento sono inferiori ai benefici che saranno ottenuti da una sua gestione, allora l'impresa può decidere di accettare il rischio. Questo significa che le misure di gestione sono adeguate e non sarà necessario adottare ulteriori misure per trattare il rischio, con l'accortezza di monitorarlo costantemente
- *Reduction.* Si tratta di misure atte a modificare la distribuzione della variabile aleatoria riducendone probabilità e relative conseguenze e sarà attuata nel caso in cui l'eliminazione risulti eccessiva in termini di tempo e costi[186].

[184] Floreani (2004); Ricerca commissionata da CoSO (2012); Refsdal et al. (2015).
[185] Lo standard ISO 3100 indica che esso "può riguardare: evitare il rischio non intraprendendo o interrompendo l'attività che genera il rischio; assumere o incrementare un rischio al fine di perseguire un'opportunità; eliminare le fonti di rischio (risk source); modificare la probabilità (*likelihood*); modificare le conseguenze; trasferire il rischio ad un'altra controparte; trattenere il rischio dopo aver preso una decisione informata. La seguente classificazioni si basa, oltre che sulla definizione data dallo Standard ISO appena indicata, anche su Floreani (2004); Charted Accountants Australia and New Zeland.
[186] Floreani (2004) suddivide questa misura in prevenzione (che riduce la probabilità che si verifichino scenari sfavorevoli aumentando invece la probabilità degli scenari favorevoli) e in protezione (che riduce le perdite derivanti dagli scenari sfavorevoli).

- *Transfer*. È una misura atta al trasferimento del rischio ad un soggetto terzo il cui tipico strumento è rappresentato dalla stipula del contratto di assicurazione, ma ne sono validi esempi anche la stipula di contratti con fornitori di servizi o l'*outsourcing* della gestione di specifici *asset*.

Un'impresa che intraprende una nuova attività potrà quindi, a conclusione della fase di risk assessment e di un'analisi costi benefici circa il trattamento di gestione del rischio, decidere di non intraprendere il progetto (non assunzione) in quanto i rischi sono ritenuti non accettabili, di accettare il rischio senza alcun intervento (ritenzione) passando direttamente alla fase di monitoraggio dello stesso o infine, di gestire il rischio. Quest'ultima fase modificherà il profilo di rischio precedentemente calcolato con la conseguenza che l'impresa dovrà monitorare esclusivamente i rischi residuali[187] (vedi Fig. 2.21).

Fig. 2.21 – Il processo di risk treatment



Fonte: rielaborazione personale tabella Floreani (2004) I rischi aziendali e il processo di risk management

[187] Floreani (2004).
Si specifica inoltre che i rischi residuali sono i rischi che l'impresa si trova a dover sostenere dopo aver svolto il processo di gestione del rischio.
Per un'impresa che invece ha già avviato un'attività o un progetto lo schema risulterà analogo ad eccezione della mancanza della possibilità di non intraprendere l'attività (come si può notare nella parte sottostante della fig, 2.16).

Il processo di trattamento del rischio è poi formalizzato in un *risk tretament plan* nel quale vengono esplicitate le modalità di trattamento (non assunzione, ritenzione, riduzione trasferimento), i sistemi di controllo esistenti e gli eventuali sistemi di controllo che sarà necessario implementare e infine le modalità e la frequenza del monitoraggio[188].

6.5. FASE 4: Monitoraggio, Reporting, Comunicazione e Revisione

La decisione circa il trattamento del rischio non rappresenta l'ultima fase del processo di ERM: una volta che sono state decise le modalità con cui gestire il rischio, questo dev'essere monitorato perché

«I rischi non sono statici. La magnitudo e la probabilità di un determinato rischio è determinata dai controlli interni (mitigazione) così come dai cambiamenti dell'ambiente esterno"[189] e ancora, "il processo di ERM di un'impresa cambia nel tempo. Le modalità di risposta al rischio che un tempo erano efficienti potrebbero non esserlo più; le attività di controllo potrebbero essere meno efficienti o non più performanti; gli obiettivi dell'impresa potrebbero essere cambiati»[190].

L'ERM è quindi un processo ciclico che non si conclude con la fase di monitoraggio e *reporting*, ma anzi è proprio da queste ultime fasi che un nuovo ciclo deve iniziare. È perciò necessario che vi sia una continua e adeguata comunicazione circa i cambiamenti interni ed esterni che potrebbero ostacolare (o rafforzare) il raggiungimento degli obiettivi dell'impresa in modo tale che ogni *manager* responsabile valuti come questi cambiamenti possano influire su obiettivi e rischi ad essi connessi.

Gli obiettivi della fase di monitoraggio consistono nel controllo dell'andamento dei rischi assunti e dei rischi residuali e nel monitoraggio dell'obsolescenza dei risultati delle analisi, dei risultati che seguono le decisioni circa le modalità di trattamento del rischio ed infine del monitoraggio circa l'efficienza e l'efficacia del processo di ERM nel suo complesso[191]. La frequenza con cui l'attività di monitoraggio può essere svolta si rileva che essa può essere eseguita attraverso

[188] Lo Standard ISO 31000 sostiene che «Il *risk treatment plan* può riguardare, la ridefinizione dei controlli esistenti, l'introduzione di nuovi controlli, o il monitoraggio dei controlli esistenti. Rischi a basso impatto possono richiedere un monitoraggio periodico mentre i rischi a più alto impatto possono richiedere una maggiore attenzione da parte del *management*»
[189] Fraser e Simkins (2010).
[190] CoSO (2004).
[191] Damodaran (2016); Floreani (2004).

valutazioni periodiche o su base continua. Si sottolinea che esse non sono modalità reciprocamente esclusive, ma anzi possono essere combinate tra di loro per monitorare in modo più efficiente.

Le valutazioni periodiche vengono eseguite se l'intenzione è quella di concentrarsi sul processo di ERM come processo globale che riguarda tutta l'impresa e possono variare a seconda dello scopo, della frequenza o a seconda del grado di significatività del rischio: così ad esempio, i rischi con priorità più elevata verranno valutati più spesso di quelli a bassa priorità. Si rileva inoltre che le valutazioni periodiche riguardanti il processo di ERM nel suo complesso avverranno con minore frequenza rispetto alle sue componenti in quanto ciò si rende necessario a seguito di specifici cambiamenti che incorrono con minore frequenza, come ad esempio cambiamento del *management* o della strategia, fusioni o acquisizioni o rilevanti cambiamenti nell'ambiente esterno. Il limite delle valutazioni periodiche consiste nel fatto che generalmente esse vengono effettuate solamente dopo che il fatto si è verificato e perciò non vi sarà un'adeguata proattività.

Viceversa, il monitoraggio su base continua permette di analizzare in tempo reale le normali operazioni aziendali, fornendo dei *feedback* circa l'efficacia del processo di ERM attraverso un'analisi delle specifiche componenti. In questo modo il monitoraggio risponde dinamicamente ai cambiamenti che avvengono all'interno dell'impresa.

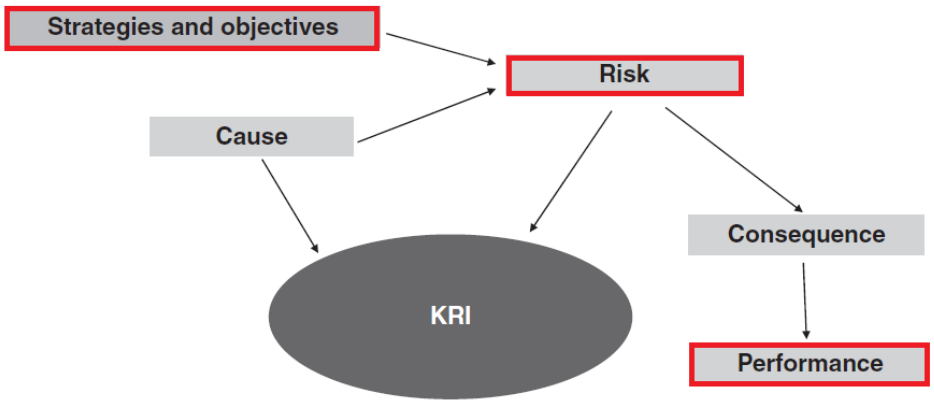
Una delle principali tecniche di monitoraggio su base continua è rappresentata dai *Key Risk Indicators* (*KRIs*) i quali vengono definiti come «Dati statistici che forniscono potenziali approfondimenti circa le situazioni future»[192], rappresentando quindi una misura che indica la potenziale presenza, il livello o il *trend* di un rischio: I *KRIs* sono uno strumento di misurazione ma possono anche indicare se un rischio si è verificato o se sta per verificarsi, indicandone il livello di esposizione al rischio e il *trend*. I *KRIs* misurano quindi il "*well-being*" di un'impresa e se correttamente definiti possono essere usati come strumento per anticipare gli eventi futuri ed essere utilizzati come strumenti di *warning* per i possibili cambiamenti nel profilo di rischio di un'impresa[193].

Sebbene alcuni *Key Performance Indicators* (*KPIs*) vengano utilizzati come *KRIs* è importante sottolineare come i primi siano delle misure circa la performance attuale dell'impresa (volume d'affari, fatturato, azioni di mercato, soddisfazione clienti), mentre i *KRIs* sono degli indicatori che supportano la fase di monitoraggio dei rischi e dei loro limiti e sono legati a rischi, performance e strategie[194] (vedi Fig. 2.22).

[192] Fraser e Simkins (2016).
[193] Fraser e Simkins (2010).
[194] Fraser e Simkins (2010).

Fig. 2.22 – Alcuni esempi di KRIs e il collegamento tra rischi performance e strategie

Human Resource	Information Technology	Finance
• Average time to fill vacant positions • Staff absenteeism/sickness rates • Percentage of staff appraisals below "satisfactory"	• Systems usage versus capacity • Number of system upgrades/version releases • Number of help desk calls	• Daily profit and loss adjustments (number, amount) • Reporting deadlines missed (number) • Incomplete profit and loss sign-offs (number, aged)
Legal/Compliance	**Audit**	**Risk Management**
• Outstanding litigation cases (number, amount) • Compliance investigations (number) • Customer complaints (number)	• Outstanding high-risk issues (number, aged) • Audit findings (number, severity) • Revised management action target dates (number)	• Management overrides • Credit defaults (number, amount) • Limit breaches (number, amount)



Fonte: rielaborazione personale tabella Fraser e Simkins, Enterprise risk management (2010)

I *KRIs* possono supportare strategia e performance nei seguenti modi: validano la struttura organizzativa e monitorando le performance in quanto un'attenta analisi dei *risk drivers* nel processo di definizione dei *KRIs* fornisce l'opportunità di verificare quanto siano realistici piani e obiettivi con la diretta conseguenza che i *KRIs* possono diventare parte integrante del processo di pianificazione strategico; I *KRIs* migliorano l'efficacia e l'efficienza aiutando le imprese a capire come allocare le risorse per ottenere il maggior rendimento *risk-adjusted*. Questo obiettivo può essere raggiunto considerando i *KRIs* nel processo di *risk assessment*; definiscono le aspettative legate al *risk-taking* in quanto, data la stretta correlazione tra *KRIs* e rischi più significativi, l'impresa sarà in grado di evidenziare le aree che richiedono maggiore attenzione nella fase di monitoraggio. Inoltre, i *risk limits* legati ai *KRIs* chiariscono ciò che è accettabile gestire e ciò che non lo è riflettendo il *risk appetite* dell'impresa anche perché essi sono misurabili; Infine, grazie alla capacità dei *KRIs* di monitorare in tempo reale il livello di rischio corrente nonché i *trend* e i cambiamenti ad esso legati, essi forniscono

un utile strumento di segnalazione per agire tempestivamente prevenendo o minimizzando le possibili perdite[195].

Ogni singola fase del processo di ERM, dalla definizione delle politiche di *risk management* fino alla fase di monitoraggio, richiede un costante flusso di comunicazione sia verso gli *stakeholders* esterni (investitori, banche, agenzie di rating), sia verso gli stakeholders interni (*Board of Directors*, *Management*, *manager* delle funzioni aziendali e delle *business unit*). Se la comunicazione avviene in modo regolare e trasparente allora essa potrà essere uno strumento per individuare le debolezze del processo in atto nonché il profilo di rischio dell'impresa. l'attività di reporting coinvolge tutta l'impresa e le comunicazioni possono derivare dall'alto, dal basso e orizzontalmente tra i diversi livelli aziendali circa l'esistenza del rischio, la sua natura, la forma, la probabilità, l'impatto, la valutazione, il grado di accettabilità, il trattamento o qualsiasi altro aspetto del processo di risk management[196].

[195] Fraser e Simkins (2010).
[196] Fraser e Simkins (2010)

CAPITOLO 3
GOVERNANCE E GESTIONE DEL RISCHIO

1. OWN RISK AND SOLVENCY ASSESMENT (ORSA)

L'art. 45 della direttiva *Solvency II* dispone per le imprese di assicurazione l'obbligo di effettuare una *procedura di valutazione interna del rischio e della solvibilità* (*ORSA*): questa viene definita dalla *European Insurance and Occupational Pension Authority* (*EIOPA*) come

«l'insieme di processi e procedure volte a identificare, valutare, monitorare, gestire e riportare i rischi a breve e a lungo termine che un'impresa di assicurazione affronta o potrebbe affrontare e a determinare i fondi propri necessari a garantire che i requisiti di capitale siano garantiti in ogni istante»[197].

L'art. 45 dispone inoltre che la valutazione riguarda almeno: il fabbisogno di capitale per assolvere agli obblighi di solvibilità con riferimento al profilo di rischio specifico, ai limiti di tolleranza al rischio e della strategia operativa dell'impresa di assicurazione (paragrafo 1 lettera a); la continua osservanza dei requisiti patrimoniali e delle riserve tecniche (paragrafo 1 lettera b); la misura in cui il profilo di rischio dell'impresa di assicurazione si discosta dal requisito patrimoniale di solvibilità calcolato mediante formula standard o mediante modello interno (paragrafo 1 lettera c).

L'art. 45 sancisce inoltre al paragrafo 2 il rispetto del *principio di proporzionalità* imponendo alle imprese di assicurazione di attuare processi commisurati alla natura, alla portata e alla complessità dei rischi della propria attività al fine di individuare e valutare i rischi a breve e a lungo termine. Lo stesso art. 45 al paragrafo 4 dispone inoltre che *la procedura ORSA è parte integrante della strategia operativa* e che deve essere considerata in modo sistematico in sede di decisione strategica sancendo poi al paragrafo 5 che essa debba essere effettuata periodicamente e immediatamente nel caso in cui si verifichi una variazione significativa del proprio profilo di rischio.

Il CRO Forum (2012) evidenzia come ORSA sia un "*termine ombrello*" per indicare una procedura che in realtà comprende: *un framework* in quanto definisce una serie di elementi di *risk governance* quali *risk tollerance* e *risk appetite* nonché la necessità di costituire una *policy* per la definizione dei *risk limits* e per le attività di monitoraggio e in generale è un processo che definisce

[197] EIOPA Guidelines.

un quadro di riferimento per l'attività di gestione del rischio; comprende poi *un report* (chiamato *ORSA Report*) il quale permette di confrontare l'approccio all'assunzione dei rischi rispetto al processo ORSA in corso, evidenziandone l'efficacia e mostrando i riflessi attuali e futuri che tale procedura ha e/o avrà sulla solvibilità; *Una policy* (*ORSA policy*) che contiene i principi e le descrizioni del processo ORSA, nonché la definizione dell'attività di *reporting*; Infine, l'ORSA è una *procedura di assessment di rischi e capitali* e include componenti di tipo *forward-looking*, in quanto considera anche i rischi a medio-lungo termine.

L'EIOPA, allo scopo di chiarire quali siano gli obiettivi che la procedura ORSA intende perseguire, emana delle linee guida suddividendole in 4 sezioni[198]:

- *Sezione 1, Considerazioni generali;*
- *Sezione 2, Evidenza del processo ORSA;*
- *Sezione 3, Funzionalità specifiche relative alle performance dell'ORSA;*
- *Sezione 4, Specificità per il processo ORSA a livello di gruppo.*

L'EIOPA sottolinea come l'impresa di assicurazione debba sviluppare un *processo ORSA su misura*, che si adatti alla propria struttura organizzativa e al proprio sistema di gestione dei rischi ribadendo la necessità di settare la procedura rispettando il *principio di proporzionalità* considerando quindi natura e complessità dei rischi assunti (*Guideline 1*) e suggerisce che l'Organo Amministrativo Direttivo o di Vigilanza (OADV o *Administrative Management or Supervisory Body, AMSB*) debba partecipare attivamente all'ORSA (*Guideline 2*)[199].

L'EIOPA indica poi che l'impresa deve dotarsi almeno della seguente documentazione (*Guideline 3*): la prima documentazione richiesta è l'*ORSA policy* e come indicato dall'art. 41 della direttiva Solvency 2 si richiede che l'impresa di assicurazione debba redigere per iscritto una *policy* di *risk management*[200] contenente (*Guideline 4*):

- Descrizione dei processi e delle procedure per la valutazione prospettica dei rischi;

[198] Il Consultation Paper On the Proposal for Guidelines on ORSA (EIOPA-CP-11/008 del 7 Novembre 2011) fornisce una linea guida articolata in 24 punti e racchiusa in 4 sezioni di cui nella seguente trattazione verranno esaminate solamente le prime 3 sezioni (nonché i primi 15 punti). Si specifica inoltre che nell'edizione EIOPA-BoS-14/259 IT (Orientamenti sulla valutazione interna del rischio e della solvibilità del Settembre 2015) non è presente la suddivisione nelle 4 sezioni e i punti componenti la linea guida sono 20 dei quali si esamineranno i primi 14.

[199] Nel Consultation Paper (2011) l'EIOPA sottolinea come l'ORSA sia uno strumento fondamentale per la comprensione dei rischi da parte dell'AMSB in quanto aiuta ad identificare e a valutare i rischi nonché ad assicurare che l'SCR sia adeguato ai rischi assunti. L'AMSB approva l'ORSA policy ed è sua responsabilità tenere in considerazione le risultanze del processo ORSA per il capital planning, la risk strategy e per l'assunzione dei rischi.

[200] L'ORSA policy è parte della risk management policy, EIOPA (2011) p. 15.

- Considerazione della relazione tra profilo di rischio, limiti di tolleranza e del fabbisogno di solvibilità globale;
- I metodi e le metodologie comprese le informazioni riguardanti le modalità e la frequenza degli *stress test*, le analisi di sensibilità, lo *stress test* inverso o altre analisi rilevanti, il *data quality*, la frequenza nella valutazione e il fondamento della sua adeguatezza nonché le tempistiche per l'esecuzione della valutazione e le circostanze che potrebbero generare la necessità di una nuova valutazione a prescindere dalle tempistiche di cui si è fatta precedente menzione.

L'impresa di assicurazione deve dotarsi di *un'evidence del processo ORSA* (*Guideline 5*) perché il risultato del processo dovrebbe essere dimostrato e documentato indicando le analisi di rischio individuali, il collegamento tra rischi e allocazione del capitale nel rispetto della *risk tolerance* e dei limiti di rischio, una descrizione dei metodi utilizzati e di come questi vengano validati, l'ammontare del fabbisogno di solvibilità richiesto per un singolo esercizio e per ogni esercizio considerato nel *business plan*, le conclusioni della valutazione, eventuali scostamenti tra *risk profile* e calcolo dell'*SCR*, i piani d'azione e infine come i fattori interni ed esterni siano presi in considerazione in un'ottica *forward-looking*; una terza tipologia di documentazione richiesta dall'EIOPA è *la relazione interna circa il processo ORSA* (*Guideline 6*) in quanto l'impresa di assicurazione dovrebbe comunicare almeno i risultati e le conclusioni tratte dal processo ORSA a tutto il personale interessato una volta che processo e risultati sono stati approvati dall'OADV. L'ultimo documento richiesto dall'EIOPA è infine *l'informativa per l'autorità di vigilanza*.

L'impresa di assicurazione deve stimare qualitativamente e quantitativamente il proprio fabbisogno di capitale necessario a rispettare i requisiti di solvibilità, fornendo anche una descrizione degli altri mezzi necessari per far fronte a tutti i rischi assunti indipendentemente dal fatto che essi siano quantificabili (*Guideline 8*) e sottoporre tutti i rischi individuati a una serie sufficientemente ampia di *stress test* o di *scenario analysis* per ottenere un'adeguata base per la valutazione del fabbisogno di solvibilità globale (*Guideline 9*), ricordando che tale valutazione deve avvenire in un'ottica prospettica (*forward-looking prospective*, *Guideline 10*). Nel caso in cui le basi per la contabilizzazione e la valutazione utilizzate siano diverse da quelle stabilite da *Solvency II* rispetto a quanto concerne la valutazione del fabbisogno di solvibilità, l'impresa di assicurazione deve indicare come esse risultino maggiormente in linea con il proprio profilo di rischio, la propria *risk tolerance* e con i propri *risk limits* fornendone una valutazione qualitativa e quantitativa (*Guideline 7*).

Il processo ORSA deve quindi garantire una chiara valutazione del fabbisogno di solvibilità in relazione alla strategia, al profilo di rischio, alla *risk tolerance* e ai limiti di rischio, valutandola in un'ottica di breve e di lungo termine in modo tale che l'impresa di assicurazione possa decidere se coprire i rischi col proprio capitale, utilizzare strumenti di mitigazione o entrambi.

In ottemperanza all'art. 45 paragrafo 1 lettera b, l'EIOPA indica la necessità per l'impresa di assicurazione di garantire che il processo ORSA consideri almeno[201]: le procedure che consentono all'impresa di monitorare in modo affidabile la sua compliance alla regolamentazione in materia di requisiti patrimoniali su base continuativa tenendo in considerazione anche le potenziali variazioni future del profilo di rischio (*Guideline 11 lettera a*); le procedure che permettono all'impresa di assicurazione di monitorare e gestire la qualità e la *loss assorbing capacity* dei fondi propri per tutto il periodo di pianificazione dell'attività (*Guideline 11 lettera b*)[202].

L'EIOPA richiede inoltre, nel rispetto dell'art. 45 paragrafo 1 lettera b, che l'impresa di assicurazione garantisca che la propria funzione attuariale accerti che vi sia un continuo rispetto dei requisiti riguardanti il calcolo delle riserve tecniche (*Guideline 12 lettera a*) e che individui i potenziali rischi che derivano dalle incertezze connesse a tale calcolo (*Guideline 12 lettera b*). le disposizioni contenute nell'art. 45 e nelle *Guideline* 11 e 12 derivano dalla necessità per l'impresa di verificare costantemente il proprio profilo di rischio in quanto cambiamenti ad esso legati, possono incidere anche sull'MCR e sull'SCR e non solo per quanto riguarda il normale svolgimento dell'attività assicurativa, ma anche in situazioni di *stress* e si richiede inoltre che le riserve tecniche debbano essere conformi in ogni momento ai requisiti di solvibilità.

L'EIOPA richiede poi che debbano essere valutate le eventuali variazioni tra il *risk profile* e le ipotesi sottostanti al calcolo dell'SCR attraverso un'analisi qualitativa e nel caso in cui vi siano scostamenti, attraverso una valutazione quantitativa (*Guideline 13*).

Si richiede altresì che vi sia un collegamento tra procedura ORSA e il processo di gestione strategica disponendo che le imprese di assicurazione debbano prendere in considerazione i risultati del processo ORSA almeno per quanto riguarda la gestione del capitale, la pianificazione dell'attività e per lo sviluppo e la progettazione dei prodotti (*Guideline 14*). L'EIOPA dispone infine che le imprese di assicurazione debbano attuare la procedura ORSA con frequenza almeno annuale (*Guideline 15*).

---

[201] EIOPA, Consultation Paper (2011)

[202] EIOPA-BoS-14/259 IT (Settembre 2015) tratta la Guideline 11 del Consultation Paper (2011) alla voce "orientamento 10" inserendo una lettera c, indicando che nel processso ORSA l'impresa di assicurazione deve considerare anche "*l'articolazione dei fondi propri in più livelli e come essa possa cambiare in relazione a dati di rimborso, restituzione a scadenza durante il periodo di pianificazione dell'attività*".

Il processo ORSA viene quindi descritto dal *National Association of Insurance Commissioners* (*NAIC*) come una valutazione interna svolta dalle imprese di assicurazione al fine di identificare e valutare i rischi attraverso una procedura su misura che deve adattarsi alle dimensioni e alla complessità dell'attività svolta[203].

Secondo il NAIC (2015) esiste una stretta relazione tra processo ORSA ed ERM, in quanto si afferma che gli obiettivi del processo ORSA consistono nel favorire la costituzione di un efficace sistema di ERM e nel favorire una prospettiva di gruppo su rischi e capitali (quest'ultimo punto si riferisce alle imprese di assicurazione facenti parte di un gruppo). Per una maggiore comprensione di tale procedura il NAIC ha prodotto nel 2012 un modello chiamato *Risk Management and Own Risk and Solvency Assessment Model Act (#505)* il cui scopo principale consiste nel fornire i requisiti necessari per la conservazione di un risk management framework, per completare il processo ORSA e per fornire una guida per la redazione dell'ORSA Summary Report[204].

l'*ORSA Summary Report* rappresenta il *report* finale redatto dall'impresa di assicurazione a seguito dell'attività di *own risk assessment*, il quale permette alle autorità di vigilanza di comprendere se l'attività di gestione del rischio sia adeguata e sottolinea come esso possa consistere in una combinazione di singoli *report* [205]. Sebbene molto simile, si tratta di un *report* differente da quello proposto dal *CRO Forum* (2012) in quanto l'*ORSA Report* indicato nell'elaborato di quest'ultimo è destinato principalmente all'Organo Amministrativo Direttivo o di Vigilanza (OADV o AMSB) perché lo scopo principale consiste nel fornire supporto alla pianificazione strategica, nel fornire una revisione annuale del sistema di *risk management* nonché una valutazione oggettiva di ogni processo decisionale. Il CRO Forum (2012) fornisce a scopo illustrativo una possibile struttura dell'*ORSA Report* (vedi Fig. 3.1):

[203] NAIC (2015).
[204] ORSA Model Act #505 (NAIC, 2012).
[205] ORSA Model Act #505 (NAIC, 2012); ORSA: Origins and Implications for ERM (NAIC, 2012).

Fig. 3.1 Struttura ORSA Report

Valutazione della solvibilità attuale e analisi per tipologia di rischio	Le imprese di assicurazione forniranno informazioni sulla situazione patrimoniale nonché una valutazione di come il capitale sia stato adeguato alla gestione dei rischi quantificabili e di quelli non quantificabili
Business planning e proiezione della valutazione di solvibilità	Dopo aver valutato la solvibilità attuale, l'impresa di assicurazione può fornire informazioni circa un business plan di medio termine e può includere in questa sezione anche una proiezione dei rischi e dei capitali
ORSA assessment	In questa sezione viene fornita una valutazione delle pratiche ORSA includendo un riassunto dei cambiamenti rispetto all'ultimo processo ORSA attuato
Descrizione dell'impresa di assicurazione	In questa sezione vengono fornite le informazioni circa la propria struttura di business e le modalità operative nonché una specificazione dell'ambiente in cui l'impresa di assicurazione si trova ad operare
Risk e Capital management framework	Questa sezione può fornire un approccio integrato per una gestione strategica di rischio e capitali. Per quanto riguarda il risk management ci si aspetta di ottenere una comprensione quanto più completa del risk framework dell'impresa di assicurazione e di come questa gestisca l'esposizione ai fattori esterni. Per quanto riguarda il capital management le imprese di assicurazione potrebbero fornire alcune informazioni circa le loro scelte di investimento e su come la gestione del capitale risponda a variazioni nell'esposizione
Panoramica sui modelli interni	In questa sezione viene fornita una panoramica circa i modelli interni, su come questi vengano utilizzati nei processi decisionali, nei reporting e nella gestione di rischi e capitale. Questa sezione fornisce quindi una visione circa i modelli interni, le loro limitazioni e i loro output

Fonte: Elaborazione personale Paper on ORSA, CRO Forum, Maggio 2012

Nell'*ORSA Guidance Manual* del 2014 rilasciata dal NAIC si riconosce l'ORSA come un processo unico per ogni impresa di assicurazione e come un processo che riflette le scelte di business plan, le scelte strategiche nonché il proprio sistema di ERM. L'*ORSA Summary Report* è quindi il prodotto del processo di ERM attuato dall'impresa di assicurazione e di conseguenza le informazioni in esso contenute dovrebbero essere consistenti con le informazioni prodotte dal processo di ERM. Questa stretta correlazione discende dalla necessità per l'*ORSA Summary Report* di essere supportato dalle informazioni sul rischio elaborate internamente dall'impresa di assicurazione richiedendo quindi di documentare l'ERM *framework*.

Secondo il NAIC (2015) l'ORSA *Summary Report* è costituito da tre sezioni: la prima è rappresentata dalla *descrizione dell'ERM Framework* nella quale l'impresa di assicurazione descrive il proprio processo di ERM includendo almeno i seguenti *reporting principles* previsti dal Modello #505 (vedi Fig. 3.2):

Fig. 3.2 – Principi sezione 1 Model #505

Risk Culture e Governance	Verranno indicati i ruoli e le responsabilità circa il processo di ERM e la struttura di governance. Sarà inoltre necessario reportare la propria risk culture
Risk Identification e Risk Prioritization	Verranno fornite giustificazioni circa il processo di risk identification. Questo principio può essere visto come un stimolo all'implementazione di un processo di ERM olistico che consideri e categorizzi i rischi, qualitativi e quantitativi a livello di impresa e non di singole business unit, descrivendo come questi rischi sono stati individuati
Risk Appetite, Tolerance e Limits	Con questo principio si vuole stimolare le imprese di assicurazione a creare un "formal risk appetite statement" nonché definire in modo esplicito la propria risk tolerance e i propri risk limits
Risk Management e Risk Control	Si richiede di documentare le misure utilizzate per ridurre la frequenza e la severity dei rischi nonché gli effetti che si intende ottenere da tali pratiche. È un processo su base continua che richiede di controllare costantentemente il proprio processo di gestione del rischio indicando come esso viene valutato, implementato e monitorato
Risk Reporting e Communication	Questo principio richiede che le imprese di assicurazione adottino un sistema di reporting e di comunicazione trasparente nei confronti di tutti gli stakeholder nonché del board of directors e delle autorità di vigilanza

Fonte: elaborazione personale ORSA Origin and Implication for ERM (NAIC, 2015)

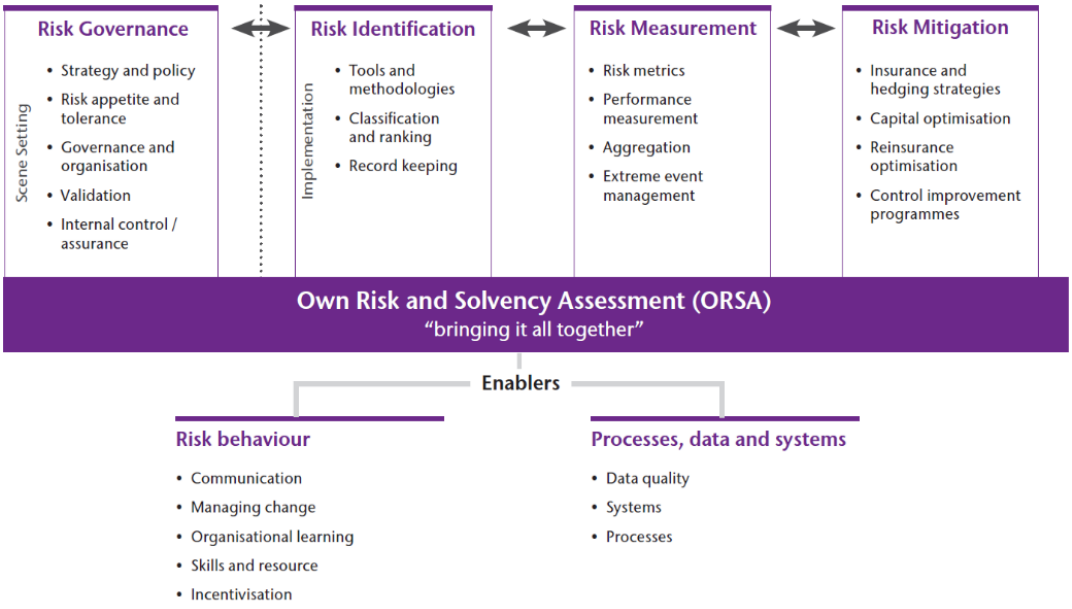
La seconda sezione è quella di *Risk assessment* nella quale si richiede alle imprese di assicurazione riportino i risultati della procedura di *assessment*, fornendo una descrizione dei rischi, dei possibili impatti e delle probabilità stimate nonché le assunzioni usate per analizzare i rischi, gli strumenti di mitigazione e il risultato dei possibili scenari di perdita; L'ultima sezione individuata è infine quella di *Group risk assessment*[206].

NAIC e CRO Forum propongono due tabelle nelle quali viene rispettivamente effettuato un confronto tra i principi proposti dal NAIC in merito alla procedura ORSA, gli standard ISO 31000 e CoSO e un possibile *ORSA framework* a supporto della tesi secondo cui la procedura ORSA è strettamente collegata al processo di ERM[207] (vedi Fig. 3.3).

[206] La terza sezione dell'*ORSA Summary Report* non è oggetto di studio nella seguente tesi. Per approfondimenti si rimanda a *ORSA: Origin and Implication for ERM (NAIC, 2015)*.
[207] CRO Forum (2012); NAIC (2015).

Fig. 3.3 – Processo ORSA e Processo ERM: le evidenze di NAIC e CRO Forum

ORSA Minimum Principles	COSO ERM Components	ISO 31000 Process
Risk Culture and Governance	Internal Environment Objective Setting	Establishing the Context
Risk Identification and Prioritization	Event Identification Risk Assessment	Risk Assessment Risk Identification Risk Analysis Risk Evaluation
Risk Appetite, Tolerance and Limits	Internal Environment	Establishing the Context
Risk Management and Controls	Risk Response Control Activities	Risk Treatment
Risk Reporting and Communication	Information and Communication Monitoring	Communication and Consultation Monitoring and Review



Fonte: Rielaborazione personale tabelle *ORSA: Origin and Implication for ERM (NAIC, 2015)* e CRO Guide to Solvency II (CRO Forum, 2012)

In conclusione, viene esaminata la lettera IVASS al mercato del 20 Febbraio 2019 riguardante l'andamento della procedura ORSA basandosi sui *Report ORSA 2017*.

La prima informazione che è possibile trarre dalla Lettera IVASS al mercato consiste nel progressivo allineamento al regolamento ORSA[208] per quanto riguarda l'orizzonte temporale (3-5 anni), i tempi di trasmissione all'autorità di vigilanza e per l'utilizzo dello schema della relazione per il supervisore[209]. È possibile poi osservare una maggiore integrazione nel processo di gestione

[208] Il regolamento menzionato è il regolamento n. 32 del 9 Novembre 2016 recante disposizioni in materia di valutazione del rischio e della solvibilità. Alla pagina 1 di tale regolamento si legge "*Le linee guida EIOPA, sono corredate da indicazioni più di dettaglio (c.d. explanatory text) che l'Istituto considera nell'esplicazione concreta dell'attività di vigilanza anche laddove, rilevata la loro natura, non siano riprese in disposizioni regolamentari*" e infatti è possibile notare numerose similitudini tra le linee guida EIPA citate in questo capitolo e il presente regolamento.

[209] L'IVASS nel Regolamento n. 32 del 9 Novembre 2016, per quanto riguarda la relazione da trasmettere al supervisore fa riferimento all'*ORSA Supervisory Report* ovvero un report, definito dalla Prudential Regulation Authority (PRA), che includa un chiaro riassunto del processo svolto e dei risultati ottenuti, che non sia eccessivamente lungo e che sia fornito di adeguata documentazione.

dell'impresa che conferma il processo ORSA come necessario per l'aggiornamento del piano strategico nonché ai fini del processo decisionale. Cresce l'importanza dell'attuario all'interno del processo ORSA soprattutto per quanto concerne l'individuazione dei rischi tecnici e per le definizioni di *baseline scenario* e di scenari avversi.

Si evidenzia una maggior consapevolezza dei rischi da parte delle imprese con un progressivo rafforzamento del *Risk Appetite Framework* (*RAF*) e si osserva un irrobustimento del processo di analisi delle esposizioni presenti e potenziali, nonché una maggiore chiarezza per quanto concerne la definizione di criteri, metodologie, dei processi di *assessment* e nella definizione degli obiettivi di solvibilità e dei principali rischi. Si sottolinea però la necessità di un miglioramento del processo di determinazione degli obiettivi di solvibilità e delle soglie di tolleranza oltre che di una maggiore specificazione delle azioni correttive da attivare nel caso tali soglie vengano raggiunte.

Emerge poi come i rischi di natura finanziaria (primo fra tutti il rischio *spread* seguito dal rischio tasso di interesse e dal rischio azionario) siano percepiti come maggiormente rilevanti rispetto a quelli "tecnici". Inoltre, si osserva un'insufficiente attenzione relativa ai rischi non inclusi nel primo pilastro con la conseguente necessità da parte delle imprese di assicurazione di porre ulteriori attenzioni circa il processo di definizione, rilevazione e mitigazione dei rischi che non generano requisiti patrimoniali.

2. IL SISTEMA DEI CONTROLLI INTERNI

Il sistema dei controlli interni (SCI) rappresenta l'insieme di strutture, procedure e regole che sovrintendono al corretto funzionamento e al buon andamento dell'impresa nel contesto economico e normativo di riferimento[210]. Lo scopo principale è quello di assicurare che gli obiettivi dell'impresa siano perseguiti e supportati da un adeguato monitoraggio e un'efficace gestione dei rischi, ottenute mediante la predisposizione di idonee *policy* e procedure e mediante un'adeguata attività di controllo[211]. Il sistema dei controlli interni è composto sia dagli organi sociali (amministrativo e di controllo) che dalle funzioni cosiddette di controllo interno oltre che dalle funzioni operative e di *business*[212]. Il sistema dei controlli interni si articola su 3 livelli[213] (vedi Fig. 3.4): *Il primo livello*

[210] Febbi e Bobbo (Giugno 2016).
[211] Febbi e Bobbo (Giugno 2016). Gli autori sostengono inoltre che un'altra finalità del sistema di controllo interno è rappresentata "*dal monitoraggio dell'economicità operativa della struttura aziendale, attraverso la costante verifica che le operazioni gestionali siano eseguite secondo principi di efficacia (raggiungere gli obiettivi prestabiliti) efficienza (raggiungere gli obiettivi con l'uso razionale di risorse) economicità (capacità di svolgere le attività utilizzando risorse al minor costo possibile*", cit. p. 1.
[212] Febbi e Bobbo (Giugno 2016).
[213] Febbi e Bobbo (Giugno 2016).

definito come "*controlli di linea*", è svolto dai soggetti impiegati nelle funzioni operative e di *business* e assicura che tali operazioni siano svolte correttamente. Questi sono definiti "*controlli diretti*" perché svolti nell'esercizio delle attività aziendali; *il secondo livello* ricomprende la funzione di *risk management* e di conseguenza l'attività di misurazione monitoraggio e gestione dei rischi nonché la funzione di *compliance*, la quale si occupa di verificare la conformità delle operazioni aziendali alle normative e ai regolamenti; infine, *il terzo livello* riguarda la funzione di *internal audit* ed è in esso che si verificano la completezza, l'adeguatezza, l'efficacia e l'efficienza di tutto il sistema dei controlli interni. Il secondo e il terzo livello vengono definiti "*controlli indiretti*" perché basati su flussi informativi derivanti da accertamenti diretti.

Fig. 3.4 – Gerarchia del sistema dei controlli interni

Fonte: www.generali.com Controllo interno e gestione dei rischi

In ambito assicurativo il sistema dei controlli interni viene fatto rientrare dalla direttiva *Solvency II* all'interno del secondo pilastro nell'art. 46, nelle disposizioni dedicate ai controlli e alla *governance* e viene disposto che «le imprese di assicurazione e di riassicurazione dispongono di un sistema di controllo interno efficace» e che «tale sistema includa almeno procedure amministrative e contabili, un quadro di riferimento del controllo interno, disposizioni di segnalazione adeguate a tutti i livelli dell'impresa ed una funzione di verifica della conformità»[214].

A livello Nazionale l'art. 46 è stato recepito dal Codice delle Assicurazioni Private (CAP) all'art. 30-quarter, il quale reca al comma 1 «L'impresa si dota di un efficace sistema di controllo interno»[215] e continua al comma 2 disponendo che esso comprenda almeno

«la predisposizione di idonee procedure amministrative e contabili l'organizzazione di un adeguato sistema di trasmissione delle informazioni per ogni livello dell'impresa, nonché l'istituzione

[214] Art. 46 Direttiva Solvency II paragrafo 1 comma 1 e 2.
[215] Art. 30-quarter comma 1.

della funzione di verifica della conformità dell'attività dell'impresa alla normativa vigente, alle direttive e alle procedure aziendali»[216].

A livello regolamentare i principi generali dettati dal CAP sul sistema dei controlli interni, vengono disciplinati dal Regolamento ISVAP n. 20 del 26 marzo 2008 (*Regolamento 20*), integrato poi con Provvedimento IVASS n.17 del 15 Aprile 2014 (*Provvedimento 17*) al fine di allinearne i contenuti agli "*Orientamenti sul sistema di governance proposto dall'EIOPA*"[217]. Secondo L'art. 4 del Regolamento 20 così come modificato dal Provvedimento 17:

- Il sistema dei controlli interni deve essere strutturato nel rispetto del principio di proporzionalità in quanto si deve tenere conto della natura, della portata e della complessità dei rischi aziendali inerenti alla propria attività, anche in un'ottica prospettica (attuali e prospettici)[218];
- Viene ripresa la definizione di sistema di controlli interni come esposta all'inizio del presente paragrafo, indicando che esso garantisce[219]: efficacia ed efficienza dei processi aziendali; adeguato controllo dei rischi attuali e prospettici; tempestività del sistema di *reporting* delle informazioni aziendali; attendibilità e l'integrità delle informazioni contabili e gestionali; salvaguardia del patrimonio anche in un'ottica di medio-lungo periodo; conformità dell'attività dell'impresa alla normativa vigente, alle direttive e alle procedure aziendali.
- «I presidi […] coprono ogni tipologia di rischio aziendale, anche secondo una visione prospettica ed in considerazione della salvaguardia del patrimonio. La responsabilità è rimessa agli organi sociali […]. L'articolazione delle attività aziendali nonché dei compiti e delle responsabilità degli organi sociali e delle funzioni deve essere chiaramente definita»[220].

All'art. 46 della Direttiva *Solvency II* e all'art. 30-quater del CAP viene poi disciplinata la *funzione di verifica della conformità* (*compliance*) che dispone che essa

[216] Art. 30-quarter comma 2.
[217] Gli orientamenti EIOPA sul sistema di governance possono essere esaminati nel Consultation Paper EIOPA-CP-13/08 "Guidelines on System of Governance".
[218] Art. 4 comma 1 Regolamento ISVAP n. 20 del 26 Marzo 2008 modificato dal Regolamento IVASS n. 17 del 15 Aprile 2014.
[219] Art. 4 comma 2 Regolamento ISVAP n. 20 del 26 Marzo 2008 modificato dal Regolamento IVASS n. 17 del 15 Aprile 2014.
[220] Art. 4 comma 2 bis Regolamento ISVAP n. 20 del 26 Marzo 2008 modificato dal Regolamento IVASS n. 17 del 15 Aprile 2014.

«[…] svolge l'attività di consulenza al consiglio di amministrazione sull'osservanza delle norme legislative, regolamentari e delle norme europee direttamente applicabili, effettuata la valutazione del possibile impatto sulle attività dell'impresa derivanti da modifiche del quadro normativo e degli orientamenti giurisprudenziali e identifica e valuta il rischio di non conformità»[221].

Il Regolamento 20 all'art. 22 definisce gli obiettivi della funzione di conformità sottolineando come si inserisca nel sistema dei controlli interni e viene poi disposto che le imprese si dotino ad ogni livello aziendale pertinente di specifici presidi per evitare il rischio di incorrere in sanzioni giudiziarie, amministrative, perdite patrimoniali o danni reputazionali a seguito di violazioni di leggi, regolamenti o provvedimenti delle Autorità di vigilanza[222].

Lo stesso Regolamento 20 all'art. 23 definisce l'attività della funzione di *compliance* ricordando che essa, essendo una funzione che si inserisce nel sistema dei controlli interni, debba rispettare il principio di proporzionalità (dev'essere proporzionata alla natura, alla portata e alla complessità dei rischi che riguardano la propria attività d'impresa) e che essa debba possedere adeguati requisiti di indipendenza[223]: identificare in modo continuativo le norme applicabili all'impresa e valutarne l'impatto su processi e procedure aziendali[224]; valutare l'adeguatezza e l'efficacia delle misure organizzative adottate al fine di prevenire il rischio di non conformità alle norme suggerendo inoltre eventuali modifiche organizzative e procedurali[225]; valutare l'efficacia degli adeguamenti organizzativi che discendono dalle modifiche suggerite[226]; predisporre adeguati flussi informativi diretti a agli organi sociali dell'impresa e alle altre strutture coinvolte[227].

La funzione di *internal audit* rappresenta un controllo di terzo livello e riveste un ruolo molto importante all'interno del sistema dei controlli interni in quanto assolve alla funzione di verifica generale circa la struttura e la funzionalità di questi ultimi.

L'*internal audit* è disciplinato dalla Direttiva *Solvency II* all'art. 47 e recepito nel nostro ordinamento nell'art. 30-quinquies del CAP che dispone:

[221] Art. 30-quater comma 3 CAP.
[222] Art. 22 comma 1 Regolamento ISVAP n. 20 del 26 Marzo 2008 modificato dal Regolamento IVASS n. 17 del 15 Aprile 2014.
[223] Art. 23 commi 1 e 4 Regolamento ISVAP n. 20 del 26 Marzo 2008 modificato dal Regolamento IVASS n. 17 del 15 Aprile 2014.
[224] Art. 23 comma 3 lettera a Regolamento ISVAP n. 20 del 26 Marzo 2008 modificato dal Regolamento IVASS n. 17 del 15 Aprile 2014 (Regolamento 20).
[225] Art. 23 comma 3 lettera b Regolamento 20.
[226] Art. 23 comma 3 lettera c Regolamento 20.
[227] Art. 23 comma 3 lettera d Regolamento 20.

- L'impresa istituisce un'efficace funzione di revisione interna garantendone autonomia di giudizio e indipendenza rispetto alle funzioni operative[228]. Il Regolamento 20 dispone inoltre che «la collocazione della funzione nell'ambito della struttura organizzativa deve essere tale da garantirne l'indipendenza e l'autonomia, affinché non ne sia compromessa l'obiettività di giudizio; la funzione di revisione interna non dipende gerarchicamente da alcun responsabile di aree operative»[229];
- La funzione di revisione interna valuta l'adeguatezza e l'efficacia del sistema dei controlli interni e delle ulteriori componenti del sistema di governo societario dell'impresa[230];
- La funzione di revisione interna comunica esiti e raccomandazioni dell'attività svolta indicando gli eventuali interventi correttivi che sarà necessario adottare. Sarà poi compito del consiglio di amministrazione definire i provvedimenti da adottare e garantirne l'attuazione[231].

La *European Confederation of Institutes of Internal Auditing* (*ECIIA*) fornisce una guida per la comprensione della funzione di *internal audit* all'interno delle imprese di assicurazione analizzando tre punti cardine di tale funzione, ovvero indipendenza, competenza e assistenza professionale ed infine l'etica professionale: il primo aspetto riguarda l'indipendenza che, come già esposto precedentemente, richiede che la funzione di *internal audit* abbia una sufficiente autorità per poter svolgere la propria attività con indipendenza e oggettività. Il soggetto responsabile della funzione di *internal audit* (*Head of the Internal Audit Function*) deve attuare una comunicazione diretta e costante con l'organo di supervisione, informare il comitato di *internal audit* circa l'adeguatezza (quantitativa e qualitativa) delle risorse utilizzate nello svolgimento dell'attività di *auditing* almeno su base annuale, nonché definire le strategie e l'organizzazione di tale funzione (nella definizione della strategia ci si aspetta che vengano definite metodologie, strategie di approvvigionamento e che venga definita la qualità dell'attività che si intende garantire). Egli deve inoltre informare il comitato di *internal audit* sui risultati dell'attività svolta senza l'ingerenza da parte del CEO o degli altri membri dell'*executive management* e deve comunicare in modo aperto e libero con gli *External Auditors*[232].

Un secondo aspetto riguarda la competenza e l'assistenza professionale per la quale si richiede che il responsabile della funzione di *internal audit* rispetti i requisiti indicati agli artt. 41 e 42 della

[228] Art. 30-quinquies comma 1 CAP e art. 47 paragrafo 1 comma 1 e 2 Direttiva Solvency 2.
[229] Art. 15 comma 2 Regolamento ISVAP n. 20 del 26 Marzo 2008 modificato dal Regolamento IVASS n. 17 del 15 Aprile 2014.
[230] Art. 30-quinquies comma 2 CAP e art. 47 paragrafo 2 Direttiva Solvency 2.
[231] Art. 30-quinquies comma 3 CAP e art. 47 paragrafo 3 Direttiva Solvency 2.
[232] ECIIA (Giugno 2019).

Direttiva *Solvency II*. Si richiede che il responsabile della funzione di *internal audit* consideri adeguatamente le capacità e le esperienze dello staff incaricato di svolgere l'attività di *internal auditing* al fine di garantire che le risorse umane impiegate in tale attività siano in grado di dare atto a tutti i punti definiti nel *piano di internal audit* per una sua corretta implementazione. Si richiede inoltre che la funzione di *internal audit* dimostri e documenti in modo adeguato la *policy* redatta per garantire la qualità della propria attività e si richiede infine che il responsabile della funzione di *internal audit* discuta e confermi assieme al comitato di *internal audit* il programma di valutazione della funzione di revisione interna[233].

Un terzo aspetto riguarda l'etica professionale per la quale si richiede che il responsabile della funzione di *internal audit* garantisca che tale funzione rispetti il codice etico specifico dell'impresa di assicurazione o in assenza, del *Global code IIA of ethic*[234].

L'ECIIA indica poi le aree che la funzione di internal audit dovrebbe considerare nello svolgimento della propria attività: la prima area esaminata è la pianificazione in quanto per il corretto funzionamento della funzione di *internal audit* risulta fondamentale pianificare adeguatamente tale attività disponendo una *policy* che sia in grado di stabilire, attuare e mantenere un idoneo processo di *internal audit* anche negli anni futuri. Si deve garantire che il piano sia sufficientemente flessibile in modo tale che possa adeguarsi il più rapidamente possibile ai cambiamenti che potrebbero intervenire nel *risk profile*, garantendo che l'attività di *internal audit* rimanga appropriata. Infine, è necessario che nella definizione dello scopo dell'attività di *internal audit* si considerino tutti sistemi di governo e di controllo, nonché delle *Key Control Functions*[235];

La seconda area considerata è rappresentata dalle *performance* in quanto l'attività di *internal audit* si sostanzia nella valutazione della progettazione e dell'efficacia operativa di *policy*, procedure e controlli stabiliti dall'impresa di assicurazione che includono (ma non si limitano solamente a questi): procedure e controlli attuati per garantire appropriati livelli di aderenza a leggi regolamenti e disposizioni delle autorità di vigilanza; *risk and control culture* dell'impresa di assicurazione; verifica del *framework* dell'attività di controllo garantisca affidabilità, efficienza e integrità dei sistemi e dei processi di gestione delle informazioni (compresa la pertinenza, accuratezza, completezza, disponibilità, riservatezza, integrità e completezza dei dati); verifica del *framework* dell'attività di

[233] ECIIA (Giugno 2019).
[234] ECIIA (Giugno 2019). Si ricorda inoltre che lo scopo di tale Istituto è quello di fornire una cultura etica per quanto riguarda la professione di internal auditor. Per approfondimenti si veda Institute of Internal Auditors IIA, *Introduction to the Code of Ethics*.
[235] ECIIA (Giugno 2019). Le key control function fanno riferimento al risk management, funzione attuariale e alla compliance.

controllo circa la modellizzazione e la gestione del capitale e dei rischi di liquidità dell'impresa di assicurazione, nonché dei mezzi di verifica delle responsabilità dell'organizzazione;

Infine, la terza area è quella del *reporting* perché al fine di garantire un dialogo adeguato con il comitato di *internal audit* e con gli altri *stakeholders*, devono essere considerati e discussi i seguenti punti (elementi che permettono di svolgere una congrua attività di *reporting*)[236]:

- *Reporting sulla pianificazione*. viene indicato lo scopo della funzione di *internal audit*, una valutazione del *risk and control environment* in cui opera la funzione di *internal audit* e un riassunto del *plan of work* proposto e delle risorse necessarie per attuarlo;
- *Reporting sui risultati*. Viene effettuato un riepilogo delle segnalazioni pubblicate nel periodo in corso di revisione e valutazione per ogni report prodotto. Verranno comunicati inoltre le risultanze dell'attività di *internal audit* effettuate nel periodo di riferimento;
- *Reporting sulle soluzioni adottate*. In questa sezione vengono indicati tutti i *Management action plans* in risposta ai *reports* prodotti dall'attività di *audit* che non sono stati ricevuti o che non sono considerati appropriati, un riepilogo circa le questioni evidenziate dall'attività di *audit* per le quali il *management* non ha proposto alcuna soluzione e che continuano a persistere e infine un riepilogo circa le criticità evidenziate e non ancora risolte per le quali era stata proposta una soluzione ma che non è stata implementata entro il termine stabilito;
- *Reporting sulle opinioni generali*. Almeno una volta all'anno è necessaria una valutazione da parte del responsabile della funzione di *internal audit* circa l'efficienza dell'attività di governance, di definizione dei rischi e dell'attività di controllo;
- *Reporting sulle risorse*. In questa sezione vengono riepilogate le risorse utilizzate dalla funzione di *internal audit* confrontandole con il *budget* inizialmente stabilito. Il responsabile della funzione di *internal audit* almeno una volta all'anno deve fornire informazioni circa l'adeguatezza di tali risorse. Annualmente devono essere confermate l'indipendenza e l'oggettività dello *staff* appartenente alla funzione di *internal audit* e ne dovranno essere riepilogate competenze e abilità.

All'interno del sistema dei controlli interni, grande importanza è attribuita all'attuario il quale, tramite l'acquisizione nel tempo di esperienza, progettualità e governance, ha permesso all'approccio attuariale di non essere più circoscritto esclusivamente alla fase di calcolo, bensì di essere considerato come una metodologia di percezione dei rischi e come metodo per affrontare l'incertezza grazie

[236] ECIIA (Giugno 2019).

all'ausilio di idonei strumenti di natura quantitativa[237]. Gli attuari sono esperti la cui attività all'interno delle imprese di assicurazione riguarda numerosi aspetti come il calcolo delle tariffe, degli accantonamenti a riserve tecniche e più in generale alla valutazione dei rischi[238]. Grazie all'analisi quantitativa svolta dagli attuari è possibile determinare l'impatto di ogni attività generatrice di rischio così da analizzare le migliori soluzioni in termini di contenimento, trasferimento o di eliminazione del rischio mediante strategie di gestione attiva o passiva[239]: l'attuario non è quindi un semplice "calcolatore", bensì un gestore di rischi che si avvale certamente di un approccio quantitativo, ma anche di un approccio qualitativo (che discende dalle acquisite capacità di managerialità e progettualità)[240].

Si può quindi notare una crescente proattività dell'attuario che lo vede sempre più impegnato nella gestione e nella governance del rischio all'interno delle imprese di assicurazioni. La Direttiva *Solvency II* attribuisce all'attuario, mediante le disposizioni di cui all'art. 48, il compito primario di "formazione delle riserve". Tale compito consiste nel coordinare il calcolo delle riserve[241], garantire l'adeguatezza di metodologie, ipotesi e modelli utilizzati per il calcolo delle stesse[242], valutare la qualità dei dati raccolti[243] e confrontare le stime con i dati tratti dall'esperienza[244], ma la stessa Direttiva *Solvency II* stabilisce inoltre che la funzione attuariale «contribuisca ad applicare in modo efficace il sistema di gestione dei rischi […], in particolare rispetto alla modellizzazione dei rischi sottesa al calcolo dei requisiti patrimoniali […] e rispetto alla valutazione di cui all'articolo 45 [procedura ORSA] »[245].

Sebbene la funzione attuariale abbia da sempre riguardato primariamente le attività operative dell'impresa di assicurazione (quali ad esempio design dei prodotti, marketing, pricing, investimenti e calcolo delle riserve tecniche), lo IAIS riconosce ora nel proprio *Standard Insurance Core Principles* (*ICP*) la funzione attuariale come una delle 4 funzioni di controllo[246]. Si riconosce perciò

[237] ANRA (Settembre 2017).
[238] Agalliu (2015) per insurancetrade.it.
[239] ANRA (Settembre 2017). Tra le strategie di gestione attiva ANRA annovera gli obiettivi aziendali, definizione e implementazione di presidi e diversificazione dei rischi, mentre cita tra le strategie passive l'adozione di strumenti finanziari/assicurativi di trasferimento del rischio e la cessione in outsourcing di funzioni/attività.
[240] Agalliu (2015) per insurancetrade.it.
[241] Art. 48 lettera a Direttiva Solvency 2.
[242] Art. 48 lettera b Direttiva Solvency 2.
[243] Art. 48 lettera c Direttiva Solvency 2.
[244] Art. 48 lettera d Direttiva Solvency 2.
[245] Art. 48 lettera i Direttiva Solvency 2.
[246] IAIS, ICP 8.2.1 «Quale parte di un sistema dei controlli interni e di gestione dei rischi, le imprese di assicurazione si dotano di alcune funzioni di controllo incluse risk management, compliance, funzione attuariale e internal audit". L'ICP 8.5 continua poi affermando che sia necessaria la presenza di "[…] Una efficace funzione attuariale in grado di valutare e fornire consulenza all'impresa di assicurazione circa, come minimo, le riserve tecniche, i premi e le attività di pricing e la compliance alle norme statali e ai regolamenti».

che la funzione attuariale, essendo parte delle funzioni di controllo, si adatta alla letteratura in materia di risk management individuando le cosiddette "tre linee di difesa del *risk management*"[247]:

- Prima linea di difesa*, "operations"*. Gli attuari sono presenti in tutto il ciclo assicurativo;
- Seconda linea di difesa*, "risk oversight"*. Gli attuari sono coinvolti nel sistema di gestione dei rischi (ad esempio *risk management* e *compliance*);
- Terza linea di difesa*, "indipendenza delle operazioni"*. Gli attuari sono coinvolti anche nelle funzioni di *internal* ed *external audit*.

Grazie all'esame circa l'evoluzione della figura dell'attuario, *l'International Actuarial Association* (*IAA*) ha individuato alcuni aspetti chiave che caratterizzano il ruolo dell'attuario[248]: ci si concentra maggiormente sul ruolo di *oversight* della funzione attuariale per l'implementazione di un efficace *risk management* notando che gli attuari non si limitano alla supervisione del rischio (ovvero, seconda linea di difesa), ma essi sono attivi in alcune e/o in tutte le tre linee di difesa; si sottolinea poi come un'indipendente *oversight* del rischio da parte della funzione attuariale sia importante per *board*, *senior management* e *supervisors* grazie alla prospettiva unica fornita dagli attuari permettendo inoltre una supervisione meno invasiva; la funzione attuariale apporta contributi materiali al processo di *risk management* e deve poter operare in modo chiaro trasparente e in modo efficiente all'interno di un'impresa di assicurazione. Questo permette di ottenere benefici sia per il management interno sia per gli *stakeholder* esterni e anche per le autorità di vigilanza.

IAA sottolinea poi la stretta correlazione tra l'attività svolta dall'attuario e l'attività svolta dal *Chief Risk Officer* (*CRO*) individuando due casi particolari: in un primo caso può risultare conveniente unire in un'unica posizione i due ruoli in quanto la *seniority* del CRO permetterebbe di comunicare direttamente con il CEO e ciò rappresenta un vero punto di forza per quanto concerne la prima linea di difesa. In un secondo caso risulta invece più conveniente mantenere separati i due ruoli affidando al responsabile della funzione attuariale (definito dall'IAA come *Actuarial Function Head*, AFH) il compito di *actuarial oversight*, lasciando invece al CRO il ruolo di responsabile della funzione di *risk management*. Questo secondo approccio permette di creare un team efficiente ma si evidenzia che tale impianto può funzionare solamente se entrambi ricoprono posizioni *senior* (che permettono ad esempio di fare rapporto direttamente al CEO)[249].

[247] Wason (2015) per IAA Risk Book Governance Management and Regulation of Insurance Operations capitolo 2; Actuarial Association of Europe (AAE, Giugno 2016).
[248] Wason (2015).
[249] Wason (2015).

3. CHIEF RISK OFFICER (CRO)

Con l'affermarsi del processo di ERM come metodo più diffuso per il governo e la gestione del rischio, si osserva una sempre maggiore proattività delle imprese nei confronti del rischio cercando di anticipare, pianificare, costituire e utilizzare adeguate metodologie qualitative e quantitative nonché ricercare il dialogo tra tutte le *business unit* in ottemperanza alla "visione olistica" proposta dall'ERM.

In questo scenario è necessaria la presenza di un soggetto che sia preposto a capo della funzione di risk management e che coordini l'attività di gestione del rischio, compito che viene affidato al *Chief Risk Officer* (CRO). È necessario precisare come, a dispetto del nome, il *risk manager* (o CRO) non si occupi della gestione dei rischi aziendali, quanto piuttosto di coordinare il processo di analisi e gestione dei rischi svolto dai vari *manager* (i veri *risk-owner*) fornendo supporto metodologico, favorendo il dialogo e integrando le informazioni provenienti da tutti i livelli. Il CRO è perciò un professionista in grado di interagire con tutte le funzioni aziendali coniugando conoscenza del *business* e degli strumenti atti alla gestione del rischio[250].

Nonostante il ruolo del CRO sia una figura tradizionalmente associata all'attività assicurativa, si rileva come esso stia acquisendo una sempre maggiore importanza in tutte le organizzazioni e soprattutto nelle società di servizi finanziari, sia per il crescente utilizzo degli strumenti finanziari da parte di altre imprese sia a causa della crisi finanziaria del 2008 che ha dimostrato la necessità di una maggiore attenzione verso la gestione del rischio[251]. Fraser e Simkins (2010) suddividono i ruoli che un CRO può rivestire in 2 macrocategorie, ovvero i ruoli afferenti alla *funzione di compliance e di controllo* e quelli che riguardano il *ruolo strategico di "business partner"*. Gli stessi autori individuano i seguenti ruoli:

1) *Compliance Champion*. Svolgere il ruolo di *compliance champion* per un CRO implica la difesa della compliance dalle pressanti richieste degli *stakeholders* nonché la ricerca di un costante adeguamento alla nuova regolamentazione e i nuovi standards che incidono su struttura e ruoli delle funzioni di *risk management*. Molti CRO costituiscono un *risk policy framework* indicante quali rischi debbano essere affrontati e da chi. In primo luogo, vengono stabiliti i limiti all'assunzione di rischi ritenuti accettabili garantendo inoltre l'appropriatezza di norme e controlli in atto[252]. I CROs rappresentano il punto di congiunzione tra il *controllo del rischio* e il *risk taking* in quanto «il CRO non è necessariamente responsabile per ogni tipologia di rischio ma deve assicurare che ogni *risk-*

[250] Articolo apparso sul sito www.ilbroker.it (novembre 2015).
[251] ANRA (aprile 2016).
[252] Fraser e Simkins (2010).

type owner utilizzi standard appropriati»[253]. In secondo luogo, il *risk policy framework* richiede una comprensione di tutti i rischi che l'impresa si trova a dover affrontare ricordando che lo spettro di rischi individuato cambia nel tempo. Infine, il *risk policy framework* fornisce uno strumento nonché l'autorità al CRO per sorvegliare l'implementazione del processo di gestione del rischio.

2) *Modeling Expert*. Il CRO riveste un ruolo fondamentale anche per quanto riguarda la selezione di personale, processi e sistemi per misurare e controllare i rischi e inoltre la varietà di strumenti, *risk models* e di sistemi di informazione, richiede che esso sia in grado di svolgere un ruolo di *Modeling expert*. In particolare, vi sono due linee di pensiero circa l'utilizzo dei *risk models*[254]:

- Scetticismo quantitativo. Alcuni CRO ritengono che i *risk models* possano essere un valido strumento solamente per una ristretta cerchia di rischi, ovvero quelli che possono essere statisticamente analizzati ritenendo quindi che l'attività di *risk modeling* non sia sufficientemente accurata per produrre un *risk profile* oggettivo ma sia utile solamente per analizzare il *trend* sottostante del rischio in esame.
- Entusiasmo quantitativo. Al contrario dei precedenti, alcuni CRO sostengono invece che il *risk modeling* sia uno strumento utile per il processo decisionale e per la pianificazione strategica.

3) *Strategic Controller*. La sempre maggiore importanza data alla visione aggregata dei rischi fa sì che il CRO possa rivestire anche un ruolo di *Strategic Controller*: tale ruolo presuppone che l'impresa abbia costituito un modello di rischio aggregato che le permetta di operare una gestione *risk-adjusted*. Il CRO che svolge questa mansione verifica che vi sia una stretta integrazione tra rischi e misurazioni delle performance garantendo inoltre che le metriche *risk-adjusted* siano affidabili. Si ricorda inoltre che la costruzione di un sistema di misurazione *risk-adjusted* è una questione "politica" e che ogni modifica apportata comporta una diversa allocazione delle risorse e di conseguenza il CRO dovrà riuscire a convincere i vertici della bontà di tale scelta perché «ogni misura di performance *risk-adjusted* non funziona automaticamente. Le misure di performance *risk-adjusted* devono essere fatte funzionare»[255].

4) *Strategic Advisor*. i CRO nello svolgimento di tale compito influenzano il *board* grazie alla loro capacità di comprensione dei rischi emergenti partecipando alle decisioni di alto livello in merito al rischio. I CRO che aspirano a tale ruolo sono solitamente degli "scettici quantitativi" non ritenendo sufficientemente accurati i modelli di rischio per una valutazione oggettiva del *risk profile*. Essi

[253] Fraser e Simkins (2010).
[254] Fraser e Simkins (2010).
[255] Fraser e Simkins (2010).

cercano di contribuire piuttosto attraverso l'unione delle proprie esperienze con la visione degli esperti dell'impresa al fine di aiutare i soggetti decisori a comprendere quali siano i rischi emergenti ed è perciò un ruolo che richiede che il CRO abbia sviluppato un'elevata credibilità altrimenti difficilmente potrà essere influente[256].

Mentre il ruolo del CRO legato alla *compliance* risulta ben definito e con poche possibili variazioni, di maggiore interesse risultano i due ruoli strategici. Il ruolo di *modeling expert* rappresenta la linea di confine tra ciò che può essere modellizzato e quindi stimato quantitativamente e ciò che invece richiede un giudizio qualitativo. Questa è anche la linea che separa i due ruoli strategici: mentre il ruolo di *strategic advisor* richiede una conoscenza approfondita del proprio business e di ciò che può andare storto implicando la necessità di un'elevata esperienza da parte del CRO, il ruolo di *strategic controller* attua una gestione del rischio basata maggiormente sull'utilizzo di *risk models*.

Il CRO deve pensare in modo strategico ampliando la propria visione, individuando le potenziali minacce anticipandole e influenzando i processi decisionali. Non è più sufficiente analizzare le minacce che tradizionalmente affliggono le società finanziarie come ad esempio il rischio di credito o di mercato, bensì è necessaria una visione più ampia che comprenda anche rischi reputazionali e di *compliance* ad esempio e solo attraverso il dialogo e la collaborazione con le altre funzioni operative tutto ciò sarà possibile[257]. Dal *Global Risk Management Survey* promosso da Delloite (2014) emerge come il 68% dei CRO intervistati comunichi direttamente al CEO e secondariamente al *board* direttivo «è una relazione che richiede la capacità di saper riportare ai vertici dell'organizzazione le proprie preoccupazioni dandogli il giusto peso, facendo comprendere il proprio pensiero ed esercitando, grazie a doti di *leadership*, un'influenza sui processi decisionali che conseguono alle discussioni»[258].

Come ha spiegato David Cookson (*recruitment consultant* per *Russell Reynolds Associates*) al *Wall Street Journal* (aprile 2016), il CRO dev'essere una figura in grado di mitigare i rischi ed essere al contempo un *leader* strategico, un punto di riferimento nonché portatore di idee innovative (vedi Fig. 3.5).

[256] Fraser e Simkins (2010).
[257] Stein (aprile 2016).
[258] Cit. ANRA (aprile 2016).

Fig. 3.5 – Differenze tra il ruolo di Strategic Controller e il ruolo di Strategic Advisor

	Strategic Controller	**Strategic Advisor**
Capacità di modeling *Obiettivo primario del risk modeling*	Misurare il profilo di rischio aggregato di prodotti e business line	Anticipare i cambiamenti nell'ambiente di rischio
Il ruolo del giudizio personale nel risk modeling	I modelli realizzati contengono il giudizio del soggetto che lo ha realizzato circa la relazione tra variabili complesse	I modelli realizzati sono deliberatamente semplici. Il gudizio personale viene utilizzato come strumento per aggiustare le implicazioni che tale modello comporta per riflettere complessità aggiuntive
Abilità strategiche *Estensione del controllo dei rischi*	Rischi quantificabili	Rischi quantificabili e non quantificabili
Essenza del ruolo di "business partner"	C'è un'integrazione del risk management con il planning and performance management Il CRO è sostenitore delle performance risk-adjusted	La funzione rischi ha la capacità di influenzare le decisioni strategiche e di spiegare ai line managers le implicazioni a lungo termine delle loro decisioni Il CRO è un esperto dirigente d'azienda
Attitudini alla modellizzazione	Entusiasmo quantitativo: grande enfasi circa l'utilità della modellizzazione e riconoscimento dell'utilità dei delle misure di performance risk-adjusted	Scetticismo quantitativo: i valori prodotti dall'analisi quantitativa vengono urilizzati come indicatori di trend. Si cerca di comprendere il vero profilo di rischio in base ai segnali provenienti dal trend. Le misure di performance risk-adjusted vengono utilizzate in modo marginale e come strumento di discussione

Fonte: nostra rielaborazione tabella Fraser e Simkins (2010).

4. IL RUOLO DEL CDA NEL PROCESSO DI ERM

Il *board* assume un'importanza cruciale per quanto concerne l'*oversight dei rischi*, svolto attraverso la pianificazione strategica e la supervisione dei compiti e dei contributi degli altri attori del Sistema dei Controlli Interni e di Gestione del Rischio (SCIGR)[259]. I compiti principali che

[259] ASSIREVI (Gennaio 2016). Gli attori del SICGR individuati da ASSIREVI nello stesso paper sono: Consiglio di Amministrazione, Collegio Sindacale, Comitato per il Controllo Interno, la Funzione di Internal Audit e il suo

spettano al *board* possono essere riassunti in tre punti[260]: definire le strategie per lo sviluppo e la realizzazione di un effettivo ed efficace processo di *risk management*; definire gli obiettivi di carattere generale in merito all'assunzione dei rischi; valutare l'efficacia del processo di *risk management* nonché dell'effettivo rispetto degli obiettivi generali menzionati al punto precedente.

Il mercato in cui oggi le imprese di assicurazione (e in generale tutte le imprese) si trovano ad operare, richiede che queste si dotino di un *board* proattivo nei confronti del *risk management*. Supervisionare la gestione del rischio è una responsabilità primaria del *board* e l'evoluzione del *business*, nonché l'evoluzione del panorama dei rischi, necessitano di un continuo miglioramento delle pratiche, in modo da definire un'efficace ed efficiente funzione di supervisione. Il *board* gioca inoltre un ruolo fondamentale nell'influenzare il processo di gestione e monitoraggio dei rischi ed è richiesto inoltre che venga valutata continuamente la struttura di *risk governance,* in quanto le imprese fronteggiano sempre nuovi rischi[261].

Secondo *l'International Association of Insurance Supervisors* (*IAIS*), il *board* è responsabile per la definizione della strategia e per la direzione generale, nonché per la supervisione della sua corretta gestione, lasciando invece la "gestione giornaliera" al *senior management*. Uno dei compiti del *board* consiste quindi nel fornire *leadership* direzione e *oversight* all'impresa di assicurazione attraverso un efficace sistema di *risk management* e un adeguata funzione di controlli interni, garantendo che i rischi principali siano correttamente fronteggiati e che le disposizioni di legge e i regolamenti siano correttamente applicati[262]. Secondo lo IAIS (2018), affinché il *board* rispetti quanto sopra indicato è necessario che stabilisca un business model sostenibile e una chiara strategia, definisca un chiaro e misurabile *risk appetite statement* e vigili sul suo rispetto ed infine che soddisfi gli obblighi normativi impostando una cultura che promuova una gestione prudente.

L'art. 5 del Regolamento 20 conferma tale impostazione attribuendo all'*organo amministrativo* la responsabilità ultima per quanto concerne il SICGR disponendo che ne debba garantire la completezza, funzionalità ed efficacia. Il *board* deve inoltre assicurare che il SICGR consenta l'identificazione e la valutazione anche prospettica di tutti i rischi che l'impresa di assicurazione deve fronteggiare garantendo «l'obiettivo della salvaguardia del patrimonio, anche in un'ottica di medio-lungo periodo»[263].

---

responsabile, il Dirigente Preposto alla redazione dei documenti contabili e infine gli altri ruoli e funzioni aziendali Con specifici compiti in tema di controllo interno e gestione dei rischi (come ad esempio compliance, risk management, comitati manageriali, eccetera).

[260] Floreani (2004).

[261] Deloitte per Wall Street Journal (Febbraio 2018).

[262] IAIS (Novembre 2018).

[263] Art. 5 comma 1 Regolamento ISVAP n. 20 del 26 Marzo 2008 modificato dal Regolamento IVASS n. 17 del 15 Aprile 2014.

Secondo quanto disposto dal Regolamento 20 l'organo amministrativo è chiamato a[264]:

- Approvare documenti di indirizzo, di carattere tecnico, che riguardano la gestione e il monitoraggio dei rischi a cui l'impresa di assicurazione è esposta, quali la politica di valutazione, anche prospettica, dei rischi recante i criteri e le metodologie da seguire per le valutazioni rilevanti[265]; il documento sulla propensione al rischio (*risk appetite*) e la tolleranza al rischio (*risk tolerance*) dell'impresa nell'ottica della salvaguardia del patrimonio[266]; la politica di gestione del rischio e le strategie per la relativa attuazione, anche in un'ottica di medio-lungo periodo[267]; le politiche relative alla sottoscrizione, alla riservazione, alla riassicurazione e alle altre tecniche di mitigazione del rischio nonché di gestione del rischio operativo[268].
- Adottare presidi di carattere organizzativo e amministrativo quali: l'approvazione di direttive in materia di SCI (che comprende la politica relativa alle funzioni di *risk management*, di *compliance*, di revisione interna e di assicurarne la coerenza con strategia e propensione al rischio)[269]; la definizione di un documento generale sull'organizzazione aziendale che riepiloga i compiti e le responsabilità degli organi sociali, dei comitati consiliari e delle funzioni di *risk management*, *compliance* e revisione interna, nonché dei flussi informativi e delle modalità di coordinamento tra tali soggetti[270]; l'adozione di una politica aziendale per la valutazione del possesso dei requisiti di idoneità alla carica (onorabilità e professionalità) da parte dei soggetti preposti alle funzioni di amministrazione, direzione e controllo, dei responsabili delle funzioni di controllo interno e di tutti coloro che svolgono funzioni "chiave" per la gestione dell'impresa[271]; verifica periodica la presenza di alcune competenze tecniche e legali all'interno dell'organo ministrativo al fine di assicurare la presenza di soggetti competenti in materia attuariale e di gestione dei rischi e degli investimenti[272].

[264] La seguente classificazione è ad opera di Febbi e Bobbo (2016) i quali hanno riassunto in due macrocategorie i punti essenziali contenuti nell'art. 5 comma 2 del Regolamento 20. Sarà ns. cura indicare il corretto riferimento al Regolamento.
[265] Art. 5 comma 2 lettera e Regolamento 20.
[266] Art. 5 comma 2 lettera f Regolamento 20.
[267] Art. 5 comma 2 lettera g Regolamento 20.
[268] Art. 5 comma 2 lettera h Regolamento 20.
[269] Art. 5 comma 2 lettera d Regolamento 20.
[270] Art. 5 comma 2 lettere a, b, j Regolamento 20.
[271] Art. 5 comma 2 lettera c Regolamento 20.
[272] Art. 5 comma 2 lettera l Regolamento 20.

Nella Fig. 3.6 vengono evidenziati gli aspetti che caratterizzano l'attività del *board* in un contesto di *risk management* e che se adeguatamente sfruttate possono portare dei vantaggi, ma che in caso contrario comportano una serie di problematiche[273].

Fig. 3.6 – Aspetti chiave dell'attività del board nel risk management

Punti chiave	Aspetti positivi	Criticità
Competenze dei membri del board	Il board dev'essere composto da un appropriato numero di membri che ne garantisca un adeguato livello di competenza in relazione alla struttura di governance.	Il processo di selezione per i futuri membri e informale o non documentato
		Il board collettivamente non è competente
		Il board collettivamente non ha esperienza del settore finanziario e/o del settore assicurativo
		le competenze dei membri del board non si evolvono in relazione ai cambiamenti del settore assicurativo
Diversità di competenze dei membri del board	La diversità nella composizione del board può portare a numerosi vantaggi, ma si richiede comunque che ogni membro abbia delle competenze minime appropriate al settore assicurativo	Il board collettivamente non è in possesso delle competenze e/o delle capacità di comprensione che il settore assicurativo richiede
		Non vi è una sufficiente diversificazione dei membri del board
Allocazione di ruoli e responsabilità	Ruoli e responsabilità del board senior management e "soggetti chiave" nelle funzioni di controllo devono essere chiaramente definiti e deve essere promossa un'adeguata separazione tra la funzione di oversight e le responsabilità della gestione.	Inadeguata allocazione dei compiti
Deleghe a compiti e/o attività del board	Il board può delegare alcune attività o compiti ad altri soggetti o comitati garantendone l'indipendenza	Le deleghe sono informali o non documentate
		Esiste un documento di delega ma questo non viene monitorato o revisionato su base regolare

Fonte: elaborazione personale informazioni contenute in "Application Paper on the Composition and the Role of the Boardpaper" IAIS (Novembre 2018)

Si sottolinea infine come un adeguato sistema di governance del rischio necessiti di un approccio di *Risk Intelligent Governance* ovvero di un approccio che «non cerca di scoraggiare un appropriato *risk-taking*, bensì cerca di incorporare adeguate procedure di gestione dei rischi in tutte le attività svolte dall'impresa»[274]. vengono individuate una serie di azioni che contribuiscono alla formazione di un approccio intelligente al governo del rischio (fig. 3.7), cercando di dare una risposta

[273] IAIS (Novembre 2018).
[274] Deloitte (2009).

alle seguenti domande[275]: Qual è il ruolo che può svolgere il *board* per definire il tono (*set the tone*) e supervisionare il processo di *risk management* verificando che esso sia attuato nel perseguimento di tutti gli obiettivi aziendali; Cos'è necessario affinché il *risk management* non sia considerato come una componente separata o *standalone*, bensì come una componente che si inserisce in ogni decisione presa dal board (vedi Fig. 3.7).

Fig. 3.7 – il ruolo del board nella Risk Intelligent governance

Definire il ruolo di risk overisght del board	Un efficace processo di supervisione del rischio aiuta il board a determinare se l'impresa adotta un sistema per identificare, valutare, dare priorità, e gestire i rischi e per fare ciò è necessario individuare chiaramente i ruoli e le responsabilità del board. Il Borgia può incoraggiare e supportare l'evoluzione dei programmi di gestione del rischio stabilendo obiettivi, ruoli, attività e metriche.
Favorire una Risk Intelligent culture	Una risk Intelligent culture riflette la generale consapevolezza, l'attitudine e il comportamento nei confronti del rischio dei soggetti impiegati nell'attività di impresa. È un key indicator di come policies e le pratiche sono state adottate, copre ogni area dell'impresa, influenza determinati comportamenti attraverso incentivi sistemi di gestione e norme comportamentali e infine aiuta a raggiungere gli obiettivi strategici.
Comprendere e approvare un adeguato risk appetite	Il concetto di risk appetite può essere in alcuni casi più quantitativo o in altri più qualitativo, ma In ogni caso valutare e approvare un appropriato livello di risk appetite e una responsabilità del board. esso rappresenta inoltre un importante meccanismo per collegare i programmi di gestione del rischio alla strategia dell'impresa eh si richiede perciò che il board consideri il risk appetite in ogni decisione importante.
Aiutare il management ad incorporare lo strategic risk thinking nella strategia	Un ruolo di primaria importanza per il board consiste nel consigliare al management come sviluppare una strategia che allinei la mission aziendale con la visione a breve e a medio-lungo termine degli stakeholders.
Valutare la "maturità" del processo di governance del rischio	È possibile valutare il livello di maturità delle abilità di risk management e del processo di risk governance da parte del board al fine di comprendere il livello di risk intelligence. Non sono stabilite specifiche soglie da raggiungere, ma ogni impresa deve raggiungere il proprio livello di maturità e ciò dipende dalle capacità di un'impresa nella gestione del proprio risk profile.

Fonte: elaborazione personale informazioni contenute in "Risk Intelligent governance Lessons from state-of-the-art board practices" Deloitte (2014)

[275] Deloitte (2014).

BIBLIOGRAFIA

Akerlof G. A., *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, The Quarterly Journal of Economics, Vol. 84, No. 3, Oxford University Press, Agosto 1970.

Arrow K. J., *Information And Economic Behavior*, Cambridge Harvard University, 1973.

Arrow K. J., *The organization of Economic Activity*, Paper pubblicato dal Joint Economic Committee of Congress, 1969.

Associazione Italiana Revisori Contabili (ASSIREVI), *L'esercizio del risk oversight da parte del consiglio di amministrazione*, Gennaio 2016.

Bellucci A., *Strategia, gestione del rischio e creazione di valore nelle imprese assicurative*, Torino, Giappichelli Editore, 2014.

Caggiola N., Cerrato S., Grosso P. et alii, *Avoid, Transfer, Retain: Aspetti giuridici dell'enterprise risk management e diritto delle assicurazioni*, Torino Giappichelli Editore, 2016.

Cappiello A., *L'attività assicurativa. Regole, gestione, business models*, Franco Angeli, 2018.

Chapman Robert J., *Simple tools and techniques for Enterprise Risk Management*, John Wiley & Sons, 2006.

Committee of Sponsoring Organizations of the Treadway Commission, *La gestione del rischio aziendale ERM enterprise risk management modello di riferimento e alcune tecniche applicative*, Edizione Italiana a cura di Associazione Italiana Internal Auditors e PricewaterhouseCoopers, Il Sole 24 Ore, 2006.

Damodaran A., Roggi O., *Elementi di finanza aziendale e risk management: La gestione d'impresa tra valore e rischio*, Maggioli Editore, 2016.

De Lorenzi V., *Contratto di assicurazione: Disciplina giuridica e analisi economica*, Cedam, 2008.

Deloitte, *Risk appetite in the financial services industry: A requisite for risk management today*, 2014.

Dittmeier C., *La governance dei rischi: un riferimento per gli organi e le funzioni di governo e controllo*, Milano, Egea, 2015.

Donati A., Putzolu G. V., *Manuale di diritto delle assicurazioni*, Roma, Giuffrè Francis Lefebvre, 2019.

Dowd K., *Beyond Value at Risk the new science of risk management*, John Wiley & Sons, 1998.

Dr. Curtis P., Carey M, Deloitte & Touche LLP, *Risk Assessment in practice*, Ricerca commissionata da CoSO, 2012.

Finkelstein A. et alii, *Moral hazard in health insurance*, New York, Columbia University Press, 2015.

Floreani A., *Enterprise Risk Management: I rischi aziendali e il processo di risk management*, Università Cattolica, 2004.

Fraser J. R., Simkins B. J., *Business Horizons Vol. 59, Issue 6, capitolo "The challenges of and solutions for implementing enterprise risk management"*, pag. 689-698, Novembre-Dicembre 2016.

Fraser J. R., Simkins B. J., *Enterprise Risk Management: Today's leading research and best practices for tomorrow's executive*, Kolb Series in Finance, 2010.

Frigo M. L., *Performance Measures That Drive the First Tenet of Business Strategy*,Strategic Finance Magazine, Settembre 2003.

Frigo M. L., *Understanding Your Organization's Genuine Assets*, Strategic Finance Magazine, Febbraio 2002.

Frigo M. L., Litman J., *Driven: Business Strategy, Human Actions and the Creation of Wealth*, 2008.

Frigo M. L., Litman J., *What Is Return Driven Strategy?* Strategic Finance Magazine, Febbraio 2002.

Gardenal G., Rigoni U., *Finanza comportamentale e gestione del risparmio*, Torino, Giappichelli Editore, 2016.

Gasparri G., *I controlli interni nelle società quotate. Gli assetti della disciplina italiana e i problemi aperti*, Quaderni Giuridici CONSOB, Settembre 2013.

Hazan M., Taurini S., *Assicurazioni private*, Wolters Kluwer, 2015.

Hun S., *The Economics of Risk and Insurance*, John Wiley & Sons, 2010.

International Association of Insurance Supervisors (IAIS), *Application Paper on the Composition and the Role of the Board*, Novembre 2018.

Knight, Petty, *Philosophies of risk, shareholder value and the CEO, in Mastering Risk Volume 1: Concepts*, James Pickford, 2001.

Koller M, *Life insurance risk management essentials*, Springer, 2011.

Kunreuther H. C., Pauly M. V., McMorrow S., *Insurance and Behavioral Economics: Improving Decisions in the Most Misunderstood Industry*, USA, Cambridge University Press, 2013.

Linsley P., Shrives P., Wieczorek-Kosmala M., *Multiple Perspectives in Risk and Risk Management, capitolo "Directors' Duties and Risk Governance"* di Beretta S., Springer, 2019.

Paci S., *Assicurazioni economia e gestione*, Milano, Egea, 2018.

Peter Bernstein, *Against the Gods the remarkable story of risk*, John Wiley & Sons, 1998.

Piccolo D., *Statistica per le decisioni*, Il Mulino, 2010.

Porter M. E., *Il vantaggio competitivo*, Einaudi, 2011.
Prandi P., *Il risk management teoria e pratica nel rispetto della normativa*, Franco Angeli, 2010.

Refsdal A. et alii, *Cyber-Risk Management*, Springer, 2015.

Santesso E., *Dispensa di Economia Aziendale*, Venezia, Cafoscarina, 2009.

Selleri L., *Viaggio nel mondo del rischio*, Youcanprint, 2015.

The Association of Accountants and Financial Professionals in Business (IMA), *Enterprise Risk Management: Tools and Techniques for Effective Implementation*, 2007

The Risk Management Association (RMA), *A Framework for Setting Risk Appetite*, 2013.

Trombetti G., *Solvency 2*, *Eurilink University Press*, 2017.

Vannucci L., *Teoria del rischio e tecniche attuariali contro i danni*, Bologna, Pitagora Editrice, 2010.

Venturelli F. *I processi di controllo interno sulla rendicontazione e la loro revisione: l'esperienza statunitense*, Cacucci Editore, 2007.

Weber C., *Insurance Linked Securities: The Role of the Banks*, Springer Gabler, 2011.

SITOGRAFIA

10th Global Conference of Actuaries, *risk faced by General Insurers*, reperibile presso http://www.dallasiia.org/PDF/090513_Lunch.pdf

Assinews.it, *Attuari sempre più risk manager*, 12 Luglio 2018, reperibile presso https://www.assinews.it/07/2018/attuari-sempre-piu-risk-manager/660054113/

Association of Insurance and Risk Management in Industry and Commerce (AIRMIC), ALARM, the public risk management association, Institute of Risk Management (IRM), *A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000*, 2010, reperibile presso https://www.ferma.eu/app/uploads/2011/10/a-structured-approach-to-erm.pdf

Associazione Italiana Financial Industry Risk Managers, *Il ruolo del RAF nella governance delle banche Associazione Italiana Financial Industry Risk Management*, Aprile 2017, reperibile presso http://www.ipeistituto.it/master/images/file-pdf/AIFIRM_PositionPaper9_Aprile2017.pdf

Associazione Nazionale dei Risk Manager e Responsabili Assicurazioni Aziendali (ANRA), *Nuovo coso ERM framework: le principali novità*, 25 Aprile 2018, reperibile presso https://www.anra.it/portal/contenuti/risk-management/1122/nuovo-coso-erm-framework-le-principali-novita

Associazione Nazionale dei Risk Manager e Responsabili Assicurazioni Aziendali (ANRA*), Cresce l'influenza del ruolo del chief risk officer*, 12 Aprile 2016, https://www.anra.it/portal/contenuti/risk-management/997/cresce-l-influenza-del-ruolo-del-chief-risk-officer

Associazione Nazionale dei Risk Manager e Responsabili Assicurazioni Aziendali (ANRA), *Il posizionamento del chief risk officer nella struttura aziendale*, 5 Febbraio 2016, reperibile presso https://www.anra.it/portal/contenuti/il-risk-manager/908/il-posizionamento-del-chief-risk-officer-nella-struttura-aziendale

Associazione Nazionale dei Risk Manager e Responsabili Assicurazioni Aziendali (ANRA), *Risk Management news numero 59*, Ottobre 2018, reperibile presso http://cdn-insurancetrade.procne.it/Notiziari/ANRA/RMNews_59/EXE_RMNews_59.pdf

Attisano F. D., Enterprise Risk Management: *Un profondo cambiamento nella gestione del rischio d'impresa*, 23 Ottobre 2019, reperibile presso http://www.riskcompliance.it/news/enterprise-risk-management-un-profondo-cambiamento-nella-gestione-del-rischio-dimpresa/

Chartered Accountants Australia and New Zeland, *Establish the context*, reperibile presso https://survey.charteredaccountantsanz.com/risk_management/small-firms/context.aspx

Chartered Accountants Australia and New Zeland, *Treat Risks*, reperibile presso https://survey.charteredaccountantsanz.com/risk_management/small-firms/treat.aspx

Crenca G., *L'attuario e l'Enterprise Risk Management*, ANRA.it, 6 Settembre 2017, reperibile presso https://www.anra.it/portal/contenuti/risk-management/1388/l-attuario-e-l-enterprise-riskmanagement

Deloitte, *Risk Oversight and the Role of the Board*, The Wall Street Journal, 10 Febbraio 2018, reperibile presso https://deloitte.wsj.com/riskandcompliance/2018/10/02/risk-oversight-and-the-role-of-the-board/

Deloitte, *Risk intelligent governance: A pratical guide for boards*, 2009, reperibile presso https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/Board%20of%20Directors/in-gc-risk-intelligent-governance-a-practical-guide-for-boards-noexp.pdf

D'Emilio S., *Il Risk Management e la nuova ISO 31000:2018: le linee guida*, 26 Settembre 2018, reperibile presso https://www.cybersecurity360.it/legal/il-risk-management-e-la-nuova-iso-310002018-le-linee-guida/

Direttiva 2009/138/ce del Parlamento Europeo e del Consiglio (Solvency II), 25 Novembre 2009, reperibile presso https://eurlex.europa.eu/legalcontent/IT/TXT/PDF/?uri=CELEX:32009L0138

Dr. Rittenberg L., Martens F., *Enterprise Risk Management Understanding and Communicating Risk Appetite*, Ricerca commissionata da CoSO 2012, reperibile presso https://www.coso.org/Documents/ERM-Understanding-and-Communicating-Risk-Appetite.pdf

Ernst & Young, *Risk Appetite: The strategic balancing Act*, Febbraio 2010, https://www.iia.nl/SiteFiles/EY-RiskAppetiteFeb2010.pdf

European Confedereation of Institutes of Internal Auditing (ECIIA), *Internal Audit in the insurance industry Guidance*, Giugno 2019, reperibile presso https://www.eciia.eu/wp-content/uploads/2019/06/ ECIIA-Display-8th-draft.pdf

Febbi S., Bobbo D., *L'evoluzione del sistema dei controlli interni delle imprese di assicurazione nel recepimento di Solvency II*, 1 Giugno 2016, reperibile presso http://www.dirittobancario.it/approfondimenti/assicurazioni/evoluzione-sistema-controlli-interni-imprese-assicurazione-nel-recepimento-solvency-ii

Financial Stability Board (FSB), *Principles for An Effective Risk Appetite Framework*, 2013, reperibile presso https://www.fsb.org/wp-content/uploads/r_131118.pdf

Hufeld F., Koijen R., Thimann C., *The invisible service: The economics, regulation, and systemic risk of insurance markets*, 30 Gennaio 2017, reperibile presso https://voxeu.org/article/economics-regulation-and-systemic-risk-insurance-markets

Institute of Risk Management, *Risk Appetite & Risk Tollerance Guidance paper*, Settembre 2011, reperibile presso https://www.iia.nl/SiteFiles/IRMGuidancePaper-Sep2011.pdf

Institute of Risk Management (IRM), *Risk appetite and tolerance Executive Summary*, reperibile presso https://www.theirm.org/what-we-say/thought-leadership/risk-appetite-and-tolerance/

Insurance Regulatory Authority (IRA), *Guideline on risk management and internal controls*, Febbraio 2013, reperibile presso, https://www.ira.go.ke/images/docs/Guideline_on_Risk_Management_and_Internal_Controls.pdf

International Association of Insurance Supervisors (IAIS), *Insurance Core Principles and ComFrame*, Novembre 2019, reperibile presso https://www.iaisweb.org/page/supervisory-material/insurance-core-principles-and-comframe//file/87202/iais-icps-and-comframe-adopted-in-november-2019

ISO/Guide 73:2009 Risk management – Vocabulary, reperibile presso https://www.iso.org/standard/44651.html

IVASS, *Solvency 2 la nuova regolamentazione prudenziale del settore assicurativo: Una guida semplificata*, Novembre 2016, reperibile presso https://www.ivass.it/pubblicazioni-e-statistiche/pubblicazioni/ altre-pubblicazioni/2016/guida-solvency-ii/Guida_Solvency_II.pdf

Jeges R., *Risk Appetite and ISO 31000*, 1 Luglio 2015, reperibile presso http://jeges.com.au/risk-appetite-and-iso-31000/

KPMG , *COSO Internal Control: Integrated Framework 2013*, 2013, reperibile presso https://assets.kpmg/content/dam/kpmg/pdf/2016/05/2750-New-COSO-2013-Framework-WHITEPAPER-V4.pdf

Manoukian J., *Risk Appetite and Risk Tolerance: What's the Difference?*, 29 Settembre 2019, reperibile presso https://enablon.com/blog/risk-appetite-and-risk-tolerance-whats-the-difference/

McIvor K., *Three drivers of epic risk culture Failure*, 29 Maggio 2019, reperibile presso https://www.willistowerswatson.com/en-US/Insights_/2019/05/3-drivers-epic-risk-culture-failures

National Audit Office, *Supporting innovation: Managing risk in government departments*, Londra, 2000, reperibile presso https://www.nao.org.uk/wp-content/uploads/2000/08/9900864.pdf

Organisation for Economic Cooperation and Development (OECD), *OECD Guidelines on insurer governance*, 2017, reperibile presso https://www.oecd.org/daf/fin/insurance/48071279.pdf

PricewaterhouseCoopers (PWC), *Board oversight of risk Defining risk appetite in plain English, Maggio 2014*, reperibile presso, http://www.ceolearningnetwork.com/_assets/library/2014/08/Defining-Risk-Appetite.pdf

PricewaterhouseCoopers (PWC), *COSO's Updated Internal Control Integrated Framework*, 2013, reperibile presso, https://www.actuariesindia.org/downloads/gcadata/10thGCA/Risks%20faced%20by%20Gen%20Insurers_Neha%20Gupta.pdf

PricewaterhouseCoopers (PWC), *Internal Audit Expect More: 2019 Internal Audit planning: Insurance and asset and wealth management*, Settembre 2018, reperibile presso https://www.pwc.co.uk/audit-assurance/assets/pdf/pwc_2019_ia_planning_ins_and_awm.pdf

Risk Management LTD, *Risk appetite and criteria compared, considered and developed*, Settembre 2015, reperibile presso https://www.riskmgmt.co.nz/fileadmin/documents/Risk_appetite.pdf

Savoca F., *Nuove professioni: il chief risk officer*, 11 Agosto 2015, reperibile presso https://ilbroker.it/2015/11/08/nuove-professioni-il-chief-risk-officer/

Steins M. L., *Chief Risk Officers Are Taking on a Broader Role*, The Wall Street Journal, 1 Aprile 2016, reperibile presso https://blogs.wsj.com/riskandcompliance/2016/04/01/chief-risk-officers-are-taking-on-a-broader-role/

The Institute of Internal Auditors, *Code of ethics*, reperibile presso https://global.theiia.org/standards-guidance/mandatory-guidance/ Pages/Code-of-Ethics.aspx

Walker P. L., Shenkir W. G., Barton T. L., *Establish a risk challenge culture*, Strategic Finance Magazine, 1 Aprile 2015, reperibile presso https://sfmagazine.com/post-entry/april-2015-establish-a-risk-challenge-culture/

Walker P. L., Shenkir W. G., Barton T.L., A risk challenge culture, Association of Accountants and Financial Professionals in business (ACCA_IMA), 2013, https://www.accaglobal.com/content/dam/acca/global/PDF-technical/corporate-governance/pol-tp-arcc.pdf

Wason S., *IIA risk book, capitolo 2 "actuarial function"*, 21 Agosto 2015, reperibile presso https://www.actuaries.org/LIBRARY/Papers/RiskBookChapters/Ch2_ActuarialFunction_2015-08-21.pdf

Williams C*., ISO 31000 vs. CoSO: Comparing and contrasting the world's leading risk management standards*, 8 Aprile 2019, reperibile presso https://www.erminsightsbycarol.com/iso-31000-vs-coso/

Williams C., *Five effective methods to identify risk in your organization*, reperibile presso https://www.erminsightsbycarol.com/

Williams C., *Enterprise risk analysis: Prioritizing risks for maximum benefit to the organization*, 23 Luglio 2018, reperibile presso https://www.erminsightsbycarol.com/enterprise-risk-assessment/

Williams C., *Enterprise risk assessment: Transforming risk information into action*, 23 Aprile 2018, https://www.erminsigh tsbycarol.com/enterprise-risk-assessment/

Wood A., *Changing risk culture and the dynamic CRO*, 15 Aprile 2019, reperibile presso https://www.willistowerswatson.com/en-US/Insights/2019/04/changing-risk-culture-dynamic-cro