
aracne

Classificazione Decimale Dewey

— 658.155 (23.) GESTIONE FINANZIARIA DELLE ENTRATE E DELLE USCITE

Thema

— Soggetto: KJM. Management e tecniche gestionali

— Qualificatori: 4CT. Per l'istruzione superiore/terziaria/universitaria

MIRCO CARLONI
SACHA BALSAMO TAGNANI
NICOLÒ PIERINI
CESARE MORLINO

RISK MANAGEMENT E INTERNAL AUDIT

LA SAPIENTE SCELTA DI COME GESTIRE I RISCHI D'IMPRESA E BENEFICIARE DEI RELATIVI CONTROLLI INTERNI

aracne



©

ISBN
979–12–218–3046–0

PRIMA EDIZIONE
ROMA 6 NOVEMBRE 2026

INDICE

7 *Prefazione*

11 Introduzione

19 Capitolo 1
Storia ed evoluzione della disciplina dell'Enterprise risk management

1.1. La nascita dell'Enterprise risk management: una disciplina in continuo divenire, 19 – 1.2. Il concetto di rischio: definizioni e rilevanza per l'economia dell'impresa, 21 – 1.3. Le origini della disciplina: la funzione "sicurezza" di Henri Fayol (1916) e la distinzione tra rischio e incertezza di Frank Knight (1921), 23 – 1.4. Il dibattito del secondo Novecento: dall'*irrelevant principle* di Modigliani e Miller (1958) al contributo di Mehr e Hedges (anni '60), 26 – 1.5. Dalla gestione assicurativa dei rischi puri alla crisi petrolifera del 1973: l'emersione della distinzione tra rischi puri e rischi speculativi, 28 – 1.6. Gli anni '90 e il risk management *business oriented*: dalla gestione per "silos" alla visione integrata, 31 – 1.7. L'affermazione dell'approccio sistemico: l'Enterprise risk management e il concetto di *risk appetite*, 34 – 1.8. La formalizzazione della disciplina: dal framework CoSO (2004) allo standard ISO 31000 (2009-2018). Rinvio, 36 – 1.9. L'integrazione dell'ERM nella corporate governance e la creazione di valore per gli azionisti e gli stakeholder, 38.

41 Capitolo II
Le categorie di rischio ed i principali approcci e modelli di gestione

2.1. La classificazione dei rischi d'impresa: rischi strategici, operativi e gestionali e le principali categorie di rischio, 41 – 2.2. Il rischio operativo: dalla definizione degli anni '70 alla normativa di Basilea II – rischi operativi puri e rischi operativi speculativi, 44 – 2.3. La *Business Impact Analysis* (BIA) e i *Key Risk Indicators* (KRI) quali strumenti di individuazione e monitoraggio dei rischi operativi, 46 – 2.4. L'Operational Risk Management: l'approccio tradizionale e quello moderno a confronto, 48 – 2.5. Gli eventi estremi e imprevedibili: la teoria del *Cigno Nero* di Taleb e le strategie di resilienza e antifragilità, 51 – 2.6. Le nuove frontiere del rischio tecnologico: la sicurezza informatica, la protezione dei dati personali e l'intelligenza artificiale, 54 – 2.7. Il rischio legale e di non conformità: la responsabilità amministrativa degli enti ex D.Lgs. 231/2001 e il modello di organizzazione, gestione e controllo, 59 – 2.8. Il processo di risk management e i principali approcci di gestione: *process oriented* e *business oriented*, 67 – 2.9. I modelli di gestione in ambito ERM: il *Risk Management Cycle*, il framework CoSO e la serie ISO 31000 – il raccordo con la ISO 9001 e la comparazione tra i framework, 69.

75 Capitolo III
Corporate governance e sistema dei controlli interni

3.1. La corporate governance: definizione, 75 – 3.2. Obiettivi e classificazione delle strutture di governance aziendale, 78 – 3.3. La corporate governance bancaria, 83 – 3.4. Il sistema dei controlli interni ("SCI"), 86 – 3.5. I controlli di secondo livello in ambito bancario, 93 – 3.6. L'evoluzione nel tempo della Funzione Compliance: le nuove sfide tra cui l'AI, 102 – 3.7. I controlli di terzo livello in ambito bancario, 106 – 3.8. La gestione integrata dei rischi e il *risk appetite framework*, 111 – 3.9. L'efficacia del sistema dei controlli: flussi informativi, anomalie e miglioramento continuo, 118.

127 Conclusioni

131 *Bibliografia*

PREFAZIONE

Il progetto nasce dalla volontà di rendere, in *primis* ai nostri studenti, ma vale per qualsiasi lettore incuriosito dall'ambito di ricerca, un testo semplice e di immediata percezione, di una materia, quella della gestione dei rischi e dei controlli interni d'impresa, che non è particolarmente approfondita in ambito universitario, trattandosi di una disciplina più conosciuta nell'ambito professionale (bancario e finanziario) rispetto a quello accademico puro.

La cattedra in *Risk Management & Internal Auditing* (d'ora in avanti anche "RMIA"), istituita nell'anno 2019, presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Urbino Carlo Bo, nasce da una idea del dott. Mirco Carloni e del dott. Ric. Sacha Balsamo Tagnani, entrambi ex studenti presso il medesimo Ateneo urbinate.

Nonostante si tratti di un corso a scelta "opzionale" si è sempre registrata una certa partecipazione in tutti gli anni accademici in cui si è tenuto il corso in RMIA. Gli studenti di tutti gli anni hanno prevalentemente apprezzato il taglio pratico e professionalizzante del corso, e non a caso alcuni di loro hanno intrapreso carriere in ambito *risk* e *compliance* all'interno di aziende operanti nel mondo finanziario o del credito.

Come abbiamo sempre affermato all'inizio dell'anno accademico

> questo corso ha l'obiettivo principale di manifestare negli studenti un certo grado di interesse verso la disciplina dei rischi d'impresa e della loro gestione, con anche un focus sui modelli e processi di maggior successo. Non da ultimo vi è l'idea che il sistema dei controlli interni aziendali, soprattutto nell'ambito del mercato bancario e finanziario sia interessante per gli studenti, soprattutto perché negli ultimi tempi vi è ampia domanda di professionisti esperti in tali materie.

Quello che, in altri termini, è sempre stato l'obiettivo del corso risiede nella volontà di fornire le basi per far sì che gli studenti possano "ragionare" su delle professioni che, in Italia ancora sono poco conosciute, soprattutto da chi decide di orientarsi verso gli studi di diritto o economia, ancora fortemente ancorati al concetto delle classiche professioni legali o commerciali.

Il mercato finanziario, oggi, richiede sempre più competenze specifiche orientate al mondo dei rischi e a quello dei controlli interni. Non è solo una tendenza insita nello specifico mercato di riferimento, ma la conoscenza e la strutturazione di funzioni a tale scopo dedicate sono richieste direttamente dal legislatore, sia quello europeo che quello nazionale. Basti aprire un sito *internet* a caso di una banca o di un intermediario finanziario qualsiasi per notare che le più frequenti posizioni ricercate riguardano l'ambito del Risk manager o del Compliance manager o dell'Auditor.

Oggi, la centralità delle Funzioni di controllo interno è molto maggiore rispetto a venti anni fa, questo lo si deve prevalentemente a due fattori: il primo è legato alla imponente legiferazione in ambito finanziario, assicurativo e bancario ma soprattutto di quello europeo, in materie del tutto nuove rispetto alle classiche (si pensi all'ambito della normativa di recente emanazione del DORA oppure del MiCAR o dell'AI ACT) leggi bancarie.

È in tale scenario che si colloca l'esigenza di innovare il nostro corso. Dopo quasi dieci anni dall'inizio del nostro progetto accademico avvertiamo la necessità (o meglio la forte esigenza) di sistematizzare in un unico testo tutto il lavoro di ricerca svolto in questi ultimi anni, mettendo a disposizione degli studenti del corso in RMIA un "manualetto"

pronto all'uso, nel quale sono prontamente riportate tutte le presentazioni utilizzate durante le lezioni degli anni precedenti (aggiornate ai tempi correnti), che possa stimolarli ad appassionarsi a questo ambito del sapere giuridico ed economico, che sempre più è ricercato dal mondo del lavoro.

INTRODUZIONE

Il testo affronta dapprima la disciplina dell'*Enterprise risk management* (anche "ERM"), ossia di quell'approccio strategico e olistico che le organizzazioni (sia pubbliche che private) utilizzano per identificare, valutare e mitigare i rischi aziendali. Il suo principale obiettivo è proteggere il valore dell'azienda e supportare il *management* nel prendere decisioni informate in linea con gli obiettivi di *business*[1]. Si tratta di una disciplina relativamente giovane e in continuo divenire, che insegue il progresso economico e tecnologico e che, come si vedrà, ha tratto da ogni crisi l'occasione del proprio rinnovamento.

Il rischio rappresenta una condizione esistenziale ineliminabile di ogni azienda e può essere definito, in prima approssimazione, come il potenziale verificarsi di eventi che siano in contrasto con gli obiettivi che l'azienda si prefigge di realizzare[2]. Si tratta di un fenomeno intrinseco[3] al

(1) Cfr. per una prima analisi dell'ERM l'articolo apparso sul seguente link: *https://www.pwc.com/it/it/services/consulting/pwc-enterprise-risk-management.html*.

(2) Potito L. (a cura di), *Economia Aziendale*, Giappichelli, Torino, p. 31

(3) La natura imprescindibile del rischio per il funzionamento del sistema aziendale è riconosciuta in modo concorde dalla dottrina. In merito, Zappa osserva che: «*Sebbene fattore perturbatore dell'attività economica, il rischio è l'elemento che forse caratterizza meglio l'azienda, al punto che, in assenza del rischio, l'attività aziendale non è neppure concepibile*». Zappa G., *Le produzioni nell'economia delle imprese*, Giuffrè, Milano 1956-1957. In maniera speculare, Dezzani considera il rischio come «*ineliminabile proiezione nel futuro di ogni sistema aziendale, qualunque sia l'oggetto che ne qualifica la funzione strumentale*», così ipotizzando che, in assenza di rischio, non si configura più l'opportunità di proseguire l'attività aziendale. Dezzani F., *Rischi e politiche d'impresa. Contenuto e relazioni*, Giuffrè, Milano 1971. Similmente, Bertini rileva che «*il rischio, la*

concetto di azienda, di natura sistematica[4], che assume carattere dinamico in funzione delle manifestazioni di vita della stessa e che influenza le condizioni di equilibrio economico, finanziario e patrimoniale.

Di definizioni se ne trovano molteplici. La Treccani, ad esempio, definisce il rischio come *l'eventualità di subire un danno connessa a circostanze più o meno prevedibili*[5]. In una prospettiva aziendalistica, tuttavia, il rischio può essere inteso come la possibilità che accada qualcosa che impatti sugli obiettivi e che possa determinare – negativamente ma anche positivamente – una perdita o un guadagno: accezione, questa, accolta dagli standard internazionali più recenti, che definiscono il rischio come «effetto dell'incertezza sugli obiettivi».

In ambito internazionale, la gestione dei rischi è nota come *risk management*. Il *risk management*, nella sua accezione moderna, è inteso come un processo di identificazione e valutazione dei rischi cui l'azienda è esposta, al fine di decidere la migliore strategia di trattamento degli stessi sulla base di adeguate valutazioni, e comprende un insieme di azioni intraprese nel tentativo di modificare il livello di rischio proveniente dalle principali aree di business[6]. Tradizionalmente, le attività di *risk management* erano condotte in maniera isolata da parte della specifica funzione aziendale interessata, ossia secondo un orientamento definito *silo by silo*[7], senza avvalersi di una visione unitaria del profilo

---

cui durata è legata alla vita dell'azienda, cessa con la fine di questa». Bertini U., *Introduzione allo studio dei rischi nell'economia aziendale*, Cursi, Pisa 1969 (rist. Giuffrè, Milano 1987).

(4) Il primo studioso italiano che ha evidenziato la sistematicità dei rischi aziendali è Sassi, descrivendoli come «*un'assidua coordinazione che è atta a costituirli in sistema economico, al pari del complesso delle funzioni da cui essi sono espressi*», altresì specificando che «*la stretta connotazione simultanea e successiva dei rischi d'azienda (…) manifesta, in particolare, l'impossibilità di autonome presunzioni di quei fenomeni*». Sassi S., *Il sistema dei rischi d'impresa*, Vallardi, Milano 1940. Il carattere sistemico dei rischi è stato poi approfondito successivamente da Giannessi E., *Le aziende di produzione originaria*, vol. I, *Le aziende agricole*, Cursi, Pisa 1960.

(5) Cfr. dal vocabolario Treccani al seguente link: *https://www.treccani.it/vocabolario/rischio_res-af319d2b-e3b2-11eb-94e0-00271042e8d9/*.

(6) Dittmeier C., *Internal auditing. Chiave per la corporate governance*, Egea, Milano 2007 (2ª ed. 2011).

(7) Il silo-based approach al risk management è un approccio disaggregato alla gestione dei rischi, inizialmente adottato dalle istituzioni finanziarie e poi diffusosi anche nelle aziende non finanziarie. I limiti di tale approccio, principalmente riconducibili alle inefficienze derivanti dalla mancata coordinazione tra le diverse unità deputate alla gestione del rischio e, dunque, dall'assenza di una visione complessiva della rischiosità d'impresa sono stati riconosciuti dalla letteratura e dai practitioners.

di rischio dell'impresa: un'impostazione il cui superamento costituisce il tratto distintivo dell'ERM.

Come anche affermato da Bettanti e Lanati

> L'identificazione dell'esposizione ai rischi e del loro impatto sull'azienda porta a stabilire una gerarchia dei rischi individuati e a stabilire le priorità negli interventi, fornendo al gestore gli elementi necessari a stabilire le proprie linee d'intervento[8].

Una corretta mappatura dei rischi d'impresa può garantire all'imprenditore una maggiore produttività, riducendo di gran lunga le perdite e i conseguenti danni economici, non solo per l'impresa stessa, ma anche per gli azionisti e per i portatori di interesse in generale: il rischio è costoso per le imprese, ma la sua gestione consapevole crea valore.

Naturalmente, come si avrà modo di approfondire nel prosieguo, le categorie di rischio sono numerose e ognuna di esse risulta caratterizzata da differenti modalità di individuazione e gestione. In senso ampio, le tradizionali (e tipiche) categorie di rischio sono quelle "strategiche", quelle "operative" e quelle di "gestione".

I rischi strategici, come dice anche il termine stesso, riguardano la comprensione delle tendenze del mondo "esterno": le azioni degli altri *players* del mercato (competitori), l'evoluzione delle tecnologie (di ogni tipologia), le richieste del mercato (dei clienti) ricadono in quest'area, ossia in quella maggiormente collegata alle scelte imprenditoriali di lungo termine. I rischi operativi, prevalentemente di natura tecnico-operativa, sono quelli maggiormente conosciuti dall'impresa stessa, in quanto interni, e strettamente connessi allo svolgimento dell'attività ordinaria e tipica dell'impresa.

Infine, il rischio gestionale è quello più strettamente collegato alla corretta gestione dell'impresa ed è segnatamente interconnesso con la reputazione e con i danni che ne derivano. La reputazione è senz'altro un valore fondamentale per ogni azienda che operi in un mercato aperto al pubblico, e lo è ancor più oggi, nell'epoca dei *social media*: una buona reputazione è appunto fondamentale nei rapporti con i propri portatori

(8) A. Bettanti, A. Lanati, *ERM. Enterprise risk management. Nuovi orizzonti per la creazione di valore in azienda*, McGraw-Hill Education, Milano 2019, p. 7.

d'interesse, clienti, fornitori, finanziatori, azionisti, istituzioni statali[9].

Accanto a questa classificazione di fondo, il testo esamina le categorie di rischio che maggiormente interessano l'economia del corso: il rischio operativo, nelle sue declinazioni pure e speculative e con i relativi strumenti di individuazione, misurazione e monitoraggio; gli eventi estremi e imprevedibili; il rischio tecnologico; il rischio legale e di non conformità. È proprio dall'analisi del rischio tecnologico che emerge con maggiore nitidezza la chiave di lettura dell'intera opera. La digitalizzazione pressoché integrale dei processi aziendali ha trasformato la sicurezza informatica da questione tecnica, confinata nei reparti IT, a rischio d'impresa di primaria grandezza; e il legislatore europeo ha scelto di governare tale rischio non con prescrizioni tecniche rigide, bensì imponendo alle organizzazioni un vero e proprio sistema di controlli interni basato sul rischio.

Il Regolamento europeo sulla protezione dei dati (GDPR) ne offre l'esempio più compiuto: il principio di responsabilizzazione (*accountability*), la protezione dei dati, le misure di sicurezza adeguate al rischio e il loro collaudo periodico, la procedura di gestione delle violazioni dei dati personali, la valutazione d'impatto sulla protezione dei dati (DPIA) e la figura del Data Protection Officer (DPO) traducono in obblighi giuridici l'intera grammatica del *risk management* – valutazione del rischio, trattamento mediante misure adeguate, monitoraggio e riesame continui, documentabilità – e, quanto al DPO, i requisiti di indipendenza propri delle funzioni aziendali di controllo. La medesima impostazione si ritrova nel Regolamento (UE) 2024/1689 sull'intelligenza artificiale (AI Act), che estende l'approccio basato sul rischio a un rischio tecnologico di nuovo tipo: non più soltanto la violazione di un sistema o la sottrazione di un dato, ma la possibilità che lo stesso sistema, pur funzionando secondo le modalità per le quali è stato progettato, produca risultati errati, discriminatori o poco trasparenti, e che l'eccessivo affidamento sulla risposta della macchina riduca l'effettività del controllo umano. Analoga logica, di tipo premiale, connota la responsabilità amministrativa degli enti *ex* D.Lgs. 231/2001, nella quale tanto la responsabilità dell'ente quanto la sua esenzione ruotano attorno alla qualità dell'organizzazione e dei presidi di prevenzione.

(9) *Ibidem*.

Ne discende il filo conduttore che lega le due "anime" del corso in RMIA: la gestione del rischio non è un insieme di tecniche scollegato dall'apparato di norme che regola l'attività d'impresa, ma è sempre più spesso tradotta dal legislatore – europeo e nazionale – in obbligo giuridico, e trova la propria collocazione istituzionale nella corporate governance e nel sistema dei controlli interni (SCI). Partendo dal rischio e dalla sua corretta gestione, è dunque naturale passare alla "seconda" anima del corso, ossia all'ambito della corporate governance, attraverso il sistema dei controlli interni, sino alle funzioni di controllo di secondo e terzo livello in ambito bancario e finanziario.

Riassumendo, nel primo capitolo si ripercorrono la storia e l'evoluzione dell'ERM: dalle intuizioni di Fayol e di Knight, attraverso il dibattito del secondo Novecento, la crisi petrolifera del 1973 e i dissesti degli anni '80 e '90, sino all'affermazione dell'approccio sistemico e del concetto di *risk appetite*, alla formalizzazione della disciplina in modelli e standard e alla sua integrazione nella corporate governance. Nel secondo capitolo si affrontano le varie categorie di rischio: la classificazione in rischi strategici, operativi e gestionali; il rischio operativo, con la distinzione tra rischi puri e speculativi, gli strumenti della Business Impact Analysis (BIA) e dei Key Risk Indicators (KRI) e il confronto tra l'approccio tradizionale e quello moderno all'Operational Risk Management; gli eventi estremi e la teoria del "Cigno Nero" di Taleb; le nuove frontiere del rischio tecnologico – la sicurezza informatica, la protezione dei dati personali e l'intelligenza artificiale –; il rischio legale e di non conformità, con particolare riguardo alla responsabilità amministrativa degli enti ex D.Lgs. 231/2001 e al modello di organizzazione, gestione e controllo. Il capitolo si chiude con l'analisi del processo di gestione del rischio, dei due principali approcci del *process oriented* e del *business oriented* e dei tre modelli in ambito ERM: I) il Risk Management Cycle; II) il framework CoSO (*Committee of Sponsoring Organizations of the Treadway Commission*); III) la serie della normativa ISO 31000[10], con il raccordo con lo standard certificabile ISO 9001 e la comparazione tra i framework.

Nell'ultimo capitolo l'attenzione si sposta sulla corporate governance – nella sua definizione, nei suoi obiettivi e nei principali modelli, anche in prospettiva comparata – e, in particolare, sulla corporate governance

(10) *Op. cit.*, p. 69 e ss.