LUISS

Dipartimento di

Impresa e Management

Corso di Laurea Magistrale in Amministrazione Finanza e Controllo

Cattedra: Corporate Governance and Internal Auditing

Il fraud audit come strumento di prevenzione delle frodi aziendali: analisi dell'efficacia del sistema di controllo interno attraverso un caso empirico

Prof. Saverio Bozzolan

RELATORE

Prof. Simone Scettri

CORRELATORE

Alice Capaldi matr. 788421

CANDIDATO

Anno Accademico 2024/2025

INTRODUZIONE

Obiettivi della ricerca

Il presente lavoro di tesi si inserisce nell'ambito degli studi sui sistemi di prevenzione delle frodi aziendali, con particolare riferimento al contributo che il *fraud audit* può offrire in tale prospettiva. L'analisi della letteratura scientifica nazionale e internazionale ha permesso di delineare il quadro teorico e normativo di riferimento, ricostruendo l'evoluzione del ruolo del revisore nella gestione del rischio di frode nonché le principali pratiche operative consolidatesi nel tempo. Sono state altresì analizzate le metodologie di revisione più diffuse, con particolare riferimento all'approccio *top-down* e alle modalità di interazione con il management finalizzate all'individuazione delle aree a maggiore esposizione al rischio.

Su queste premesse si fonda il presente lavoro di tesi. La domanda di ricerca che ne ha orientato lo sviluppo riguarda la capacità del sistema di controllo interno di costituire un presidio realmente efficace nella prevenzione delle frodi aziendali, verificandone l'effettiva operatività e il grado di affidabilità mediante l'applicazione delle metodologie proprie del *fraud audit*. L'attenzione non si è quindi limitata alla capacità dei controlli di rilevare eventuali irregolarità a posteriori, ma si è concentrata soprattutto sulla loro funzione preventiva, ossia sulla possibilità che i presidi organizzativi e procedurali riducano in maniera sostanziale l'esposizione dell'impresa a fenomeni fraudolenti. Tale prospettiva ha costituito il filo conduttore dell'intero elaborato, orientando sia la ricostruzione teorica sia l'indagine empirica, che si è concretizzata nell'analisi di un'impresa reale assunta come caso di studio e oggetto di revisione durante l'esperienza di tirocinio curriculare presso la società di revisione EY.

Il lavoro è stato svolto a stretto contatto con il team di revisione di cui ho fatto parte, con il supporto dei colleghi senior e manager, e grazie alla collaborazione della società oggetto di analisi, che ha fornito documentazione rilevante e ha reso possibile l'approfondimento di aspetti operativi tramite colloqui diretti con i responsabili aziendali coinvolti nei processi di controllo. Questa esperienza ha consentito di osservare da vicino il funzionamento dei presidi interni, valutarne la coerenza rispetto ai rischi identificati e verificarne l'applicazione concreta nei diversi cicli aziendali. L'indagine ha permesso così

di coniugare l'approccio metodologico del fraud audit con la valutazione sostanziale dei controlli interni, al fine di comprenderne l'efficacia nella prevenzione delle frodi.

Metodologia di ricerca

Per garantire la solidità e la coerenza dell'analisi è stato adottato un percorso metodologico articolato, che ha combinato strumenti di indagine teorici ed empirici. L'approccio ha previsto, da un lato, un'analisi qualitativa di tipo descrittivo-analitico e, dall'altro, lo studio di un caso reale, così da integrare la riflessione accademica con l'osservazione diretta della prassi aziendale.

L'indagine è stata sviluppata in due fasi principali. La prima fase ha riguardato la costruzione del quadro teorico e normativo di riferimento, realizzata attraverso un'analisi documentale della letteratura scientifica nazionale e internazionale, e delle principali fonti normative in materia di fraud audit e sistemi di controllo interno. Tale analisi ha consentito di individuare i criteri metodologici e gli strumenti operativi più idonei alla valutazione dei sistemi di controllo finalizzati alla prevenzione delle frodi.

La seconda fase del lavoro ha avuto carattere empirico e si è concretizzata nell'esame di un'impresa reale assunta come caso di studio. L'indagine ha riguardato sia la dimensione documentale, attraverso l'analisi di policy, procedure, organigrammi, flussi informativi e report di controllo, sia la dimensione operativa, mediante interviste strutturate e semi-strutturate rivolte ai responsabili delle principali funzioni aziendali. Tale approccio ha consentito di integrare l'esame formale dei presidi di controllo con la valutazione della loro effettiva applicazione nei processi aziendali.

L'analisi ha seguito un approccio *top down*: dalla valutazione del disegno complessivo del sistema di controllo interno si è passati all'approfondimento dei singoli processi e cicli aziendali maggiormente esposti al rischio di frode. Particolare attenzione è stata dedicata alla verifica della corrispondenza tra procedure formalmente adottate e prassi operative effettivamente in uso, nonché all'efficacia delle attività di monitoraggio e follow-up. La triangolazione delle fonti — letteratura, documentazione aziendale e confronti diretti con i referenti aziendali — ha permesso di ottenere una visione completa

e affidabile, riducendo al minimo il rischio di distorsioni interpretative e garantendo la solidità delle evidenze raccolte.

Il lavoro si articola in tre capitoli. Il primo capitolo approfondisce la letteratura scientifica e le principali fonti normative in materia di *fraud audit* e sistemi di controllo interno, con l'obiettivo di delineare il quadro teorico e regolamentare di riferimento, richiamare le metodologie più consolidate nella prassi professionale e chiarire il ruolo che il revisore assume nella gestione e nella mitigazione dei rischi di frode.

Il secondo capitolo introduce l'analisi empirica attraverso lo studio di un'impresa reale, la cui denominazione non viene riportata per garantire la riservatezza. L'attenzione è rivolta alla descrizione del sistema di controllo interno finalizzato alla prevenzione del rischio di frode, osservato nella sua configurazione complessiva e nelle modalità di integrazione nella gestione aziendale, così da ricostruire l'assetto formale dei presidi predisposti.

Il terzo capitolo presenta l'applicazione pratica delle metodologie di *fraud audit* sulla società oggetto di studio, illustrando l'impostazione del lavoro di revisione, le principali attività svolte e le evidenze raccolte. L'analisi consente di individuare le aree a maggiore esposizione al rischio di frode e di osservare i presidi messi in atto dalla società per contenerli, fornendo infine un quadro complessivo dei risultati emersi dall'analisi.

CAPITOLO 1 – FRAUD AUDIT E CONTROLLO INTERNO: METODOLOGIE E RUOLO DEL REVISORE NELLA GESTIONE DEI RISCHI DI FRODE

1.1 Definizione di fraud audit

Il termine “fraud” trae origine dal latino fraus, avente il significato di “inganno”. In ambito giuridico, la frode è comunemente intesa come l’impiego deliberato di artifici o mezzi illeciti, volti a privare un soggetto di risorse economiche, di proprietà o di diritti riconosciuti dalla legge. A tal proposito, l’Association of Certified Fraud Examiners (ACFE) definisce la frode come *“l’abuso del proprio ruolo per un arricchimento personale facendo leva sull’utilizzo degli asset e delle risorse aziendali”*. (ACFE, 2024) Tale definizione risulta particolarmente utile per inquadrare la natura del fenomeno, in linea con l'approccio adottato nel suo celebre studio, dove la frode viene considerata una minaccia sistemica per la governance e la sostenibilità del business. L’ACFE inoltre distingue tre grandi categorie di frode: l’appropriazione indebita di beni, comprendente furti, malversazioni e l’uso non autorizzato di risorse aziendali quali inventari o dati finanziari sensibili; la frode nella rendicontazione finanziaria, caratterizzata da bilanci redatti con dichiarazioni intenzionalmente fuorvianti; e la corruzione, che include pratiche quali tangenti e conflitti di interesse nei processi di acquisto e vendita. (ACFE, 2024)

La frode nella rendicontazione finanziaria, oggetto centrale del presente elaborato, compromette la credibilità dei report aziendali e può avere ripercussioni drammatiche: dalla perdita di fiducia da parte degli investitori—con conseguenti difficoltà nell’accesso al capitale o nell’ottenimento di condizioni finanziarie favorevoli—fino al dissesto di grandi gruppi, come ben documentato dagli scandali Enron (2003) e WorldCom (2002). Nel contesto aziendale, tale fattispecie può essere letta alla luce di una distinzione più ampia, che riconduce le condotte fraudolente a due macro-tipologie: da un lato quelle poste in essere dai dipendenti, spesso connesse a sottrazioni di beni o a pratiche corruttive volte a mascherare furti o tangenti; dall’altro quelle originate dal management, dai dirigenti o dai proprietari, più frequentemente associate a manipolazioni contabili finalizzate a sovrastimare o sottostimare i risultati di bilancio e, conseguentemente, ad alterare la percezione esterna delle performance aziendali. Sul versante della responsabilità sociale, gli stakeholder richiedono con crescente determinazione che le

imprese adottino standard etici rigorosi e sistemi di controllo efficaci, accrescendo l'urgenza di strategie di prevenzione e di detection tempestiva delle frodi (Paranamanna & Dissanayake 2021). Analogamente, le società di revisione che omettono di intercettare casi di frode, specie quelli di rilevanza mediatica, espongono sé stesse a ingenti danni reputazionali e a possibili azioni legali (Nelson et al. 2008). (Quick R.; Tümmler M., 2024)

Un modello teorico, ormai classico, elaborato oltre 60 anni fa e originato da un'ipotesi di Donald Cressey, offre una chiave di lettura delle condizioni che favoriscono l'insorgere di condotte fraudolente. Tale teoria individua tre fattori concomitanti alla base di una frode: *"Le persone tradiscono la fiducia che è stata loro accordata quando si trovano di fronte ad un problema finanziario non condivisibile con altri, quando sono consapevoli che questo problema può essere segretamente risolto approfittando del proprio ruolo a danno dell'organizzazione, e quando sono capaci di fare convivere la concezione di loro stessi come persone degne di fiducia con quella di utilizzatori non autorizzati dei fondi o delle proprietà loro affidate"*. (Cressey, 1953, citato in Abdullahi et al., 2015)

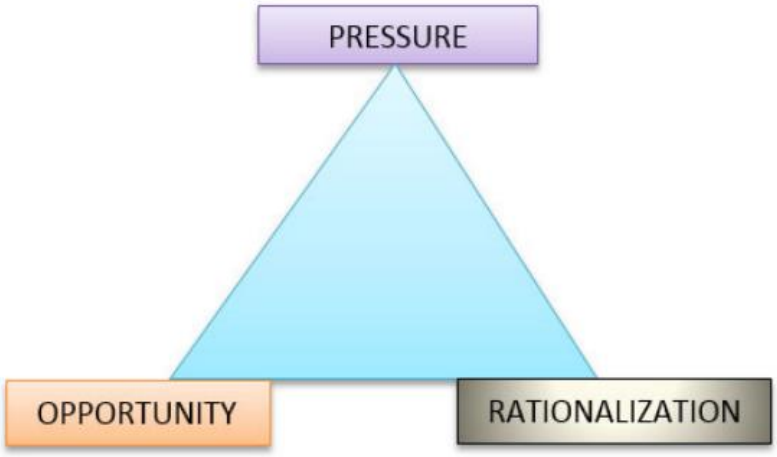
Questa descrizione corrisponde esattamente ai tre fattori che compongono il cosiddetto triangolo della frode:

- **Pressione o incentivo**, legata alla presenza di un problema finanziario o di un bisogno che non può essere condiviso;
- **Opportunità**, data dalla possibilità concreta di sfruttare la propria posizione per commettere la frode senza essere scoperti;
- **Razionalizzazione**, ossia la giustificazione psicologica che consente all'autore di conciliare l'azione fraudolenta con l'immagine di sé come persona affidabile.

L'autore paragonò quindi il fenomeno al "triangolo del fuoco": così come un incendio richiede simultaneamente ossigeno, calore e combustibile e per essere spento è sufficiente bloccare anche uno solo di questi fattori, allo stesso modo la frode si può prevenire interrompendo anche uno solo degli elementi che la alimentano. (Cressey, 1953, citato in Abdullahi et al., 2015)

Di seguito è riportata una rappresentazione grafica comunemente utilizzata in letteratura per sintetizzare i tre elementi individuati da Cressey, nota come "Fraud triangle"

Figura 1: Fraud Triangle



Fonte: (Abdullahi R.; Mansor N. , 2015)

Questa comprensione delle leve psicologiche e organizzative che alimentano la frode è tanto più cruciale in un contesto in rapida evoluzione: l'introduzione di tecnologie avanzate—dalla blockchain all'intelligenza artificiale—ha affinato le strategie di attuazione delle frodi, imponendo ai revisori un costante aggiornamento delle tecniche di audit per fronteggiare schemi sempre più complessi. La natura dinamica delle frodi, che si evolve adattandosi ai nuovi controlli, e la diffusione globale delle catene di fornitura e delle piattaforme digitali hanno trasformato il fenomeno in una questione transnazionale come dimostrano i recenti casi di Carillion (2018) e Patisserie Valerie (2019) nel Regno Unito, Wirecard (2020) e il Gruppo Adler (2022) in Germania, NMC Health (2020) negli Emirati Arabi Uniti, ed Evergrande (2024) in Cina che mettono in luce la persistenza e la gravità del problema su scala globale. (Quick R.; Tümmler M., 2024)

In questo contesto il *fraud audit* rappresenta una particolare declinazione dell'attività di revisione contabile orientata alla prevenzione, rilevazione e analisi delle frodi all'interno di un'organizzazione che si pone come principale obiettivo l'identificazione di comportamenti intenzionalmente illeciti che mirano a conseguire vantaggi indebiti, arrecare danni economici a terzi o compromettere la trasparenza del sistema aziendale. Il revisore esterno svolge un ruolo centrale, formulando valutazioni professionali sull'esposizione al rischio di frode e affiancando il management nell'implementazione di presidi preventivi e di rilevazione efficaci. Parallelamente, l'internal auditor assume funzioni complementari, garantendo un presidio continuo sul sistema di controllo interno

e supportando l'organizzazione nell'integrazione del fraud audit all'interno del più ampio Enterprise Risk Management, come verrà opportunamente approfondito in un paragrafo successivo dedicato alla descrizione di queste due figure. L'efficacia del fraud audit si fonda essenzialmente su tre obiettivi interconnessi: la prevenzione delle frodi, attraverso l'individuazione e il rafforzamento dei punti di vulnerabilità nei sistemi di controllo interno; la rilevazione tempestiva di anomalie e transazioni sospette mediante analisi approfondite dei dati aziendali; e infine l'investigazione, finalizzata a determinare natura, entità e responsabilità delle condotte fraudolente, nonché a predisporre una documentazione probatoria idonea a sostenere eventuali azioni legali o disciplinari. La guida *Managing the Business Risk of Fraud* evidenzia come tali risultati debbano tradursi in interventi sistematici a supporto della governance e del risk management, evitando che le informazioni raccolte rimangano isolate e inefficaci. (IIA ; AICPA ; ACFE, 2008)

A ciò si aggiunge il prezioso contributo delle tecnologie digitali, come Machine Learning e data analytics, strumenti in grado di rivoluzionare i processi di audit, che rendono più rapida e precisa l'individuazione dei pattern sospetti e dei segnali precoci di frode. Integrato in una cultura aziendale fondata sull'etica e sulla trasparenza, il fraud audit si rivela così uno strumento strategico indispensabile per assicurare la resilienza e l'integrità delle imprese nell'attuale contesto globalizzato e altamente interconnesso.

1.2 Evoluzione normativa e best practices nel fraud audit

Nel corso degli ultimi venti anni, l'ambito del fraud audit si è caratterizzato per una crescente complessità normativa e per l'adozione di best practices sviluppate sia dalle organizzazioni professionali sia dalla ricerca accademica. L'armonizzazione tra standard internazionali (ISA) e statunitensi (AU-C e AS del PCAOB) ha favorito un approccio condiviso alla gestione del rischio di frode, enfatizzando l'integrazione della fraud risk assessment nelle fasi di pianificazione e di esecuzione dell'audit. Contestualmente, le linee guida sviluppate da associazioni come l'IIA e l'ACFE hanno codificato metodologie operative – fra cui il fraud brainstorming e l'uso sistematico di data analytics – da tempo illustrate in letteratura come pratiche efficaci per individuare anomalie e schemi fraudolenti. (Quick R.; Tümmler M., 2024)

Parallelamente, la funzione di auditing ha subito una trasformazione profonda a causa sia della crescente complessità della attività fraudolente, sia delle innovazioni tecnologiche applicate alle procedure di controllo. Diversi lavori di ricerca hanno messo in luce il ruolo cruciale che gli auditor svolgono nel processo di rilevazione delle irregolarità, nonché l'impatto determinante delle tecnologie emergenti e dei quadri normativi sul rafforzamento dei meccanismi di detection. In primo luogo, l'efficacia dei professionisti nell'identificare attività fraudolente risulta sensibilmente influenzata dalla dimensione e dalle risorse della società di appartenenza: Kassem & Omoteso (2023) mostrano come i professionisti impiegati presso le "Big 4" riescano a intercettare con maggiore puntualità le inesattezze di bilancio, beneficiando della consolidata esperienza, di strumenti analitici evoluti e dell'accesso a metodologie di detection all'avanguardia. Infatti, numerose evidenze empiriche sottolineano come l'integrazione dei big data si sia rivelata determinante nel potenziare l'efficacia delle procedure di audit. In linea con tali evidenze Rahman & Xu (2022) dimostrano che i modelli di machine learning, in particolare le tecniche "ensemble"[1], superano nettamente gli approcci tradizionali basati su singoli algoritmi nell'identificazione di condotte fraudolente. Analogamente Mandal & Amilan (2023) sottolineano come l'introduzione di soluzioni basate su intelligenza artificiale e blockchain nel processo di revisione non soltanto migliori la qualità e trasparenza dei dati, ma contribuisca altresì a ridurre le possibilità di frode non rilevata. Accanto alle innovazioni tecnologiche, permangono differenze settoriali e territoriali nell'efficacia dei controlli antifrode. Ad esempio Ismajli et al. (2019) evidenziano come gli auditor del settore pubblico debbano spesso fare i conti con pressioni politiche e vincoli burocratici che ne ostacolano l'autonomia, differentemente dal settore privato, caratterizzato da contesti normativi più definiti. Dal punto di vista regolamentare, Damayanti & Agustia (2024) rilevano che l'inasprimento degli standard contabili e delle norme anti-frode si associa a tassi di detection sensibilmente più elevati; d'altro canto, Khersiat (2020) avverte che un'eccessiva rigidità normativa può avere l'effetto contrario di scoraggiare la segnalazione di potenziali irregolarità per il timore di sanzioni o responsabilità

[1] Con il termine "***metodi ensemble***" (o *apprendimento d'insieme*) si indica una famiglia di algoritmi di machine learning che, anziché basarsi su un singolo modello, combinano i risultati di più modelli predittivi (classificatori o regressori). L'idea di fondo è che l'aggregazione di modelli diversi riduca il rischio di errore e porti a previsioni complessivamente più accurate, stabili e robuste, poiché i limiti di ciascun modello vengono compensati dai punti di forza degli altri. (Davis, N.A.; Harris, S.A, 2024)

professionale, evidenziando la necessità di bilanciare rigore normativo e autonomia professionale. Alla luce di queste trasformazioni, i continui progressi negli strumenti di auditing digitale hanno rimodellato in modo sostanziale le strategie di individuazione delle frodi, rendendo imprescindibile un costante adeguamento del quadro normativo internazionale, tema che verrà approfondito nel paragrafo successivo. (Lestari P.A. ; Edeh F.O., 2024)

1.2.1 Quadro normativo internazionale

Nel corso degli ultimi decenni il panorama regolamentare internazionale in materia di fraud audit ha conosciuto un'ampia e progressiva evoluzione, trasformandosi da un insieme di principi generali di revisione in un vero e proprio corpus di standard e normative vincolanti, concepiti per garantire un approccio sistematico e coordinato alla prevenzione e all'individuazione delle frodi. Al vertice di questo quadro si collocano gli International Standards on Auditing (ISA) emanati dall'International Auditing and Assurance Standards Board (IAASB), che rappresentano il punto di riferimento mondiale per l'attività di auditing.

Tra essi, l'ISA 240, pubblicato nella sua formulazione originale nel 2009 e applicabile ai bilanci con esercizi iniziati dal 15 dicembre 2009, definisce in modo dettagliato le responsabilità del revisore in relazione al rischio di frode nel bilancio. Il principio stabilisce innanzitutto che l'obiettivo del revisore è ottenere una ragionevole sicurezza che il bilancio sia privo di errori significativi, incluse quelle dovute a condotte fraudolente, distinguendo la frode dall'errore alla luce del carattere intenzionale che contraddistingue la prima. Pur ribadendo che la prevenzione e la rilevazione delle frodi spettano primariamente al management e agli organi di governance, il principio impone al revisore di mantenere un livello di scetticismo professionale costante e di organizzare, all'avvio dell'incarico, una discussione strutturata con il team di lavoro per ipotizzare come e dove un'eventuale frode potrebbe manifestarsi nei conti. La procedura di risk assessment, il processo sistematico attraverso cui il revisore individua e misura la probabilità e l'impatto di inesattezze rilevanti nei bilanci, richiede interviste con le funzioni chiave, analisi comparative e la valutazione dei cosiddetti fraud-risk factors—pressioni o motivazioni, opportunità e razionalizzazioni—nonché dell'integrità del management. Dopo aver identificato e valutato i rischi al livello di bilancio e di

asserzione, il revisore deve progettare risposte adeguate: strategie complessive quali l'assegnazione di personale esperto o la modifica della tempistica dei test e procedure mirate, fra cui il controllo delle scritture di rettifica, la revisione delle stime critiche e l'esame di transazioni significative inusuali. Particolare attenzione è dedicata al fenomeno dell'*override* dei controlli da parte del management, inteso come l'elusione volontaria e consapevole delle procedure di controllo interno da parte dei soggetti apicali, la cui posizione consente di modificare, sospendere o ignorare i presidi predisposti, compromettendo così l'affidabilità complessiva del sistema di controllo. Il principio disciplina, inoltre, le modalità di comunicazione delle anomalie, imponendo l'obbligo di informare tempestivamente il management e gli organi di governance, e richiede la documentazione di tutte le valutazioni, discussioni e decisioni assunte. In caso di divergenze insanabili con la direzione o di rischio di revisione non riducibile a un livello accettabile, il revisore deve modificare la propria relazione o considerare la rinuncia all'incarico. (IASB- International Auditing and Assurance Standards Board, 2024) (IASB- International Auditing and Assurance Standards Board, 2009)

A febbraio 2024 l'IAASB ha pubblicato un Exposure Draft volto a revisionare l'ISA 240 e ad allinearlo in modo più rigoroso con i restanti standard di risk assessment e risposta ai rischi, in particolare l'ISA 315 (Identificazione e valutazione dei rischi di errori materiali) e l'ISA 330 (Procedure di audit in risposta ai rischi valutati). Tra le principali novità proposte, il documento intende rafforzare le prescrizioni relative al mantenimento dello scetticismo professionale, esplicitare ulteriormente le responsabilità del revisore in tema di frode e introdurre un maggiore dettaglio circa i requisiti di documentazione e i meccanismi di reporting verso gli organi di governance. Inoltre, l'Exposure Draft propone di rinominare alcuni "fattori di rischio di frode" come "indicatori di frode" per evitare sovrapposizioni con i concetti analoghi presenti nell'ISA 315, e di precisare meglio come tali indicatori debbano essere collegati alla valutazione complessiva del rischio. Nel dettaglio, il progetto di revisione presenta un'espansione delle procedure minime che il revisore deve applicare quando emergono segni di frode o dubbi fondati, includendo riferimenti più espliciti ai passi da compiere e ai livelli di approfondimento richiesti. Il progetto approfondisce inoltre il tema delle *Key Audit Matters (KAM)*, ossia le questioni che, per rilevanza e complessità, hanno richiesto la maggiore attenzione da parte del revisore nello svolgimento dell'incarico, invitandolo a valutare se e in che misura

segnalare nel report aspetti legati alla frode, così da bilanciare la necessità di trasparenza verso gli stakeholder con una corretta gestione delle aspettative del mercato. Parallelamente, vengono potenziate le indicazioni sul dialogo con il management e con gli organi di governance, nella convinzione che uno scambio tempestivo e strutturato sulle criticità fraudolente sia essenziale per ridurre il rischio residuo. L'obiettivo complessivo di queste innovazioni non è soltanto formalizzare con maggior precisione le *best practices* esistenti, ma anche rispondere alle sollecitazioni dei regolatori e delle associazioni professionali che, alla luce delle ispezioni condotte e dei risultati degli studi empirici, chiedevano standard più chiari e operativi per fronteggiare un fenomeno imprenditoriale – la frode – divenuto sempre più sofisticato e globale. (IASB- International Auditing and Assurance Standards Board, 2024)

Parallelamente agli ISA, l'Unione Europea ha istituito un proprio quadro normativo per rafforzare la lotta alle frodi a tutela degli interessi finanziari comunitari. Il Trattato sul Funzionamento dell'Unione Europea (TFEU), in particolare negli articoli 310 e 325, impone all'UE e agli Stati membri l'adozione di misure per prevenire, individuare e sanzionare le frodi che minacciano il bilancio comunitario. Su questa base, la Convenzione di Bruxelles del 1995 sulla protezione degli interessi finanziari delle Comunità Europee introdusse una prima definizione unificata di frode e impose agli Stati membri di adottare pene effettive; tale testo fu in larga parte sostituito dal Regolamento (CE, Euratom) n. 2988/95, che stabilì un regime sanzionatorio organico per le irregolarità finanziarie. (UNIONE EUROPEA, 1995)

Nel 2017 la Direttiva (UE) 2017/1371 – nota come "PIF Directive" – ha ulteriormente armonizzato le definizioni, le sanzioni e le regole di competenza giurisdizionale circa i reati di frode, corruzione e riciclaggio connessi agli interessi finanziari dell'Unione, uniformando le normative penali degli Stati membri al fine di garantire un contrasto coerente su tutto il territorio comunitario. (European Parliament, 2024)

Sul fronte statunitense, il Sarbanes–Oxley Act (SOX) del 2002 ha rappresentato una svolta normativa fondamentale in materia di audit e fraud audit. In particolare, le sezioni 302 e 404 hanno introdotto l'obbligo per CEO e CFO di certificare l'efficacia dei controlli interni e di attestare l'assenza di errori materiali. (Lyn Spooner; George Lekatis, 2025) A sua volta, nell'ambito della propria missione di rafforzare la trasparenza e

l'affidabilità delle informazioni finanziarie, il PCAOB, l'ente statunitense indipendente istituito nel 2002 per vigilare sulla qualità delle revisioni contabili delle società quotate in Borsa, ha emanato l'Auditing Standard (AS) 2401, intitolato "*Consideration of Fraud in a Financial Statement Audit"*. Questo standard è pensato come complemento dell'AU-C Section 240 dei *Clarified Statements on Auditing Standards* (AU-C) dell'American Institute of Certified Public Accountants (AICPA), che disciplina le procedure di audit relative al rischio di frode per le entità non quotate. L'AS 2401 specifica in modo più dettagliato le modalità con cui il revisore deve identificare i rischi di frode, gestire tempestivamente le comunicazioni di eventuali irregolarità ai livelli dirigenziali e di vigilanza, nonché documentare in modo esaustivo le conclusioni raggiunte e i supporti oggettivi raccolti durante l'incarico. In tal modo, AS 2401 innesta un quadro procedurale rigoroso e formalizzato, volto a garantire che la funzione di auditing negli Stati Uniti si avvalga di linee guida esplicite e comparabili a quelle previste a livello internazionale, promuovendo un approccio uniforme e trasparente nella prevenzione e nella rilevazione delle frodi. (PCAOB, 2004) Infine, le best practices internazionali sono arricchite da guide e position papers delle principali associazioni professionali. Il Position Paper "Fraud and Internal Audit" dell'Institute of Internal Auditors (IIA) stabilisce linee guida non obbligatorie ma ampiamente adottate in tema di fraud risk governance e ruoli dell'internal auditor. Il documento sottolinea come il presidio antifrode non possa limitarsi all'esecuzione di singole verifiche, ma debba essere integrato in un più vasto sistema di risk governance, in cui l'internal auditor contribuisce sia alla progettazione di efficaci controlli, sia alla verifica continua della loro operatività, e funge da soglia di allerta nei confronti del board. (The institute of internal auditors, 2019) Sul fronte delle metodologie di detection, il systematic literature review di Wang et al. (2024) presenta una sintesi critica delle ricerche sperimentali più recenti nel campo della rilevazione delle frodi e valorizza il fraud brainstorming come pratica chiave per l'individuazione precoce dei rischi. Gli autori evidenziano come le sessioni strutturate di brainstorming—condotte con team multidisciplinari e supportate da checklist standardizzate—facilitino l'emersione di scenari fraudolenti non immediatamente identificabili mediante le sole analisi dei dati, rafforzando così la capacità dell'organizzazione di mappare in modo proattivo i fattori di rischio. (Quick R.; Tümmler M., 2024)

Insieme, questi documenti forniscono un'ancora metodologica e culturale che affianca gli standard formali, promuovendo un approccio di fraud audit tanto rigoroso sul piano tecnico quanto ancorato a una responsabilità condivisa tra funzioni di governance, risk management e internal audit.

1.3 Il ruolo del revisore e dell'internal auditor nella prevenzione delle frodi

Il revisore esterno e l'internal auditor assumono ruoli differenti ma complementari nella prevenzione delle frodi aziendali poiché, pur operando su piani distinti, concorrono in modo sinergico all'efficacia del sistema di controllo interno e alla tutela della rendicontazione finanziaria. Da un lato, il revisore esterno, chiamato a esprimere un'opinione indipendente sui bilanci, rivolge particolare attenzione ai rischi di frode nelle fasi di pianificazione e svolgimento dell'audit, esercitando scetticismo professionale e applicando le indicazioni dell'ISA 240 per rilevare possibili manipolazioni contabili.

L'International Standard on Auditing 240 (ISA 240) intitolato *"Le responsabilità del revisore relative alla frode nell'audit del bilancio"* impone al revisore esterno di: *"Effettuare la valutazione del rischio di frode nel contesto della valutazione complessiva del rischio di revisione, identificando e valutando i rischi di errori significativi dovuti a frode, incluso il possibile override dei controlli da parte del management"*. Questa attività deve coprire sia i rischi a livello di entità sia quelli a livello di transazione, e richiede l'analisi dei controlli esistenti per mitigarli. (IASB- International Auditing and Assurance Standards Board, 2009)

Il Center for Audit Quality del PCAOB, nella pubblicazione del 2024, sottolinea come la capacità del revisore esterno di agire come deterrente dipenda non solo dall'adozione rigorosa degli standard internazionali, ma anche dalla qualità e dalla tempestività della comunicazione verso il comitato per il controllo interno e il Consiglio di amministrazione. Il report raccomanda di integrare nei working papers sezioni dedicate all'analisi dei red flags più ricorrenti — quali variazioni anomale nei margini operativi, discrepanze tra risultati di periodo e budget rappresentati in fase di approvazione, nonché segnalazioni di whistleblowing non adeguatamente investigate — e di predisporre una matrice di valutazione delle frodi, volta a classificare i rischi in funzione dell'impatto potenziale e della probabilità di accadimento. (Center for Audit Quality, 2024)

Per supportare l'analisi del ruolo e delle competenze del revisore esterno, Al Karabsheh (2021) ha realizzato un'indagine empirica volta a valutare in che misura il revisore possa fungere da deterrente e da primo strumento di rilevazione di frodi e corruzione finanziaria nelle società di servizi quotate all'Amman Stock Exchange. A tal fine, nella sua analisi ha formulato quattro ipotesi principali e le ha sottoposte a verifica mediante test t di "one sample" su un campione di 333 revisori affiliati all'Ordine dei Dottori Commercialisti giordani. La prima ipotesi (H1) sostiene che il revisore esterno svolga un ruolo statisticamente significativo nell'individuazione di illeciti economico-finanziari all'interno dei bilanci aziendali. Il test restituisce un valore di $t = 34{,}117$ ($p < 0{,}05$), confermando con forza il consenso degli intervistati sull'importanza primaria del revisore nell'identificare frodi e corruzione.

La seconda ipotesi (H2) esamina l'esistenza di vincoli professionali che possano ostacolare l'efficacia del revisore esterno. Anche in questo caso il risultato è significativo ($t = 12{,}117$; $p < 0{,}05$), evidenziando come fattori quali la scarsa comprensione del ruolo del revisore da parte dei comitati di controllo e l'assenza di politiche chiare sulle sue responsabilità possano limitare il potenziale di rilevazione delle frodi.

La terza ipotesi (H3) riguarda l'aderenza agli standard internazionali di audit – in particolare ISA 220, 230 e 240 – come fattore in grado di potenziare l'efficacia delle procedure di revisione nella scoperta di irregolarità. Il test $t = 32{,}271$ ($p < 0{,}05$) conferma che un forte commitment verso le norme professionali incrementa significativamente la capacità del revisore di riconoscere manipolazioni contabili e pratiche corruttive.

Infine, la quarta ipotesi (H4) valuta l'impatto di una pianificazione strutturata e dettagliata delle attività di audit sulla rilevazione delle frodi. Il valore $t = 29{,}681$ ($p < 0{,}05$) sottolinea l'importanza di un programma di lavoro esaustivo e ben documentato per massimizzare l'efficacia delle verifiche antifrode.

Nel complesso, queste evidenze empiriche confermano che, per svolgere appieno il proprio ruolo di deterrente e di primo baluardo nella prevenzione delle frodi aziendali, il revisore esterno deve non solo godere di un adeguato grado di indipendenza e di competenza tecnica, ma anche beneficiare di mandati chiari, del sostegno attivo dei comitati di audit e di un'adesione rigorosa agli standard internazionali, integrati in una pianificazione d'audit solida e coerente. (Al karabsheh F.I., 2021)

Parallelamente l'internal auditor è la figura centrale della cosiddetta "terza linea di difesa" nel modello di controllo interno, ovvero colui che fornisce un'assicurazione indipendente e approfondita sulle attività di risk management e sui controlli implementati dalle funzioni operative e di supervisione. Il modello delle "Three Lines of Defence" definisce un'architettura di governance nella quale la prima linea – rappresentata dalle funzioni operative – gestisce i rischi attraverso controlli integrati nei processi, la seconda linea – costituita da funzioni di compliance e risk management – sovrintende all'applicazione di policy e standard, mentre la terza linea fornisce un'assicurazione indipendente sull'efficacia complessiva del sistema di controllo interno; in questo contesto l'internal auditor assume il ruolo di terza linea di difesa, garantendo valutazioni obiettive e strategiche direttamente al Comitato di Audit e al Consiglio di Amministrazione. L'internal auditor, quale perno di questa terza linea di difesa, è investito di un ampio spettro di responsabilità che ne sanciscono al contempo l'autonomia professionale e la rilevanza strategica all'interno dell'azienda. In primo luogo, egli è chiamato a definire e periodicamente aggiornare il Charter dell'Internal Audit, documento guida che stabilisce missione, obiettivi, ambito operativo e linee di reporting della funzione, assicurando che tali elementi rimangano sempre allineati alle priorità di rischio e agli indirizzi del Comitato di Audit e del Consiglio di amministrazione. Questo impegno di governance interna implica non solo la formalizzazione delle procedure d'audit, ma anche la predisposizione di un programma di Quality Assurance and Improvement che comprenda valutazioni interne e, su base triennale, assessment esterni indipendenti, al fine di verificare la conformità alle Norme Professionali dell'Institute of Internal Auditors e di promuovere un piano di formazione continua per il team di audit. L'adozione di un approccio risk-based costituisce il nucleo metodologico dell'attività di internal audit: il professionista effettua innanzitutto un'analisi sistematica dei rischi organizzativi – con particolare attenzione ai fattori che facilitano la frode quali incentivi distorti, opportunità di manipolazione e razionalizzazioni –, dopodiché traduce tale valutazione in un piano di audit strutturato per priorità di rischio, in cui le procedure preventive (ad esempio, la verifica del disegno dei controlli), detective (controlli di conformità e analisi delle eccezioni) e correttive (raccomandazioni e follow-up) vengono calibrate sulla base dell'impatto potenziale e della probabilità di accadimento individuati. L'articolazione di queste attività non si limita all'esame a campione delle transazioni, ma include anche

tecniche di continuous monitoring, volte a integrare strumenti tecnologici per l'analisi dei dati e dashboard di indicatori chiave di performance e di rischio, che permettono di segnalare tempestivamente deviazioni rispetto ai parametri attesi e di avviare interventi mirati.

Inoltre, l'internal auditor svolge un ruolo chiave nell'assicurare che i flussi informativi, sia verso l'alto – attraverso report periodici al senior management e comunicazioni dirette al Comitato di Audit – sia verso il basso – garantendo che policy, procedure e lezioni apprese giungano a tutto il personale –, siano gestiti in modo trasparente e bidirezionale. Ciò presuppone non solo la predisposizione di report articolati sui risultati delle missioni d'audit e delle raccomandazioni di miglioramento, ma anche l'organizzazione di sessioni di feedback e formazione, finalizzate a diffondere la cultura del controllo e a rafforzare la sensibilità di manager e operatori rispetto ai rischi di frode. In quest'ottica il Chief Audit Executive (CAE) è il vertice della funzione di internal audit e dunque rappresenta l'elemento di sintesi tra la visione strategica del Consiglio di amministrazione e l'operatività dell' internal audit function, avendo la responsabilità di tradurre gli obiettivi di governance e controllo in un piano di audit coerente e dinamico. Per quanto riguarda l'adozione dei framework internazionali, il CAE svolge un ruolo di primo piano nel contestualizzare e integrare modelli quali COSO e la Fraud Risk Management Guide dell'IIA all'interno dei processi aziendali, coordinando la mappatura dei controlli esistenti, la revisione delle policy e la personalizzazione delle metodologie di valutazione del rischio di frode in linea con i cambiamenti regolamentari e con le specificità operative dell'organizzazione. Infine, attraverso la definizione di indicatori di performance e di cruscotti di monitoraggio, il CAE assicura un costante allineamento tra i risultati delle missioni di audit e le esigenze di miglioramento continuo, favorendo un processo evolutivo delle misure di prevenzione e rilevazione delle frodi che sia tanto reattivo quanto proattivo. (The institute of Internal auditors, 2024)

A sostegno di questo inquadramento teorico, sono stati utilizzati diversi studi empirici che mettono in luce le determinanti e gli effetti concreti dell'attività di internal audit nella prevenzione delle frodi aziendali. In particolare, nel loro studio empirico volto a comprendere i fattori che determinano il livello di impegno dell' internal audit function (IAF) nelle attività di prevenzione e rilevazione delle frodi, Bonrath e Eulerich (2024) raccolgono dati da 275 Chief Audit Executives di imprese quotate in Germania, Svizzera

e Austria, somministrando un questionario volto a misurare qualità del governance framework, frequenza dei contatti con audit committee e senior management, nonché grado di adozione di strumenti tecnologici avanzati per l'audit . Sulla base di un modello teorico di ordered logistic regression, gli autori formulano innanzitutto l'ipotesi (H1) secondo cui un ambiente di corporate governance più solido dovrebbe tradursi in un maggiore coinvolgimento dell'IAF nelle attività antifrode. Parallelamente, pongono al centro dell'analisi il "serving-two-masters issue" (H2), ossia la possibilità che incontri aggiuntivi con il comitato di audit possano vincolare l'autonomia operativa dell'IAF, mentre contatti più frequenti con il senior management ne stimolino al contrario l'azione proattiva. Infine, postulano che l'utilizzo di tecniche di audit analytics e continuous auditing, indicate congiuntamente come "Technology", favorisca un più marcato orientamento dell'IAF alla fraud risk management (H3) .

L'analisi dei dati conferma la solidità del modello complessivo ($p < 0{,}001$) e offre risultati significativi per tutte le ipotesi proposte. In particolare, il coefficiente associato alla qualità del governance framework assume valore positivo e altamente significativo ($\beta = 0{,}608$; $p < 0{,}01$), a conferma della relazione auspicata in H1. Quanto all'"audit committee effect" (H2), l'aumento delle riunioni riservate con il comitato di audit mostra un impatto negativo sull'attenzione antifrode dell'IAF ($\beta = -0{,}800$; $p < 0{,}01$), mentre la maggiore frequenza di incontri con il senior management evidenzia un effetto positivamente significativo ($\beta = 0{,}932$; $p < 0{,}05$). Infine, il parametro relativo all'adozione di strumenti tecnologici ottiene un coefficiente positivo pari a 0,321 ($p < 0{,}01$), dimostrando che l'integrazione di audit analytics e continuous auditing potenzia l'efficacia delle attività di fraud risk management. Il Nagelkerke R^2 di 0,246 suggerisce che, pur essendo rilevanti i driver esaminati, rimangono margini per indagare ulteriori determinanti dell'impegno dell'IAF nelle pratiche anti-frode. In sintesi, i risultati dello studio mettono in luce come un solido framework di corporate governance, caratterizzato da strutture decisionali chiare e da un ambiente di controllo robusto, si traduca in un coinvolgimento significativamente maggiore dell'internal audit function nelle attività di prevenzione e rilevazione delle frodi, mentre l'instaurarsi di frequenti e costruttivi confronti con il senior management funge da ulteriore catalizzatore dell'azione proattiva dell'IAF, consentendo di individuare tempestivamente i rischi emergenti e di concordare interventi correttivi mirati; d'altro canto, l'adozione di strumenti tecnologici

avanzati – quali audit analytics e procedure di continuous auditing – si conferma un fattore chiave per potenziare l'efficacia delle verifiche antifrode, amplificando la capacità di identificare anomalie e pattern sospetti, mentre un'eccessiva formalizzazione dei rapporti con il comitato di audit può paradossalmente ostacolare l'agilità operativa dell'IAF, limitando la tempestività delle azioni di controllo e la flessibilità nell'adattare le strategie di audit alle esigenze reali dell'organizzazione.

Non può tuttavia essere trascurato il valore aggiunto derivante dalla sinergia tra revisione esterna e internal audit: laddove l'internal auditor, grazie alla continuità di osservazione, offre insight puntuali sulle dinamiche operative e sui punti critici del sistema di controllo interno, il revisore esterno apporta una prospettiva indipendente e un'analisi focalizzata sulla correttezza della rappresentazione di bilancio. Bonrath e Eulerich evidenziano come il regolare scambio di report di audit e la partecipazione congiunta a meeting di risk assessment consenta di affinare le valutazioni dei rischi fraudolenti, riducendo le sovrapposizioni di attività e ottimizzando l'impiego delle risorse. (Bonrath A. ; Euleric M., 2023)

In definitiva, l'efficacia complessiva del sistema di controllo interno nella prevenzione delle frodi si fonda sull'integrazione armonica delle competenze e delle metodologie di revisione esterna e internal audit, sulla capacità di utilizzare congiuntamente tecniche avanzate di analisi dei dati e sulla rigorosa osservanza degli standard internazionali, sia in termini di risk assessment e pianificazione delle procedure, sia in termini di documentazione e reporting. Solo un approccio coordinato, caratterizzato da una comunicazione trasparente e da una condivisione costante di informazioni sui rischi e sulle anomalie rilevate, può garantire un'efficace barriera difensiva contro le frodi aziendali e accrescere la qualità e l'affidabilità dell'informazione finanziaria trasmessa al mercato.

1.4 Metodologie di revisione per valutare l'efficacia del sistema di controllo interno e rilevare frodi

Nel contesto di un audit integrato, il revisore esterno deve valutare l'efficacia del sistema di controllo interno sull'informativa finanziaria (Internal Control over Financial Reporting, ICFR), basandosi su evidenze adeguate e sufficienti che offrano un

ragionevole grado di sicurezza circa l'assenza di carenze significative alla data di valutazione della direzione. Tale obbligo sussiste anche se il bilancio non presenti errori materiali, poiché la sola individuazione di una debolezza rilevante compromette già l'affidabilità complessiva del sistema. A guidare questo approccio è il principio PCAOB AS 2201, che integra l'esame dei controlli interni con la revisione del bilancio: il professionista deve formulare la propria opinione "in un determinato istante" e "nel suo insieme", pur distinguendo chiaramente gli obiettivi di ciascun incarico e pianificando le procedure in modo da soddisfare simultaneamente entrambi. (Public company accounting oversight board, 2024) Durante la fase di pianificazione, il revisore deve considerare la conoscenza accumulata sui presidi di controllo maturata in precedenti incarichi, nonché valutare l'incidenza di fattori esterni quali le prassi di rendicontazione peculiari del settore, le condizioni macroeconomiche, gli sviluppi normativi e tecnologici, oltre ad aspetti interni quali struttura organizzativa, caratteristiche operative, fonte e natura del capitale, eventuali cambiamenti recenti nei processi o nei sistemi informativi, giudizi preliminari su materialità e rischio, carenze già comunicate in precedenza alla governance, contenziosi o questioni regolatorie in corso, disponibilità ed entità di evidenze già esistenti sull'efficacia dei controlli, informazioni pubbliche rilevanti sulla società, rischi individuati in sede di accettazione o mantenimento del cliente e, da ultimo, la complessità complessiva delle operazioni. Tale complessità si traduce in un costrutto graduato: imprese di minori dimensioni o con processi scarsamente articolati – contraddistinte da un numero limitato di linee di business, sistemi contabili centralizzati, forte coinvolgimento del senior management nell'operatività quotidiana e una struttura gerarchica piatta – possono conseguire gli obiettivi di controllo con modalità meno formali e più dirette rispetto a realtà di grandi dimensioni, caratterizzate da flussi transazionali eterogenei e stratificazione decisionale.

Poiché la valutazione del rischio rappresenta il fulcro di tutto il processo di revisione delineato dall'AS 2201, il revisore, nell'individuare i conti e le informative significativi, le relative asserzioni rilevanti e i controlli da testare, deve riconoscere che il grado di attenzione da destinare a un'area è direttamente proporzionale alla probabilità che in tale area possa annidarsi una debolezza significativa. Tale probabilità, di norma, è più elevata per i rischi connessi a frodi rispetto a quelli riferiti a meri errori non intenzionali; conseguentemente l'attività di audit dovrà concentrarsi sulle aree a maggiore esposizione,

evitando, per contro, di impiegare energie su controlli che, anche se inefficaci, non avrebbero verosimili ripercussioni materiali sul bilancio. Inoltre, le dimensioni e il grado di complessità di un'impresa – unitamente alla configurazione dei suoi processi operativi e delle unità organizzative – incidono sensibilmente sia sulle modalità con cui essa persegue i propri obiettivi di controllo, sia sulla natura dei rischi di errore che possono manifestarsi e, di riflesso, sui presìdi necessari a mitigarli. In tale prospettiva, il principio di scalabilità rappresenta l'estensione coerente dell'approccio risk-based, poiché consente di calibrare le procedure di revisione alla struttura specifica di qualunque realtà organizzativa. Ne deriva che un'entità di minori dimensioni o caratterizzata da processi poco articolati – così come una grande impresa con assetto operativo semplificato – può conseguire un livello di affidabilità paragonabile a quello di organizzazioni più complesse adottando controlli differenti ma proporzionati alla propria esposizione al rischio.

L'approccio top-down, inteso come schema logico e sequenziale di analisi piuttosto che come rigido ordine operativo delle procedure, guida il revisore nella progressiva individuazione dei rischi significativi e nella conseguente selezione dei controlli da sottoporre a verifica. Muovendo dai livelli più elevati – vale a dire dalla prospettiva d'insieme sul bilancio, sull'ambiente di controllo e sul contesto di governance – il professionista discende via via verso i processi, i conti, le informative e le singole asserzioni che presentano la maggiore probabilità di errore o di frode, così da concentrare l'attività di test sulle aree di effettiva rilevanza. Tale impostazione logica, pur delineando una gerarchia di analisi, non impone che le procedure di revisione siano materialmente eseguite nello stesso ordine: l'iter applicativo può infatti adattarsi alle circostanze senza tradire la logica di fondo, che rimane quella di collegare in maniera coerente i rischi riconosciuti ai controlli pertinenti.

In questo quadro concettuale, il revisore è tenuto a ottenere evidenze sui controlli che operano a livello di entità ogniqualvolta essi incidano in misura significativa sul giudizio finale circa l'efficacia complessiva del sistema di controllo interno sull'informativa finanziaria. L'esito di tale valutazione potrà legittimamente condurre, a seconda dei casi, a un'estensione o a una riduzione dei test da svolgere sui controlli di livello inferiore: controlli a presidio dell'ambiente di controllo particolarmente robusti, ad esempio, potrebbero consentire di limitare le verifiche su procedure di dettaglio; viceversa, qualora l'esame dei presìdi a livello di entità evidenziasse criticità o carenze, il revisore dovrà

incrementare la profondità delle sue indagini sui processi sottostanti, assicurandosi che l'insieme dei test resti sufficiente a fondare un'opinione attendibile sull'affidabilità del reporting finanziario aziendale. Nel corso dell'identificazione e verifica dei controlli a livello di entità e della selezione di quelli di processo, il revisore è chiamato a incorporare i risultati della risk assessment sui rischi di frode, accertandosi che i controlli individuati siano realmente in grado di mitigare tali rischi, inclusa l'eventualità di override da parte della direzione. In questa prospettiva risultano particolarmente rilevanti i controlli sulle transazioni significative e insolite, sulle rettifiche di fine periodo, sulle operazioni con parti correlate, sulle stime contabili a forte discrezionalità e, in generale, su tutti i meccanismi volti a ridurre incentivi e pressioni che potrebbero indurre il management a manipolare i risultati. Ove tali controlli presentino carenze, il professionista dovrà rifletterne gli effetti nella risposta ai rischi di errori significativi previsti dall'AS 2110, rafforzando le procedure di validità.

Al fine di acquisire evidenze, il revisore può, con giudizio professionale proporzionato al rischio del controllo in esame, utilizzare il lavoro svolto o l'assistenza diretta degli internal auditor, di personale aziendale debitamente supervisionato o di terze parti incaricate dalla direzione o dal comitato di audit, fermo restando che l'entità di tale affidamento decresce al crescere del rischio intrinseco. La materialità adottata per pianificare la revisione del controllo interno deve essere la medesima utilizzata per il bilancio d'esercizio. I controlli a livello di entità, peraltro, variano in natura e precisione: alcuni, ad esempio quelli relativi all'ambiente di controllo, esercitano un'influenza indiretta ma pervasiva sull'insieme dei processi di rilevazione e prevenzione di un errore e sugli altri controlli che il revisore seleziona per la verifica; altri monitorano l'efficacia di controlli di livello inferiore; altri ancora – disegnati con elevata granularità – sono in grado di prevenire o rilevare tempestivamente errori su talune asserzioni e, se sufficienti, consentono al revisore di ridurre la portata dei test su controlli subordinati. Tra i controlli che operano a livello di entità rientrano quelli inerenti all'ambiente di controllo, ai presìdi disegnati per prevenire l'override del management, al processo di identificazione e valutazione dei rischi aziendali, nonché ai meccanismi di monitoraggio dei risultati operativi e all'attività di sorveglianza esercitata su altri controlli, comprese le funzioni di audit interno e di autovalutazione. A tali elementi si affiancano i controlli specifici sul processo di rendicontazione di fine periodo e le politiche che regolano le principali

pratiche di gestione del rischio. Nel valutare l'ambiente di controllo, il revisore è tenuto a considerare la filosofia gestionale e lo stile operativo del top management, verificando che i valori etici siano coerenti con l'obiettivo di un reporting finanziario affidabile e che il Consiglio di amministrazione eserciti un'adeguata supervisione. Parimenti, il revisore deve valutare criticamente il processo di rendicontazione di fine periodo, analizzandone input, procedure e output, l'impiego dei sistemi IT, il coinvolgimento dei diversi livelli di management, le sedi operative interessate, le rettifiche e i consolidamenti, nonché la supervisione esercitata sulle chiusure annuali e trimestrali.

L'insieme di queste attività, articolate e sequenziali, consente al revisore di raccogliere elementi probativi sull'efficacia o meno dell'ICFR, di modulare coerentemente la propria risposta di audit alle aree a maggior rischio e, in ultima analisi, di emettere un giudizio informato e fondato, garantendo agli stakeholder l'affidabilità dell'informativa finanziaria prodotta dall'impresa. (PCAOB, 2024)

1.4.1. Focus sull'approccio top-down in audit: fasi chiave e obiettivi

Nel processo di audit integrato il revisore deve innanzitutto individuare, all'interno del bilancio consolidato, quei conti e quelle informative che rivestono carattere di significatività, nonché le correlate asserzioni che presentano una ragionevole probabilità di includere distorsioni in grado di compromettere, singolarmente o congiuntamente, la rappresentazione veritiera e corretta del rendiconto. A tal fine egli valuta congiuntamente parametri quantitativi – quali la consistenza numerica della voce e la sua esposizione a potenziali perdite – e fattori qualitativi, fra cui la natura dell'operazione, il volume e la complessità delle transazioni, l'eventuale presenza di parti correlate, l'uso di stime contabili di difficile misurazione, l'esistenza di rischi fraudolenti o di vincoli regolamentari, nonché le variazioni intervenute rispetto all'esercizio precedente nella composizione o nelle modalità di rilevazione.

Una volta circoscritte le aree di maggiore esposizione, il revisore determina le possibili fonti di errore domandandosi, per ciascuna voce significativa, «che cosa potrebbe non funzionare» lungo il flusso transazionale, dal momento dell'origine fino alla presentazione in bilancio. Tale riflessione, che include anche l'ipotesi di manipolazioni fraudolente, conduce all'identificazione dei controlli predisposti dalla direzione per

intercettare o prevenire tali distorsioni e dei presìdi volti a evitare utilizzi, acquisizioni o cessioni non autorizzate degli asset che possano generare errori materiali.

Poiché i fattori di rischio presi in considerazione coincidono nelle due componenti dell'audit integrato – la revisione del bilancio e quella dell'ICFR – la mappa dei conti e delle informative significativi risulta, di regola, identica in entrambe le prospettive. Va tuttavia rilevato che, all'interno di un medesimo conto, diverse sue componenti possono presentare profili di rischio eterogenei, circostanza che impone talvolta l'adozione di controlli differenti per affrontare adeguatamente ciascuna esposizione specifica.

Per acquisire una comprensione esaustiva delle fonti potenziali di errore, il revisore persegue quattro obiettivi principali: innanzitutto ricostruisce il flusso delle transazioni rilevanti verificando le modalità di avvio, autorizzazione, elaborazione e registrazione; in secondo luogo individua i punti critici del processo in cui potrebbe generarsi un errore materiale, ivi compresi quelli di natura fraudolenta; successivamente identifica i controlli implementati dal management per presidiare tali punti; infine prende atto dei meccanismi predisposti per scongiurare appropriazioni o utilizzi non autorizzati dei beni aziendali che potrebbero riflettersi in modo significativo sui conti. Dato il grado di giudizio richiesto, queste procedure devono essere svolte direttamente dal revisore o, in alternativa, da personale sotto la sua stretta supervisione; la comprensione dell'impatto dei sistemi informativi sul flusso delle operazioni rappresenta parte integrante – e non separata – di questo approccio top-down.

Tra le tecniche più efficaci per conseguire tali obiettivi figura il walkthrough, mediante il quale il revisore segue una transazione campione attraverso l'intero ciclo, avvalendosi degli stessi documenti e degli stessi sistemi informatici utilizzati dal personale aziendale. Combinando indagini, osservazione, ispezioni documentali e ripetizione dei controlli, il walkthrough fornisce evidenza diretta circa la corretta progettazione e l'effettiva applicazione dei presìdi, mettendo in luce, attraverso domande di approfondimento rivolte agli addetti, eventuali punti in cui un controllo indispensabile risulti assente o non adeguatamente disegnato. Nel corso del walkthrough, infatti, il revisore, giunto nei punti nodali del processo, interroga il personale per accertare la loro effettiva comprensione delle procedure e dei presìdi previsti dall'azienda. Le risposte ottenute, integrate con l'osservazione diretta e con l'esame della documentazione, consentono di accertare

l'adeguatezza del disegno dei presìdi e di individuare eventuali lacune nei punti di maggior criticità. Un dialogo che si estenda oltre la singola transazione campione, inoltre, consente al professionista di acquisire un quadro più ampio delle varie tipologie di operazioni significative gestite dal processo, rafforzando così la propria comprensione globale del sistema di controllo interno.

Nella fase successiva il revisore seleziona i controlli da sottoporre a test, concentrandosi su quelli che, singolarmente o in combinazione, mitigano in misura sufficiente il rischio di errore valutato per ciascuna asserzione rilevante. Non è pertanto necessario verificare la totalità dei controlli esistenti, né quelli ridondanti, a meno che la ridondanza non sia essa stessa un obiettivo di controllo: la decisione di testare un presidio non dipende dalla sua etichetta formale – che si tratti di controllo a livello di entità, di transazione, di monitoraggio o preventivo – bensì dalla capacità effettiva di ridurre il rischio individuato.

Il revisore, una volta individuati i controlli rilevanti, è tenuto a verificarne l'efficacia accertandosi che, se applicati secondo le modalità previste da personale dotato di adeguata autorità e competenza, essi consentano di conseguire gli obiettivi di controllo definiti dall'impresa prevenendo o intercettando tempestivamente errori o frodi potenzialmente in grado di generare distorsioni significative nei bilanci. Nell'eseguire tale valutazione occorre considerare che organizzazioni di dimensioni ridotte o con strutture operative meno articolate possono raggiungere il medesimo traguardo di presidio mediante soluzioni alternative rispetto a quelle adottate da entità di maggior complessità; il revisore deve pertanto stabilire se questi presìdi sostitutivi risultino effettivamente idonei.

La verifica della progettazione dei controlli si fonda su un insieme di indagini rivolte al personale responsabile, sull'osservazione diretta delle prassi operative e sull'ispezione della documentazione di supporto, combinazione che generalmente fornisce un livello di evidenza sufficiente per formulare un giudizio circa l'adeguatezza del disegno. Per quanto concerne l'efficacia operativa, il professionista deve stabilire se il controllo funzioni come concepito e se l'operatore disponga dell'autorità e della perizia necessarie: ciò richiede, oltre alle procedure già descritte, la ripetizione autonoma del controllo (re-performance) così da confermare la correttezza dei risultati conseguiti.

La quantità e la qualità delle evidenze richieste variano in ragione del rischio associato a ciascun presidio: quanto maggiore è la probabilità che un controllo inefficace si traduca

in una debolezza significativa, tanto più rigorose dovranno essere le procedure di test. Tale rischio è influenzato, tra gli altri elementi, dalla natura e dalla materialità delle potenziali inesattezze presidiate, dal rischio intrinseco legato ai conti e alle asserzioni, dalla frequenza e complessità delle transazioni, dall'affidabilità dei controlli a livello di entità, dalla competenza del personale addetto e dall'eventuale dipendenza da sistemi informatici o da procedure svolte da terze parti.

Qualora l'attività di verifica evidenzi deviazioni dal funzionamento previsto, il revisore deve valutarne l'impatto sulla stima del rischio e sulla quantità di prove ancora necessarie, ricordando che la presenza di singole eccezioni non implica automaticamente l'inefficacia complessiva, giacché il sistema di controllo interno fornisce ragionevole – e non assoluta – sicurezza. L'evidenza complessiva fornita dai test di efficacia dei controlli effettuati dal revisore deriva dal corretto bilanciamento tra la natura delle procedure (indagine, osservazione, ispezione, re-performance), tempistiche ed estensione. Quanto alla natura delle procedure, essa dipende, in larga misura, dalla natura del controllo da testare, incluso se l'operatività del controllo dia luogo a prove documentali della sua operatività e in linea di principio, la re-performance offre il grado più elevato di affidabilità, mentre la sola indagine non è mai sufficiente. Sotto il profilo temporale, test condotti su intervalli più ampi e in prossimità della data di riferimento della valutazione assicurano un livello di evidenza superiore rispetto a verifiche limitate o eseguite in periodi remoti. Qualora i controlli siano stati esaminati a una data intermedia, il revisore deve determinare la necessità di effettuare procedure di roll-forward per coprire l'arco temporale rimanente, tenendo conto del rischio collegato al controllo, dei risultati finora ottenuti, della lunghezza del periodo non coperto e di eventuali modifiche organizzative o procedurali intervenute. In situazioni di rischio contenuto può essere sufficiente un aggiornamento mediante indagine; al contrario, ove il rischio o i cambiamenti siano rilevanti, saranno richiesti nuovi test sostanziali per confermare la perdurante efficacia del presidio. Nella fase conclusiva dell'esame dei controlli interni il revisore è tenuto a valutare, con adeguato spirito critico, la gravità di ciascuna carenza emersa, al fine di stabilire se tale difetto – preso singolarmente o in combinazione con altri – integri gli estremi di una "significant deficiency" alla data individuata dal management per la propria attestazione. È opportuno chiarire che, benché il revisore non debba ricercare carenze di rilievo inferiore rispetto alla debolezza significativa, egli deve comunque esprimersi su ogni

carenza di cui sia venuto a conoscenza nel corso del lavoro, poiché la "ragionevole possibilità" che i controlli non riescano a prevenire o a individuare un errore rappresenta il criterio essenziale per stabilire la severità della lacuna, prescindendo dal fatto che un'inesattezza si sia effettivamente verificata. La ponderazione del rischio, dunque, si fonda su due direttrici principali: da un lato, la probabilità che il sistema di controllo non intercetti una distorsione potenzialmente materiale; dall'altro, l'entità dell'errore che potrebbe scaturire da quella specifica debolezza. Nel formare il proprio giudizio il revisore prende in esame molteplici variabili, quali la natura dei conti e delle asserzioni interessati, la suscettibilità delle poste a perdite o frodi, la complessità del giudizio richiesto per la valutazione contabile, l'interrelazione tra i vari presìdi (laddove un controllo possa considerarsi ridondante o, viceversa, interdipendente con altri), il possibile effetto combinato di più carenze nonché le conseguenze prospettiche che tali difetti potrebbero determinare. Una volta individuate le carenze, il revisore deve anche considerare l'eventuale presenza di controlli compensativi: affinché tali presìdi attenuino il rischio, essi devono operare con un livello di precisione tale da neutralizzare, in misura ragionevole, l'errore potenzialmente generato dalla debolezza originaria. Qualora tuttavia si ravvisi uno degli indicatori classici di "material weakness" – come la scoperta di frodi, ancorché non significative, poste in essere dal top management; la necessità di riformulare bilanci già pubblicati; l'individuazione di errori sostanziali nell'esercizio corrente che il sistema di controllo non avrebbe altrimenti intercettato; ovvero l'inadeguatezza dell'azione di vigilanza esercitata dal comitato di audit – la carenza deve essere qualificata senz'altro come grave. Infine, nella determinazione conclusiva il professionista deve porsi dal punto di vista di un "prudent official" e domandarsi se la carenza, isolata o congiunta ad altre, potrebbe impedire a un soggetto diligente di ottenere ragionevole assicurazione che le transazioni siano contabilizzate in conformità ai principi contabili generalmente accettati. Se la risposta è affermativa, la debolezza va elevata a "significant deficiency" e comunicata nelle forme prescritte, poiché incide in modo sostanziale sull'affidabilità dell'informativa finanziaria. Al termine dell'esame, il revisore è chiamato a esprimere un giudizio sul grado di efficacia del sistema di controllo interno relativo all'informativa finanziaria, fondando tale opinione sull'insieme delle evidenze raccolte lungo l'intero processo di audit: dai test di controllo eseguiti, agli errori eventualmente rilevati nella revisione del bilancio, sino alle carenze individuate nel corso delle proprie

procedure. In questa valutazione complessiva rientra altresì l'analisi delle relazioni prodotte, durante l'esercizio, dalla funzione di internal audit – o da strutture equivalenti – che abbiano riguardato presìdi connessi al controllo interno sulla rendicontazione finanziaria, dal momento che anche le debolezze segnalate in tali report concorrono a delineare il quadro finale.

Una volta formato il proprio convincimento, circa l'affidabilità dei controlli, il professionista deve inoltre verificare che la rappresentazione fornita dal management nella relazione annuale – predisposta secondo i requisiti regolamentari imposti dalla SEC – sia completa e corretta in ogni sua parte. Qualora, in esito a questa disamina, emergessero omissioni, inesattezze o presentazioni improprie, il revisore è tenuto ad applicare le disposizioni previste dal paragrafo C2 dello standard per determinare le azioni correttive da intraprendere.

È essenziale sottolineare che l'emissione di un'opinione in merito all'efficacia del controllo interno è possibile soltanto in assenza di limitazioni al campo d'azione dell'incarico; qualora l'estensione delle verifiche risultasse ostacolata in misura tale da non consentire l'ottenimento di sufficiente evidenza probatoria, il revisore dovrà dichiarare l'impossibilità di esprimere un giudizio ovvero, nei casi più gravi, rinunciare al mandato, conformemente alle indicazioni contenute nei paragrafi da C3 a C7 dello stesso standard. (PCAOB, 2024) (Annika Bonrath; Marc Eulerich, 2023)

1.4.2 L'interazione tra revisore esterno e management nell'identificazione di aree a rischio

Se – come prescritto dal modello di audit "top–down" – la mappatura dei rischi di bilancio prende avvio dalla definizione dei conti e delle asserzioni rilevanti, la qualità di tale esercizio dipende in larga misura dalla capacità del team di revisione di instaurare un dialogo tecnico-professionale con il vertice aziendale fin dalle primissime fasi di pianificazione. La letteratura empirica più recente evidenzia, infatti, che la condivisione bidirezionale di informazioni fra il partner di revisione e il management non soltanto amplia la gamma dei fattori di rischio considerati ma favorisce anche un'applicazione più coerente del principio di scetticismo professionale. Un primo contributo particolarmente significativo è fornito da *Kassem (2023)*, il quale – attraverso ventiquattro interviste semi-strutturate a revisori delle Big Four operanti negli Stati Uniti, nel Regno Unito e in

vari Paesi del Golfo – evidenzia che, teoricamente, integrità e motivazioni del top management costituiscono i fattori di frode ritenuti più critici dai professionisti; nella pratica, però, tali elementi vengono sistematicamente trascurati, perché considerati "troppo complessi" da attestare empiricamente e scarsamente supportati dalle linee guida degli standard internazionali. Ciò genera un fenomeno di autoselezione che induce i revisori a concentrare le proprie procedure quasi esclusivamente sulle opportunità di frode (debolezze di controllo, transazioni atipiche), lasciando in ombra la dimensione psicologica delle pressioni e delle razionalizzazioni. *Kassem* dimostra, inoltre, che tale distorsione riduce la completezza della valutazione del rischio e, di conseguenza, la qualità complessiva dell'audit: ne deriva l'esigenza di un dialogo più approfondito con la direzione volto a ricavare elementi sul clima etico e sui sistemi di incentivazione, così da colmare la lacuna informativa riguardante i fattori soggettivi. (Kassem R., 2023)

Se, da un lato, il colloquio con il management è indispensabile per ottenere informazioni di contesto, dall'altro lato esso introduce variabili relazionali che possono compromettere l'imparzialità del giudizio. Su questo punto si innesta la ricerca sperimentale di *Bennett e al*. che chiarisce in proposito il ruolo della *"likeability"* del management, intesa come l'insieme di tratti percepiti come positivi, quali cordialità, disponibilità, capacità di comunicare con chiarezza e, in generale, quella percezione di affabilità relazionale che genera fiducia e riduce la distanza professionale. Gli autori dimostrano che, quando i dirigenti vengono percepiti come particolarmente affidabili sotto questi profili, i revisori tendono ad attribuire un rischio di frode significativamente più basso; l'effetto si attenua soltanto in presenza di meccanismi stringenti di accountability o di un bagaglio di esperienza esplicitamente focalizzato sulla rilevazione delle frodi. La conseguenza operativa è che la qualità informativa del dialogo con il management deve essere bilanciata da robuste salvaguardie procedurali, quali la documentazione analitica delle evidenze raccolte, la riesamina critica da parte del partner e, ove opportuno, il coinvolgimento di membri del team con minori legami personali, al fine di neutralizzare l'influenza dei fattori affettivi sulle decisioni di pianificazione. (Schafer J.; Schafer B., 2018)

A questa fase preliminare di interazione con la direzione segue, secondo i principali standard di revisione, la sessione di brainstorming del team. Carpenter, con un disegno sperimentale condotto su revisori professionisti, dimostra che il brainstorming –

concepito come discussione libera ma strutturata fra i membri del team – produce idee di frode sia più numerose sia di qualità superiore rispetto alle medesime idee generate individualmente. Il risultato è particolarmente marcato quando i partecipanti, prima dell'incontro, hanno avuto accesso a informazioni fornite dal management relative alla strategia aziendale e ai processi sensibili: tali informazioni, infatti, fungono da "innesco cognitivo" per ipotizzare schemi fraudolenti complessi che difficilmente emergerebbero in assenza di un background informativo condiviso.

Ne consegue che la fruibilità del brainstorming dipende, in larga misura, dalla pertinenza delle informazioni raccolte in precedenza dal revisore attraverso l'interlocuzione con la direzione. (Carpenter T.D., 2007) (Mohd-Nassir M.D. ; Mohd-Sanusi Z.; Ghani E.K., 2016)

Il mero svolgimento della riunione, tuttavia, non garantisce di per sé un output di qualità. Brazel, Carpenter e Jenkins, attraverso un'indagine sul campo condotta in ventidue incarichi di revisione statunitensi, rilevano che non tutte le sessioni di brainstorming sono ugualmente efficaci: le riunioni caratterizzate da partecipazione equilibrata, agenda formale e documentazione sistematica delle idee si correlano a valutazioni di rischio di frode più accurate e a una maggiore estensione delle procedure di audit. Al contrario, brainstorming superficiali o dominati da pochi partecipanti non producono benefici tangibili e finiscono con il diluire la responsabilità individuale, generando il cosiddetto "effetto social loafing" [2]; L'efficacia della riunione, pertanto, dipende anche in questo caso dall'abilità del revisore di selezionare e condividere con il team le informazioni più rilevanti emerse nei colloqui con il management, evitando che la discussione si disperda su aspetti marginali o, viceversa, si concentri eccessivamente su aree di controllo già ben presidiate. (Brazel J.F.;Carpenter T.D. ;.Jenkins J.G., 2010)

Nel loro insieme, i quattro studi presi in esame delineano un circuito virtuoso. Il revisore, anzitutto, deve negoziare con il management l'accesso a informazioni che vadano oltre le mere opportunità di frode e comprendano i fattori motivazionali e attitudinali messi in luce da *Kassem*; successivamente, deve mitigare l'influenza dei rapporti interpersonali,

[2] Per **social loafing** s'intende la tendenza degli individui a ridurre l'impegno personale quando operano in attività di gruppo, poiché la responsabilità del risultato viene percepita come condivisa; (Nichols, T. & Patterson, J. (2014)) Nel brainstorming previsto dagli standard di audit (ISA 240, PCAOB AS 2110), il social loafing può portare a trascurare ipotesi di frode cruciali.

applicando le salvaguardie suggerite da *Bennett et al*. per prevenire giudizi indulgenti; infine, deve tradurre le informazioni ottenute in un brainstorming strutturato, alla luce delle evidenze di *Carpenter* e degli elementi di qualità operativa individuati da *Brazel et al.*. Solo integrando le tre dimensioni – informativa, relazionale e procedurale – la comunicazione con la direzione aziendale si trasforma in un reale vantaggio competitivo per l'attività di revisione, permettendo di individuare con maggiore precisione le aree a rischio e di progettare risposte di audit proporzionate.

Alla luce di tali evidenze, la best practices che emerge dalla letteratura prevede che il revisore documenti sistematicamente i colloqui con il management, valuti criticamente la credibilità delle dichiarazioni ricevute, coinvolga l'intero team in una discussione strutturata e, infine, allinei la strategia di audit alle risultanze emerse, prestando particolare attenzione ai fattori di frode che gli standard tendono a disciplinare in modo meno prescrittivo. L'efficacia dell'interazione tra revisore e management, pertanto, non consiste nella mera raccolta di dati, ma nella capacità di trasformare tali dati in conoscenza condivisa all'interno del team, riducendo al minimo gli effetti distorsivi delle dinamiche relazionali e massimizzando l'allineamento fra i rischi individuati e le procedure di controllo progettate.

Le riflessioni teoriche sviluppate in questo capitolo costituiscono la cornice metodologica di riferimento per l'analisi applicativa che segue, offrendo gli strumenti concettuali necessari per interpretare e valutare le evidenze empiriche. L'attenzione viene ora rivolta alla realtà aziendale oggetto di studio, mediante la ricostruzione del modello di governance e dei presìdi di controllo formalmente adottati, così da delineare un quadro chiaro delle strutture organizzative e dei meccanismi posti a presidio della correttezza operativa e informativa. Questo passaggio intermedio riveste un ruolo centrale, poiché consente di comprendere come le linee guida teoriche trovino concretizzazione nell'organizzazione concreta, ponendo al contempo le basi per una valutazione critica della coerenza, dell'affidabilità e dell'efficacia del sistema di controllo interno implementato dalla società.

CAPITOLO 2– ANALISI DEL CASO EMPIRICO: IL SISTEMA DI CONTROLLO INTERNO E LA SUA ARTICOLAZIONE

2.1 Overview: struttura aziendale e settore di riferimento

Nel presente lavoro di tesi è stato analizzato un caso empirico relativo a un'impresa operante nel settore dell'Integrated Healthcare Technology Management (HTM), la cui denominazione non verrà resa pubblica al fine di garantire il rispetto degli obblighi di riservatezza. Si precisa, tuttavia, che la revisione contabile del bilancio d'esercizio 2024 della società è stata effettuata da EY, primaria società internazionale di revisione e consulenza, presso la quale ho svolto il tirocinio curricolare prendendo parte al team incaricato della revisione.

La scelta di approfondire, all'interno del presente elaborato, un caso aziendale operante nel settore dell'Integrated Healthcare Technology Management (HTM) è motivata dalla rilevanza strategica assunta da tale realtà sotto un duplice profilo: da un lato, si tratta di uno dei principali player europei nella gestione integrata delle tecnologie biomedicali; dall'altro, l'esperienza di tirocinio svolta presso la società di revisione EY ha permesso di analizzare direttamente le dinamiche organizzative, i presìdi di governance e il sistema di controllo interno adottato, offrendo così un punto di vista privilegiato per una riflessione critica sul tema del fraud audit. L'adozione di un approccio basato sul *case study* risponde dunque all'esigenza metodologica di tradurre i riferimenti teorici in una dimensione applicativa, permettendo di osservare come i principi di controllo interno e di fraud audit trovino concreta attuazione nella prassi aziendale e offrendo al contempo l'opportunità di valutarne criticamente l'efficacia.

La società oggetto di analisi appartiene a un gruppo industriale organizzato attorno a una holding capogruppo, che esercita funzioni di coordinamento strategico, finanziario e gestionale sull'intero perimetro delle società controllate (Si precisa che nell'ambito dell'attività di revisione, il lavoro è stato svolto dal *primary team*, con riferimento sia al bilancio d'esercizio della società analizzata sia al bilancio consolidato predisposto dalla capogruppo). Le motivazioni alla base della sua selezione saranno illustrate in un paragrafo successivo. In particolare, l'impresa scelta per questo studio opera come uno dei principali soggetti operativi del gruppo nel settore dell'Integrated Healthcare

Technology Management (HTM), contribuendo in misura significativa allo sviluppo delle attività industriali e al conseguimento degli obiettivi operativi. La holding è a sua volta partecipata in via maggioritaria da un fondo infrastrutturale, che ricopre il ruolo di azionista di riferimento e definisce le principali direttrici strategiche, con un'attenzione specifica alle politiche di investimento sostenibile e alla valorizzazione del capitale nel medio-lungo periodo.

La governance del gruppo si articola in una struttura multilivello che prevede un consiglio di amministrazione supportato da comitati specialistici – incaricati delle politiche di remunerazione, delle nomine, della gestione dei rischi e della compliance – con l'obiettivo di definire le strategie di crescita, le politiche di investimento e i meccanismi di controllo interno conformi alle best practices internazionali; sul piano esecutivo, un ufficio centrale integra le funzioni di Finance & Administration, Risorse Umane, Information Technology e Quality & Compliance, coadiuvato da un'unità di internal audit il cui mandato è verificare l'efficacia dei processi aziendali e garantire l'aderenza a normative e standard di sicurezza clinica . Sul fronte operativo, la capogruppo coordina una rete di società operative suddivise per aree geografiche (EMEA, Americas, APAC) e per linee di servizio, comprendenti unità focalizzate su ingegneria clinica, assistenza sul campo, asset management e supply chain, le quali gestiscono centralmente le attività tecnico-operative nei rispettivi mercati. L'insieme di queste strutture permette di gestire circa 1,4 milioni di dispositivi medicali in oltre 2000 strutture sanitarie, avvalendosi di centri di eccellenza regionali organizzati secondo una logica matriciale che integra standard globali e specificità locali.

Il settore di riferimento, identificato nella disciplina dell'Healthcare Technology Management, comprende l'insieme dei processi di pianificazione strategica, acquisizione, manutenzione e dismissione delle tecnologie biomedicali e diagnostiche, caratterizzato da una crescente digitalizzazione dei servizi, dall'integrazione di soluzioni interoperabili per il monitoraggio in tempo reale degli asset e dalla necessità di modelli di collaborazione pubblico-privato per ottimizzare i budget sanitari e garantire al contempo elevati standard di sicurezza e compliance . L'acquisizione della capogruppo da parte del fondo infrastrutturale, formalizzata nei mesi antecedenti all'anno di riferimento, ha esteso il perimetro operativo a più di quattordici paesi europei e al Nord America, generando un

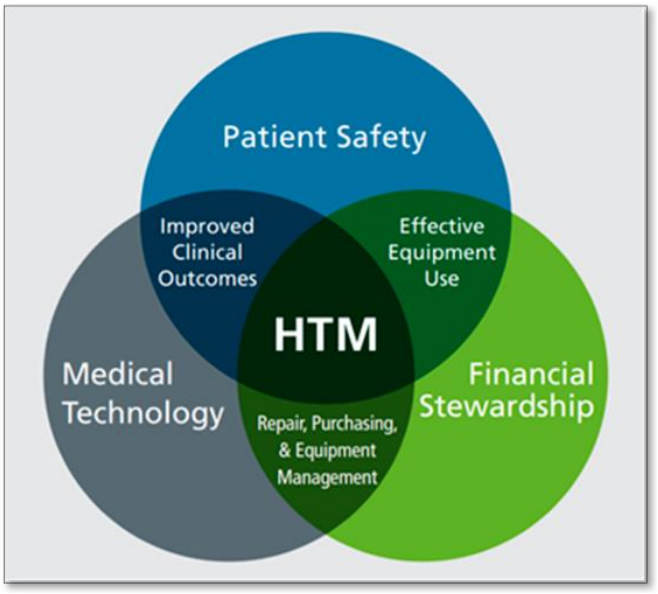
fatturato consolidato superiore a 200 milioni di euro, nonché perfezionando accordi di cessione per mercati extra-continentali per rafforzare ulteriormente il focus HTM.

Tutte le dinamiche competitive, tecnologiche e normative che caratterizzano il settore dell'Healthcare Technology Management verranno approfondite nel paragrafo successivo, dedicato alle evoluzioni di mercato e alle sfide per la gestione integrata degli asset sanitari. (Documentazione interna fornita dalla società: Linee Guida di Gruppo per il Modello 231 - Sezione Governance aziendale, ruoli e responsabilità, 2024)

2.1.1 Settore di riferimento e dinamiche di mercato

Il settore dell'Healthcare Technology Management (HTM) si configura come un ambito altamente specializzato all'intersezione tra ingegneria clinica, management sanitario e innovazione digitale, rivolto alla gestione integrata dell'intero ciclo di vita dei dispositivi medicali, dalla selezione e approvvigionamento fino alla dismissione finale. A conferma della natura multidisciplinare dell'HTM, l'Association for the Advancement of Medical Instrumentation (AAMI) propone una rappresentazione grafica in cui le attività HTM si collocano al centro della convergenza tra tecnologia medica, sicurezza del paziente e sostenibilità finanziaria (Figura 2).

Figura 2: The intersection of HTM roles and responsibilities within healthcare



Fonte: (Mahmoud T. ;Balachandran W.; Altayyar S., 2024)

La figura evidenzia come l'Healthcare Technology Management si ponga come punto di equilibrio tra questi tre ambiti, svolgendo un ruolo chiave nelle attività di gestione, acquisto e manutenzione delle apparecchiature, con l'obiettivo di migliorare gli esiti clinici e garantire un uso efficace e sicuro delle tecnologie sanitarie. Un aspetto fondamentale del settore risiede nella sua articolazione in una serie di domini funzionali che ne definiscono l'intero perimetro operativo: la pianificazione e la valutazione del bisogno, la selezione e l'approvvigionamento dei dispositivi, la gestione delle donazioni, l'inventario e il controllo di magazzino, l'installazione e il collaudo, la formazione degli utilizzatori, la manutenzione preventiva e correttiva e infine la dismissione e lo smaltimento degli apparecchi a fine vita. L'Organizzazione Mondiale della Sanità sottolinea come queste attività – comprendenti fornire consulenza tecnica, redigere specifiche, monitorare contratti, gestire workshop e staff, tenere registri, controllare parti di ricambio e implementare protocolli di sicurezza – siano indispensabili per assicurare che le tecnologie sanitarie siano disponibili, accessibili, sostenibili, appropriate e sicure, con un impatto diretto sui risultati assistenziali e sull'ottimizzazione delle risorse. (World Health Organization, 2017) . Con l'obiettivo di approfondire le peculiarità del settore, Mahmoud, Balachandran e Altayyar hanno proposto un articolato modello gerarchico di risk management appositamente concepito per l'Healthcare Technology Management, mediante il quale cinquantatré fattori di rischio distinti vengono classificati in una struttura a cinque livelli, permettendo così di delinearne in modo rigoroso priorità e interdipendenze. L'indagine ha posto in luce come queste variabili abbraccino una molteplicità di ambiti, ivi inclusi i profili tecnici inerenti al design dei dispositivi, nonché le complessità normative e organizzative che ne condizionano l'utilizzo; in tale contesto, il "Design Risk" è stato identificato quale elemento di massima criticità, a riprova della necessità di procedure di progettazione e validazione strutturate per garantire livelli adeguati di sicurezza e affidabilità. L'analisi dei pesi globali ha altresì confermato la rilevanza delle infrastrutture tecniche – comprendenti tanto la pianificazione quanto la manutenzione preventiva – e delle competenze specialistiche del personale, elementi che risultano fondamentali per contenere le vulnerabilità operative. Infine, attraverso l'applicazione di test di coerenza interna e di riproducibilità, gli autori hanno attestato la validità e la robustezza del framework, evidenziando la sua potenzialità quale strumento

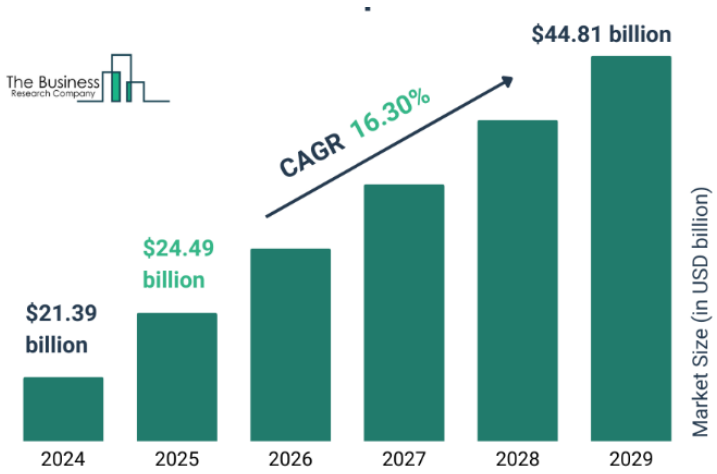
decisionale per la definizione di strategie di mitigazione orientate alla resilienza e alla sostenibilità dei servizi HTM. (Mahmoud T. ;Balachandran W.; Altayyar S., 2024).

Negli ultimi anni, le dinamiche di mercato hanno premiato i provider di HTM in grado di integrare piattaforme di monitoraggio in tempo reale e analytics predittivi, soluzioni che consentono di ridurre drasticamente i tempi di inattività dei macchinari e di ottimizzare i costi operativi mediante la pianificazione basata su dati, anziché su calendari fissi. Inoltre, i leader del settore stanno evolvendo il loro modello di servizio per trasformarsi in veri e propri partner strategici degli ospedali, offrendo non solo manutenzione corrective e preventive, ma anche consulenza per l'ottimizzazione del parco tecnologico, gestione della supply chain dei ricambi e formazione continua del personale clinico e tecnico. (PartsSource, 2024)

In base alle analisi condotte da The Business Research Company, il valore del mercato globale dell'HTM è stato stimato in 21,39 miliardi di dollari nel 2024 e si prevede raggiunga i 24,49 miliardi di dollari nel 2025, registrando un tasso di crescita annuo pari al 14,5%. Tale espansione è attribuibile a molteplici fattori, tra cui l'aumento della complessità tecnologica, la necessità di compliance normativa, la crescente attenzione alla manutenzione degli asset clinici, il bisogno di un monitoraggio efficace delle risorse e le crescenti esigenze in materia di sicurezza informatica.

Le proiezioni a medio termine indicano una prosecuzione di questa dinamica espansiva (Figura 3): entro il 2029, infatti, secondo le stime, il mercato della gestione della tecnologia sanitaria raggiungerà i 44,81 miliardi di dollari, con un CAGR stimato del 16,3%. Tra i principali driver che alimenteranno tale crescita, si segnalano lo sviluppo dei servizi di telemedicina, l'adozione sempre più diffusa dell'assistenza sanitaria basata sul valore nonché l'intensificarsi degli investimenti nella protezione dei dati e nella sostenibilità ambientale. (The Business Research Company, 2025).

Figura 3: Healthcare Technology Management Global Market Report 2025



Fonte: (The Business Research Company, 2025)

L'analisi identifica con chiarezza anche le principali tipologie di servizio offerte dagli operatori del settore. Tra queste figurano: manutenzione e riparazione delle apparecchiature, pianificazione del capitale, piattaforme software integrate, gestione operativa e della forza lavoro, approvvigionamento e gestione della supply chain, sicurezza informatica, qualità e conformità normativa. In particolare, i servizi di manutenzione e riparazione risultano essenziali per garantire la funzionalità dei dispositivi medicali nel tempo, migliorandone le prestazioni e prolungandone la vita utile. Queste attività includono interventi correttivi e preventivi, atti a preservare l'integrità delle apparecchiature impiegate nei diversi ambiti clinici.

Il mercato è inoltre segmentato per tipologia di struttura sanitaria servita: strutture di cura acuta (ad esempio ospedali, pronto soccorso, dipartimenti di emergenza), strutture di cura post-acuta (centri di riabilitazione, case di cura e strutture di lungodegenza) e strutture di cura non acuta (ambulatori, centri chirurgici ambulatoriali, servizi di assistenza domiciliare). Questa articolazione permette di adattare le soluzioni tecnologiche alle peculiarità organizzative e operative delle diverse realtà assistenziali.

Tra le principali tendenze che stanno caratterizzando il mercato nel 2025 emergono i continui progressi tecnologici, che stanno trasformando radicalmente il paradigma dell'HTM. Si osserva, in particolare, un'accelerazione nell'adozione di soluzioni basate su cloud, nell'utilizzo dell'intelligenza artificiale e dell'apprendimento automatico, nella

gestione dei dispositivi IoMT [3]e nella crescente digitalizzazione dell'intero ciclo di vita dei dispositivi medicali, inclusa la gestione della mobilità.

L'intensificarsi delle minacce informatiche ha inoltre reso la sicurezza dei dati un imperativo centrale nel settore: il costo medio globale di una violazione dei dati nel 2024 ha raggiunto i 4,88 milioni di dollari, segnando un incremento del 10% rispetto all'anno precedente e rappresentando il valore più elevato mai registrato. In questo scenario, la funzione dell'HTM si espande, integrando sistemi di rilevamento precoce delle anomalie, notifica automatica delle violazioni e protezione attiva delle informazioni sanitarie sensibili da accessi non autorizzati.

Un ulteriore impulso allo sviluppo del settore deriva dalla crescita costante dei servizi di telemedicina, i quali dipendono in larga misura da infrastrutture tecnologiche adeguate per il monitoraggio remoto dei pazienti e la gestione virtuale dei consulti clinici. Secondo i dati dei Centers for Disease Control and Prevention, nel 2022 il 37% degli adulti statunitensi ha utilizzato servizi di telemedicina. L'adozione è risultata più marcata tra le donne (42%) rispetto agli uomini (31,7%) e tende ad aumentare con l'età, raggiungendo il 43,3% tra i soggetti over 65. Tale tendenza riflette una domanda crescente di soluzioni HTM in grado di supportare efficacemente i dispositivi medici necessari alla teleassistenza.

Dal punto di vista delle strategie aziendali, il settore è attraversato da importanti dinamiche di innovazione e diversificazione dell'offerta. Molti operatori stanno introducendo sistemi automatizzati di gestione, che integrano l'elaborazione del linguaggio naturale per analizzare i feedback dei pazienti, generare alert in tempo reale e facilitare l'intervento proattivo da parte dei team clinici. Un esempio in tal senso è fornito dalla soluzione lanciata da TeleVox Software Inc. nel 2023, che consente di raccogliere, interpretare e rispondere rapidamente ai commenti degli utenti, ottimizzando la reputazione digitale delle strutture sanitarie.

[3] Nel settore della sanità, l'insieme delle tecnologie conosciuto come **Internet of Medical Things (IoMT)** include dispositivi indossabili, sensori remoti e apparecchiature mediche connesse, capaci di rilevare in tempo reale diversi parametri vitali e di inviare automaticamente tali informazioni al personale clinico per il loro utilizzo nei processi di diagnosi e cura.

In termini di distribuzione geografica, il Nord America si conferma come il principale mercato in termini di volumi nel 2024, seguito da Europa, Asia-Pacifico e altre regioni emergenti. In particolare, l'Europa si distingue per la presenza di un quadro regolamentare avanzato, che impone ai fornitori HTM rigorosi standard in termini di tracciabilità, audit, validazione delle prestazioni e documentazione dei dispositivi, in particolare alla luce del Regolamento UE MDR 2017/745. Tale regolamento, entrato in vigore nel 2021, ha introdotto requisiti più stringenti per la marcatura CE, ossia l'attestazione obbligatoria che un dispositivo medico rispetti i criteri europei di sicurezza, prestazione e qualità necessari per la sua commercializzazione nello Spazio Economico Europeo. Questi elementi premiano gli operatori in grado di garantire tempi di reazione brevi, capacità di adeguamento normativo e innovazione continua nei processi di quality assurance. (The Business Research Company, 2025)

2.1.2 Modello di business e principali flussi finanziari

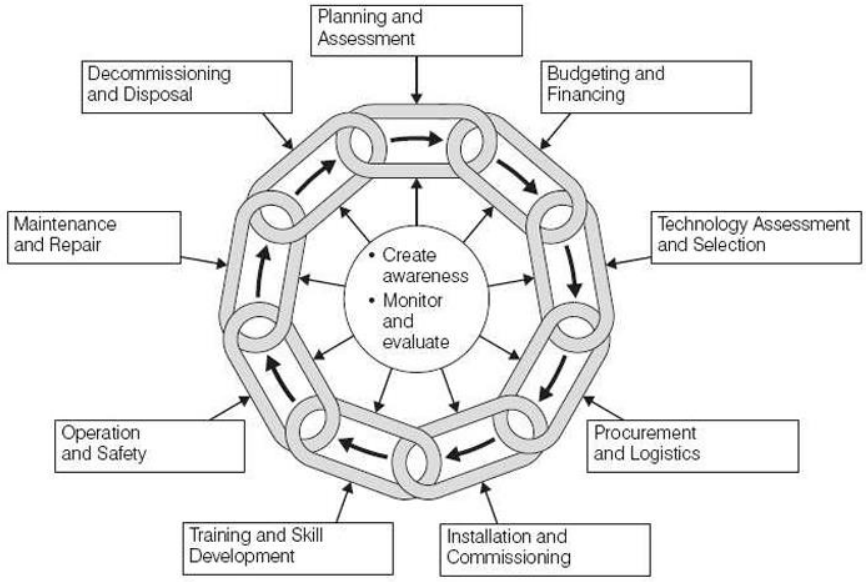
Il settore dell'Healthcare Technology Management (HTM) rappresenta una componente sempre più strategica nell'equilibrio tecnico ed economico delle organizzazioni sanitarie. L'evoluzione dei bisogni clinici, la crescente complessità delle tecnologie medicali e le tensioni economico-finanziarie che gravano sui sistemi sanitari hanno determinato un ripensamento radicale dei modelli gestionali tradizionali. Come sottolineato nel *State of HTM Report 2024,* negli ultimi anni molte organizzazioni sanitarie hanno dovuto fronteggiare problematiche legate ai backlog dei ricambi OEM [4], alla dipendenza da fornitori terzi poco efficienti e alla crescente complessità nella gestione degli asset tecnologici. In risposta, i programmi HTM più evoluti stanno adottando strategie basate sull'internalizzazione delle riparazioni, sulla razionalizzazione dei fornitori e sull'uso intensivo di strumenti predittivi e dati operativi, al fine di aumentare l'efficienza e la disponibilità clinica delle apparecchiature. (PartsSource, 2024)

Per comprendere appieno le dinamiche operative del settore Healthcare Technology Management, è fondamentale fare riferimento al cosiddetto Healthcare Technology

[4] Un **backlog** indica un insieme accumulato di ordini non ancora evasi. In ambito sanitario, riferito ai ricambi OEM (Original Equipment Manufacturer), indica un ritardo nell'approvvigionamento delle parti originali necessarie alla riparazione o manutenzione dei dispositivi medici.

Management Cycle, ovvero un modello ciclico che rappresenta tutte le fasi che scandiscono la gestione di un dispositivo medico all'interno di una struttura sanitaria. Tale modello, formalizzato nel diagramma di Lenel et al. (2005), si articola in nove fasi sequenziali, che costituiscono un riferimento consolidato per l'organizzazione sistemica dei processi tecnici, economici e gestionali connessi al ciclo di vita delle tecnologie sanitarie. Di seguito (*Figura 4*) si riportano la rappresentazione grafica e la relativa descrizione delle diverse fasi. (Lenel A.;Temple-Bird C.; Kawohl W. ; Kaur M., 2005)

Figura 4: The Healthcare Technology Management Cycle



Fonte: (Lenel A.;Temple-Bird C.; Kawohl W. ; Kaur M., 2005)

1. **Pianificazione e valutazione**

   La prima fase riguarda la definizione del fabbisogno tecnologico da parte della struttura sanitaria. In questo contesto si effettua un'analisi dei servizi clinici offerti e delle apparecchiature attualmente disponibili, al fine di individuare eventuali carenze, obsolescenze o necessità di potenziamento. La valutazione considera anche la compatibilità con l'infrastruttura esistente e con i processi sanitari in atto, ponendo le basi per una pianificazione coerente degli investimenti futuri.

2. **Budgeting e finanziamento**

   Una volta identificati i bisogni, è necessario definire le risorse economiche da destinare all'acquisizione e alla gestione delle apparecchiature. In questa fase si procede all'elaborazione del budget, comprendente sia i costi in conto capitale (CAPEX), legati all'acquisto iniziale, sia quelli operativi ricorrenti (OPEX), che includono manutenzione, formazione, pezzi di ricambio e gestione contrattuale. Vengono inoltre individuate le modalità di finanziamento più adeguate, che possono includere acquisto diretto, leasing operativo o outsourcing.

3. **Valutazione e selezione**

   Questa fase prevede una comparazione tra le diverse soluzioni tecnologiche presenti sul mercato, sulla base di criteri quali prestazioni cliniche, affidabilità, compatibilità tecnica, consumi energetici, facilità di manutenzione, durata prevista e costo totale di proprietà. L'obiettivo è individuare le tecnologie che offrono il miglior rapporto costo-beneficio nel medio-lungo termine, in relazione al contesto specifico della struttura sanitaria.

4. **Approvvigionamento e logistica**

   Una volta selezionata la tecnologia, si procede con l'approvvigionamento vero e proprio. Questo comprende la negoziazione contrattuale, la pianificazione delle consegne, la gestione delle forniture e la logistica interna. È inoltre necessario provvedere alla registrazione formale degli asset nel sistema informativo aziendale, con la creazione di un inventario tecnico che consenta la tracciabilità e il monitoraggio di ciascun dispositivo lungo tutto il ciclo di vita.

5. **Installazione e messa in servizio**

   In questa fase viene effettuata l'installazione fisica delle apparecchiature e il loro collegamento alle infrastrutture tecniche preesistenti (reti elettriche, informatiche, gas medicali). Segue il collaudo tecnico-funzionale, finalizzato a verificare la conformità alle specifiche previste. La messa in servizio rappresenta l'atto formale con cui il dispositivo diventa operativo e utilizzabile in ambito clinico, previa validazione da parte dei tecnici competenti.

6. **Formazione del personale**

   L'utilizzo efficace e sicuro delle tecnologie sanitarie richiede una costante attività di formazione rivolta al personale clinico e tecnico. In questa fase si organizzano sessioni formative iniziali e periodiche, finalizzate a garantire un utilizzo appropriato delle apparecchiature e a ridurre il rischio di errore umano. La formazione può riguardare sia aspetti operativi che di sicurezza, ed è spesso vincolata da requisiti normativi e contrattuali.

7. **Operatività e sicurezza**

   Questa fase coincide con l'impiego quotidiano del dispositivo nel contesto clinico. È cruciale che il suo utilizzo avvenga nel rispetto delle procedure operative standard, delle norme di sicurezza e delle raccomandazioni del produttore. La gestione sicura dell'uso clinico richiede anche una costante supervisione delle condizioni operative e un controllo dei parametri critici di funzionamento.

8. **Manutenzione e riparazione**

   Nel corso della vita utile dell'apparecchiatura, è necessario effettuare interventi di manutenzione preventiva e correttiva. La manutenzione preventiva ha l'obiettivo di preservare la funzionalità del dispositivo attraverso attività programmate, mentre la manutenzione correttiva interviene in caso di guasti o malfunzionamenti. Una gestione efficace di questa fase consente di minimizzare i tempi di fermo macchina, prolungare la durata operativa dei dispositivi e garantire la sicurezza del paziente.

9. **Disattivazione e smaltimento**

   L'ultima fase riguarda la dismissione delle apparecchiature obsolete o non più conformi agli standard. Il processo include la valutazione tecnica dello stato dell'asset, la disattivazione in sicurezza, la rimozione dalle reti e l'avvio a procedure di smaltimento o riciclo secondo le normative ambientali vigenti. È una fase spesso sottovalutata ma cruciale per assicurare la tracciabilità, la sostenibilità e la sicurezza dell'intero processo.

Al centro del ciclo si collocano le funzioni di monitoraggio continuo e creazione di consapevolezza, ritenute essenziali per il miglioramento continuo dell'intero sistema. (Lenel A.;Temple-Bird C.; Kawohl W. ; Kaur M., 2005)

Nel contesto del settore analizzato, le fasi centrali del ciclo (installazione, manutenzione, logistica, formazione) rappresentano anche le principali aree di costo per le aziende HTM. In particolare, vengono evidenziate come voci critiche: il personale tecnico qualificato, l'acquisizione e utilizzo di software predittivi per la manutenzione e il monitoraggio, e la gestione logistica dei pezzi di ricambio. Tuttavia, queste stesse attività costituiscono anche la principale fonte di valore generato, in quanto consentono di ridurre drasticamente i tempi di inattività delle apparecchiature, prolungarne la vita utile e migliorare la qualità e la sicurezza dell'assistenza clinica. (PartsSource, 2024)

Sul versante delle entrate, le imprese specializzate nella gestione delle apparecchiature biomedicali generano i propri ricavi prevalentemente attraverso contratti di servizio stipulati con strutture sanitarie pubbliche e private. Studi di settore evidenziano come le strutture ospedaliere siano frequentemente chiamate a gestire un numero elevato di contratti di servizio, con una media che può superare le cento unità per singolo ospedale, rendendo particolarmente complessa e onerosa la gestione amministrativa e tecnica delle apparecchiature medicali. Il risultato è un'elevata frammentazione che dunque apre spazi per operatori capaci di offrire contratti centralizzati e integrati. Inoltre, viene evidenziata una marcata variabilità nei prezzi applicati per asset identici – fino al 57% di differenza tra i costi minimi e massimi per lo stesso modello di apparecchiatura – che può essere sfruttata dai fornitori HTM per proporre offerte competitive e standardizzate. Le best practices individuate includono dunque la centralizzazione dei contratti, l'adozione di benchmark di costo e il monitoraggio delle performance tecniche, elementi che rappresentano sia fonti di valore per i clienti sia opportunità di efficienza per i fornitori specializzati, con un impatto diretto sui flussi economici in entrata e sull'ottimizzazione dei margini operativi. (PartsSource, 2025).

A fronte di ciò, viene evidenziato come stia emergendo un passaggio da modelli reattivi a modelli predittivi, in cui la gestione tecnica e contrattuale delle tecnologie viene supportata da strumenti digitali e decisioni basate su dati, capaci di migliorare la programmazione degli interventi, la qualità delle scelte di approvvigionamento e

l'efficienza complessiva dei programmi HTM. Il confronto tra le pratiche del passato e gli approcci futuri mostra una chiara transizione: dalla sostituzione prematura alla prolungata estensione della vita utile delle apparecchiature, dalla selezione dei fornitori su base reputazionale alla valutazione tramite dati oggettivi di performance, dalla manutenzione affidata completamente ai produttori OEM all'adozione di strategie contrattuali flessibili e dimensionate sul rischio reale dell'asset. (PartsSource, 2024).

In sintesi, il modello di business del settore HTM si fonda su un'equilibrata combinazione tra servizi ad alto contenuto tecnico, competenze specialistiche interne, uso estensivo di tecnologie digitali e accordi contrattuali performance-based, tutti elementi che si sviluppano e si articolano lungo le nove fasi del ciclo operativo HTM, determinandone al tempo stesso la struttura dei costi e la sostenibilità economico-finanziaria.

2.2 Il framework di controllo interno adottato

Dopo aver descritto le peculiarità del settore e le dinamiche che ne caratterizzano il funzionamento, con particolare riguardo alla crescente complessità gestionale e agli elevati profili di interesse pubblico che lo contraddistinguono, l'analisi si concentra ora sul sistema di controllo interno della società in esame, la cui rilevanza appare particolarmente significativa alla luce delle caratteristiche del settore in cui essa opera. Ai fini della ricostruzione di tale sistema in ottica antifrode, l'analisi è stata condotta sulla documentazione aziendale relativa al Modello 231, integrata dal Codice Etico e da ulteriori policy interne rese disponibili. Tale materiale, pur non esaurendo l'intero perimetro dei controlli interni, rappresenta il riferimento principale attraverso cui il Gruppo ha formalizzato i presìdi di prevenzione dei reati e delle frodi, disciplinando protocolli operativi, flussi informativi e responsabilità organizzative. La sua centralità rispetto all'obiettivo del presente elaborato risiede nel fatto che il Modello 231, unitamente agli altri strumenti di governance, costituisce lo strumento privilegiato mediante il quale l'impresa ha inteso rafforzare la propria capacità di prevenzione e individuazione delle condotte fraudolente. In questo quadro, il Codice Etico e di Condotta rappresenta il riferimento normativo e valoriale primario per tutte le funzioni aziendali, formalizzando l'impegno dell'organizzazione a garantire il rispetto della legge, la correttezza delle pratiche gestionali, l'integrità nei rapporti con i terzi, la trasparenza delle informazioni contabili e la tutela degli stakeholder interni ed esterni. La sua adozione non

ha solo una valenza simbolica o culturale, ma produce effetti giuridici concreti, poiché vincola tutti i destinatari – dipendenti, collaboratori, consulenti e partner – al rispetto delle norme e dei principi in esso contenuti. È previsto, inoltre, l'obbligo di rivolgersi ai superiori gerarchici o all'Organismo di Vigilanza, organo interno preposto a monitorare l'efficace attuazione del Modello 231, per ogni esigenza di chiarimento o interpretazione, e di informare i soggetti esterni, con cui la società intrattiene rapporti d'affari, circa l'esistenza e la portata del Codice stesso.

Dal punto di vista operativo, il Codice rappresenta un presidio trasversale del sistema di controllo interno: esso è richiamato nei contratti con i fornitori mediante specifiche clausole contrattuali, consegnato ai neoassunti all'interno del welcome kit e reso disponibile sulla intranet aziendale e sul sito web istituzionale. A conferma del suo ruolo nel rafforzamento dei controlli, ogni società del gruppo ha l'obbligo di promuoverne attivamente la diffusione e la conoscenza presso il proprio personale, anche attraverso iniziative di formazione differenziate in base al ruolo e al livello di responsabilità. I responsabili delle diverse funzioni sono chiamati a garantire, nei modi e nei tempi più opportuni, la trasmissione dei contenuti del Codice e l'allineamento comportamentale alle regole stabilite.

L'organizzazione promuove una cultura del controllo diffusa, fondata sulla consapevolezza dei rischi aziendali e sulla responsabilizzazione individuale. In tale ottica, il sistema di controllo interno viene descritto come un insieme coordinato di regole, procedure, presidi organizzativi e strumenti finalizzati a garantire, in modo integrato, la conformità normativa, la salvaguardia del patrimonio, l'efficacia dei processi aziendali e l'attendibilità delle informazioni finanziarie. Viene inoltre sottolineato come il sistema sia ispirato a best practices internazionali e conforme alla normativa applicabile, e sia strutturato per assicurare un adeguato livello di autonomia e indipendenza alle funzioni e agli organi deputati ai controlli.

Un ulteriore aspetto rilevante riguarda il rapporto con l'Organismo di Vigilanza della capogruppo e quelli istituiti presso le società di diritto italiano: tali organismi, insieme alla società di revisione legale incaricata, operano con piena autonomia e hanno accesso illimitato a dati e documentazione necessari per lo svolgimento delle rispettive attività. Allo stesso modo, ogni società del gruppo è tenuta a mantenere scritture contabili

dettagliate, complete e trasparenti, in linea con i principi contabili di riferimento e con i requisiti di tracciabilità e verificabilità delle operazioni. (Documentazione interna fornita dalla società: Modello di Organizzazione, di Gestione e Controllo All. 3 Codice Etico , 2024).

Dopo aver esaminato i principi generali contenuti nel Codice Etico e di Condotta adottato a livello di gruppo, l'analisi del sistema di controllo interno è proseguita con un focus analitico diretto su una specifica società controllata, individuata all'interno del perimetro consolidato. Tale scelta è stata guidata da motivazioni di ordine tecnico e metodologico: la società selezionata rappresenta infatti uno dei principali centri operativi del gruppo, sia in termini di rilevanza economico-finanziaria sia per la complessità dei processi gestionali coinvolti. A differenza della capogruppo, che svolge prevalentemente funzioni di indirizzo strategico e coordinamento finanziario senza essere direttamente coinvolta in attività operative, l'entità analizzata costituisce un nodo cruciale dell'esecuzione delle attività core, risultando pertanto particolarmente idonea ad una valutazione concreta dell'efficacia dei presidi di controllo antifrode.

La possibilità di osservare da vicino il funzionamento del sistema dei controlli interni, maturata grazie all'esperienza di tirocinio presso la società di revisione incaricata, ha ulteriormente rafforzato la coerenza della scelta effettuata, consentendo l'accesso a documentazione riservata e a elementi di osservazione diretta fondamentali per lo sviluppo dell'analisi.

Sebbene l'indagine sia stata condotta a livello di una singola società operativa, è stata mantenuta una prospettiva d'insieme, coerente con la logica di gruppo che regola l'organizzazione complessiva. I presidi di controllo osservati localmente si inseriscono infatti in un impianto normativo e procedurale definito a livello centrale, attraverso strumenti condivisi come il Group Accounting Manual e le policy di compliance, che assicurano un'omogeneità strutturale nell'approccio alla gestione dei rischi, compresi quelli di natura fraudolenta.

2.2.1 Struttura del sistema di controllo interno: componenti chiave

Nel contesto organizzativo della società oggetto di analisi, il sistema di controllo interno rappresenta un elemento fondante dell'assetto di governance, essendo concepito come un insieme coordinato di regole, procedure, strumenti applicativi e strutture organizzative finalizzati a garantire una conduzione dell'impresa improntata a criteri di legalità, trasparenza, correttezza e allineamento strategico con gli obiettivi aziendali. Tale sistema, pienamente integrato nei più ampi meccanismi di governo societario, è volto ad assicurare un'efficace attività di identificazione, misurazione, gestione e monitoraggio dei principali rischi, sia di natura operativa che legale, inclusi quelli connessi alla responsabilità amministrativa dell'ente ai sensi del D.Lgs. 231/2001.[5]

Le società appartenenti al gruppo adottano un modello di coordinamento di tipo matriciale, secondo il quale le funzioni aziendali delle controllate mantengono un'autonomia operativa, ma risultano collegate funzionalmente alle direzioni centrali della capogruppo. Tale assetto consente di assicurare un efficace coordinamento tra le singole legal entities e il vertice societario, nel rispetto dei criteri previsti di direzione e coordinamento dall'art. 2047 del Codice Civile, con un bilanciamento tra responsabilità operative e coerenza strategico-organizzativa.

Come emerso dall'analisi condotta sulla società e dalla documentazione esaminata, il sistema di controllo interno si articola secondo una logica strutturata su tre livelli distinti di controllo. Il primo livello, definito anche come controllo di linea, è assicurato dai responsabili delle diverse direzioni e funzioni operative e si concretizza nell'insieme dei presìdi quotidiani posti in essere nell'ambito dell'attività gestionale ordinaria. Il secondo livello di controllo è rappresentato dalle funzioni specialistiche di supporto che si occupano del presidio di specifiche aree di rischio, quali ad esempio il controllo di gestione, il sistema di gestione integrato, la funzione privacy e la compliance, sotto il coordinamento del Chief Compliance Officer. Il terzo livello, infine, è affidato al Chief Audit Executive, figura apicale cui è attribuita la responsabilità della funzione di internal auditing, e al Group Audit Steering Committee, con funzioni di supporto consultivo.

[5] Il tema sarà oggetto di approfondimento nel paragrafo successivo, dedicato all'analisi del Modello di Organizzazione, Gestione e Controllo ex **D.Lgs. 231/2001**.

In particolare, il Chief Audit Executive (CAE), oltre a essere il responsabile dell'intero sistema di controllo interno e della gestione dei rischi a livello di gruppo, riveste un ruolo chiave anche nella prevenzione dei reati ex D.Lgs. 231/2001. Tale figura sarà oggetto di un approfondimento specifico nel paragrafo successivo, dedicato all'analisi della funzione di internal Audit e compliance.

Il Group Audit Steering Committee rappresenta un organo di natura consultiva che assiste il CAE nelle attività di pianificazione, indirizzo e supervisione delle attività di audit, anche sulle società estere del gruppo, con l'obiettivo di assicurare un presidio adeguato sui rischi potenziali, in particolare quelli che possono determinare responsabilità risalenti verso la controllante. Tale comitato è composto dal Chief Audit Executive, da un membro del Consiglio di amministrazione, dal General Counsel e dal Chief Financial Officer, i quali concorrono a garantire un'efficace supervisione dei controlli in materia etica e organizzativa.

Il sistema descritto, nella sua articolazione multilivello, è oggetto di costante monitoraggio da parte del Consiglio di amministrazione, al quale spetta la responsabilità ultima di definirne le linee guida, verificarne l'adeguatezza e valutarne il funzionamento complessivo. A supporto di questa funzione, il Chief Audit Executive redige annualmente una relazione sull'efficacia del sistema di controllo interno e di gestione dei rischi, che viene sottoposta, per gli aspetti rilevanti ai fini del D.Lgs. 231/2001, all'approvazione dell'Organismo di Vigilanza, prima di essere trasmessa al Consiglio di amministrazione per la valutazione finale.

Infine, coerentemente con quanto indicato nel Codice Etico, le società del gruppo attribuiscono la responsabilità dell'attuazione effettiva del sistema di controllo interno a tutti i livelli organizzativi. In tale prospettiva, ciascun dipendente, nell'ambito delle proprie funzioni, è chiamato a contribuire in modo attivo alla costruzione e al mantenimento di un ambiente di controllo solido, alimentando la diffusione di una cultura aziendale orientata alla responsabilità, alla trasparenza e alla prevenzione dei rischi. (Documentazione interna fornita dalla società: Linee Guida di Gruppo per il Modello 231 - Sezione Sistema integrato di controllo interno , 2024)

2.2.2 Ruolo della funzione internal audit e compliance

La funzione di internal Audit e compliance all'interno del Gruppo riveste un ruolo centrale e trasversale nel presidio dei rischi aziendali, nell'assicurazione del rispetto normativo e nella verifica dell'effettivo funzionamento del sistema di controllo interno. L'articolazione di tale funzione è coerente con il modello dei tre livelli di controllo, in cui l'internal audit rappresenta il terzo livello, dotato di autonomia operativa e indipendenza gerarchica, mentre la compliance opera a cavallo tra il secondo e il terzo livello, in stretto raccordo con il Chief Audit Executive (CAE) e con le direzioni operative.

Il Chief Audit Executive è il principale garante del sistema di controllo interno a livello di gruppo. Egli è responsabile della pianificazione e della conduzione delle attività di audit, sia ordinarie sia straordinarie, compresa l'attivazione di verifiche conseguenti a segnalazioni ricevute attraverso i canali whistleblowing. Le sue attività si estendono all'intero perimetro organizzativo, comprese le società controllate, e sono finalizzate a garantire che i rischi – ivi compresi quelli connessi alla commissione di reati ai sensi del D.Lgs. 231/2001 – siano adeguatamente identificati, monitorati e mitigati.

Il CAE redige con cadenza annuale una relazione sull'adeguatezza e l'efficacia del sistema di controllo interno e di gestione dei rischi, che viene sottoposta all'approvazione dell'Organismo di Vigilanza per gli aspetti attinenti ai reati-presupposto del Decreto 231 e successivamente approvata dal Consiglio di amministrazione. Nell'ambito delle sue funzioni, il CAE opera in stretta sinergia con il Group Audit Steering Committee, organismo consultivo a composizione mista che supporta il coordinamento delle attività di audit e compliance.

Oltre alla funzione di audit, il CAE ricopre anche ruoli formali nei presidi di vigilanza delle società controllate, assumendo frequentemente la presidenza dell'Organismo di Vigilanza o il ruolo di organismo monocratico. Tale concentrazione di ruoli consente un presidio uniforme e centralizzato delle politiche di controllo e prevenzione, garantendo al contempo la coerenza tra le strategie di gruppo e le implementazioni locali. Tuttavia, essa richiede particolari garanzie di indipendenza e imparzialità, tanto che lo statuto del Gruppo vieta espressamente la sua rimozione senza giusta causa e senza parere vincolante del Collegio Sindacale, e proibisce la sua remunerazione su base incentivante legata a obiettivi economici.

La funzione compliance, sebbene distinta dal punto di vista operativo, agisce in stretto raccordo con l'internal audit, occupandosi della definizione e aggiornamento delle policy, della gestione dei flussi informativi regolati verso l'Organismo di Vigilanza e del supporto alle funzioni operative per quanto riguarda l'adeguamento alle normative di settore (tra cui salute e sicurezza, protezione dei dati personali, prevenzione della corruzione). In particolare, il Chief Compliance Officer presidia il rispetto delle normative "trasversali" e sovrintende alla gestione della documentazione informativa, alla tracciabilità delle attività e alla corretta attuazione dei protocolli di prevenzione dei reati.

Le attività delle due funzioni sono supportate da strumenti tecnologici di gestione documentale, database informativi, sistemi di tracciamento delle attività formative e piattaforme di whistleblowing, che consentono di monitorare in modo centralizzato l'effettivo grado di conformità dell'organizzazione rispetto agli standard fissati dal Modello 231 e dai regolamenti aziendali. In aggiunta, l'internal audit è chiamato a esprimere pareri consultivi sulle principali modifiche normative e organizzative, fornendo input strategici anche in sede di aggiornamento del Codice Etico e delle Linee Guida del Modello 231.

Nel complesso, l'interazione tra internal audit e compliance rappresenta uno snodo essenziale per la tenuta del sistema di controllo interno e per la prevenzione delle frodi aziendali. Il presidio centralizzato del CAE, la capillarità delle attività di controllo, e la formalizzazione delle responsabilità nei vari livelli dell'organizzazione sono elementi che, almeno sul piano teorico, contribuiscono a rafforzare la robustezza del sistema. Tuttavia, la complessità e l'elevato grado di interconnessione delle strutture coinvolte richiedono un'attenta e costante attività di supervisione, affinché le sinergie operative non si traducano in sovrapposizioni, conflitti di ruolo o lacune nel monitoraggio effettivo delle attività a rischio. (Documentazione interna fornita dalla società: Linee Guida di Gruppo per il Modello 231 - Sezione Sistema integrato di controllo interno , 2024)

2.2.3 Policy e procedure per la prevenzione dei reati: Il modello 231

Il Decreto Legislativo 8 giugno 2001, n. 231 ha introdotto nel sistema giuridico italiano la disciplina della responsabilità amministrativa degli enti, applicabile alle società, agli enti dotati di personalità giuridica e anche alle associazioni prive di personalità giuridica. Tale normativa ha segnato una svolta rilevante nel diritto penale d'impresa, affermando il principio secondo cui gli enti collettivi possono essere ritenuti responsabili, in sede penale, per determinati reati commessi nel loro interesse o a loro vantaggio.

La responsabilità dell'ente si configura in presenza di reati espressamente indicati dalla legge – i cosiddetti reati presupposto – commessi o anche solo tentati da soggetti apicali, ossia da coloro che esercitano funzioni di rappresentanza, amministrazione o direzione dell'ente, ovvero da chi ne gestisce e controlla l'attività, anche di fatto. Tale responsabilità può emergere anche nei confronti di reati commessi da persone sottoposte alla direzione o alla vigilanza dei soggetti apicali, qualora il reato sia riconducibile a lacune nel sistema di organizzazione e controllo dell'ente stesso.

Al fine di prevenire tali responsabilità e di costruire un presidio solido contro il rischio-reato, il legislatore ha previsto per gli enti la possibilità di adottare un Modello di Organizzazione, Gestione e Controllo idoneo a prevenire la commissione dei reati contemplati dal decreto. Il Modello 231 assume così un ruolo strategico all'interno dell'assetto dei controlli aziendali, ponendosi come un sottosistema specificamente orientato alla prevenzione dei rischi penali, in piena integrazione con il più ampio sistema di controllo interno. (Decreto Legislativo 8 giugno 2001, n. 231)

Il Modello 231 adottato dalla società oggetto di analisi prevede la mappatura delle aree aziendali a rischio, la definizione di protocolli comportamentali e decisionali, un sistema disciplinare, l'attivazione di un canale di segnalazione (whistleblowing) e la nomina di un Organismo di Vigilanza (OdV) autonomo e indipendente, dotato di pieni poteri di accesso, verifica e controllo.

Tra i reati presupposto che rivestono particolare rilievo ai fini dell'analisi del rischio di frode rientrano i reati societari, quali le false comunicazioni sociali, l'ostacolo alla funzione di controllo e l'illecita influenza sull'assemblea, nonché i reati tributari e

finanziari, come le dichiarazioni fraudolente, l'omessa dichiarazione, l'indebita compensazione e il riciclaggio.

Il Modello 231, nella prassi, si integra con il sistema dei controlli aziendali, grazie alla stretta collaborazione tra l'OdV, la funzione internal audit, la funzione compliance e i presìdi operativi dislocati nei processi aziendali più esposti a rischio. La valutazione dell'efficacia del modello è supportata da audit periodici, report di monitoraggio e una formazione specifica rivolta ai dipendenti, al fine di promuovere la cultura della legalità e rafforzare la prevenzione delle frodi interne ed esterne.

Nel contesto della società analizzata, il Modello 231 non è concepito come uno strumento formale, ma rappresenta un elemento sostanziale del sistema di governance, contribuendo a rafforzare la trasparenza, la tracciabilità delle decisioni e la responsabilizzazione dei soggetti coinvolti nei processi sensibili. L'effettiva applicazione e aggiornamento del modello risultano quindi determinanti per la mitigazione del rischio di frode e per la tutela dell'integrità aziendale nel suo complesso.

Il Modello di organizzazione, gestione e controllo adottato dal gruppo, in conformità al Decreto Legislativo 8 giugno 2001 n. 231, rappresenta uno dei principali presidi posti a tutela dell'integrità aziendale e della conformità normativa. Tale Modello, formalizzato secondo le Linee Guida approvate dal Consiglio di amministrazione, costituisce un insieme sistemico e coerente di principi, regole e strumenti funzionali alla prevenzione dei reati contemplati dal Decreto, attraverso un approccio integrato alla gestione dei rischi e dei controlli interni e definisce le key rules cui devono conformarsi i modelli organizzativi delle singole controllate. Le Linee Guida fungono da riferimento per la definizione dei Modelli 231 da parte delle società del Gruppo con sede nel territorio nazionale, che sono tenute ad adottare un assetto organizzativo e di controllo commisurato alla propria struttura e complessità. Resta ferma la possibilità di modulare, secondo criteri di proporzionalità, specifici aspetti come la composizione dell'Organismo di Vigilanza. La capogruppo assicura la diffusione delle Linee Guida e dei relativi aggiornamenti agli organi amministrativi delle controllate, le quali, in assenza di un proprio Modello, devono comunque garantire la prevenzione dei reati attraverso misure organizzative e di controllo interno adeguate. Alla base del Modello 231 si colloca un processo strutturato di individuazione delle attività aziendali nelle quali potrebbero manifestarsi rischi di

commissione di reati rilevanti ai sensi del Decreto. Tale processo, definito come "as-is analysis", è finalizzato alla mappatura delle aree a rischio reato e delle attività cosiddette "strumentali", ossia quei processi che, pur non costituendo attività sensibili in senso stretto, possono indirettamente facilitare o mascherare comportamenti illeciti. Il processo di mappatura viene aggiornato periodicamente e tiene conto delle evoluzioni normative, dei mutamenti organizzativi interni e dell'esperienza operativa maturata. Le attività di valutazione del rischio si fondano su audit annuali e autovalutazioni coordinate dal Comitato di Audit, oltre che su questionari somministrati ai responsabili delle diverse funzioni operative, i cui risultati confluiscono in una relazione periodica sull'adeguatezza del sistema di controllo interno, da sottoporre all'Organismo di Vigilanza (OdV).

Elemento cardine del Modello è rappresentato dai protocolli decisionali, i quali costituiscono un insieme di procedure e regole operative che disciplinano in modo analitico le modalità di esecuzione delle attività sensibili. Tali protocolli sono orientati a garantire la trasparenza, la tracciabilità e la corretta allocazione delle responsabilità nei processi aziendali maggiormente esposti a rischio. La loro implementazione avviene in raccordo con i sistemi di gestione preesistenti, in particolare con il Sistema di Gestione Integrato della Qualità già attivo presso numerose società del Gruppo, come in quella presa in esame. Tra i protocolli espressamente previsti rientrano, a titolo esemplificativo ma non esaustivo, quelli relativi all'acquisto di beni e servizi (in particolare consulenze), alla formazione del bilancio consolidato, alla gestione delle operazioni infragruppo e alle procedure amministrativo-contabili, con particolare attenzione alla prevenzione dei reati tributari.

La formazione riveste un ruolo strategico nella diffusione della cultura della legalità e del controllo. Il piano formativo previsto dal Modello è modulato in base alla funzione ricoperta e si sviluppa attraverso incontri frontali per amministratori e figure apicali, sessioni formative dedicate al personale delle funzioni commerciali e moduli in modalità e-learning per il restante personale, in modo da garantire capillarità e tracciabilità della formazione erogata. I contenuti formativi sono concordati con l'Organismo di Vigilanza e sono aggiornati periodicamente in base alle esigenze normative e operative. Oltre alla formazione, è previsto un sistema informativo che assicura la disponibilità delle procedure e dei documenti rilevanti tramite l'intranet aziendale, mentre per i soggetti

esterni (fornitori, partner commerciali e finanziari) è previsto l'accesso al Codice Etico e agli estratti del Modello pubblicati sul sito istituzionale.

Il sistema disciplinare costituisce una componente essenziale del Modello e ha lo scopo di garantire l'effettiva osservanza delle regole, sanzionando eventuali violazioni. Esso prevede misure graduate e proporzionate in funzione della gravità dell'infrazione e della qualifica del soggetto responsabile, applicabili sia a soggetti interni (dipendenti, dirigenti) sia a collaboratori esterni, consulenti e partner. Le sanzioni, conformi alla normativa vigente e ai contratti collettivi applicabili, comprendono il richiamo formale, la sospensione, la decurtazione di compensi o incentivi, fino alla risoluzione del rapporto contrattuale nei casi più gravi.

In conformità a quanto previsto dal D.lgs. 231/2001, un ruolo centrale nella gestione e nel presidio del Modello 231 è svolto dall'Organismo di Vigilanza (OdV), organo dotato di autonomia, indipendenza e pieni poteri di iniziativa e controllo, incaricato di vigilare sull'efficace attuazione del Modello, nonché sulla sua idoneità e aggiornamento continuo. Al fine di assicurare un presidio efficace e coordinato dell'intero sistema di prevenzione dei reati a livello di gruppo, la società ha adottato un modello organizzativo che prevede la nomina degli stessi soggetti fisici quali componenti dell'Organismo di Vigilanza della capogruppo e delle società controllate italiane.

Ciascuna società mantiene la propria autonomia giuridica e istituisce formalmente un proprio organismo di Vigilanza; tuttavia, la composizione personale degli organismi è identica, in un'ottica di razionalizzazione delle risorse, uniformità metodologica e presidio integrato dei rischi-reato. In linea generale, l'Organismo di Vigilanza opera con composizione collegiale ed è costituito da tre membri esterni, incluso il Presidente, selezionati per assicurare un bilanciamento tra competenze penalistiche, di revisione contabile, di audit, di analisi dei rischi e antifrode. A questi si affianca un componente interno, solitamente il Chief Audit Executive (CAE) della capogruppo, il quale può anche assumere il ruolo di Presidente dell'OdV. La presenza del CAE consente di integrare la conoscenza dei processi aziendali nel funzionamento dell'Organismo. Nelle controllate di dimensioni minori, può essere adottata una composizione monocratica dell'OdV. Inoltre, può essere prevista la partecipazione di un componente del Collegio Sindacale nell'Organismo, al fine di rafforzare il coordinamento tra organo di controllo e organo di

vigilanza. Il Presidente dell'Organismo di Vigilanza è tenuto a informare tempestivamente gli altri componenti su eventuali questioni di rilievo emerse nell'ambito del proprio ruolo all'interno del Gruppo, utilizzando qualunque mezzo ritenuto idoneo. Per garantire continuità operativa e una corretta diffusione delle decisioni dell'OdV alle strutture aziendali, alle riunioni dell'Organismo è assicurata la presenza di una segreteria tecnico-legale interna, nonché la partecipazione, in qualità di invitati esterni, di funzioni di controllo, inclusa la funzione di compliance.

Al fine di rafforzare il coordinamento con l'Organo di Controllo, le riunioni dell'OdV devono prevedere la partecipazione del Presidente del Collegio Sindacale o di un sindaco da lui delegato. Tuttavia, l'eventuale assenza di quest'ultimo non comporta l'invalidità della seduta. In caso di violazione degli obblighi o di inattività da parte di un componente dell'OdV, la relativa contestazione e l'adozione del conseguente provvedimento – disciplinare, se si tratta di un soggetto interno, o di revoca dell'incarico, se esterno – sono di competenza del Consiglio di amministrazione, su proposta del Presidente dell'Organismo, previo parere del Collegio Sindacale.

L'OdV opera secondo il principio di collegialità, fatta eccezione per le società del Gruppo che adottano un modello monocratico, e dispone di autonomi poteri di iniziativa e controllo, ai sensi dell'art. 6, comma 1, lett. b), del D.lgs. 231/2001, in conformità a quanto stabilito dal proprio regolamento interno. Le società garantiscono all'OdV le risorse necessarie per l'esecuzione dei compiti assegnati, nonché la possibilità di conferire, ove necessario, incarichi di natura meramente tecnica a soggetti terzi dotati di specifiche competenze.

Per l'efficace svolgimento delle proprie attività, l'Organismo di Vigilanza ha pieno accesso a tutte le informazioni aziendali utili allo svolgimento delle funzioni di verifica, analisi e controllo. Tutti i soggetti aziendali, compresi collaboratori e amministratori, sono tenuti a fornire risposte complete e tempestive alle richieste formulate dall'Organismo. La mancata evasione di tali richieste nei tempi previsti rappresenta una grave violazione disciplinare, suscettibile di sanzione fino al licenziamento per giusta causa. Le attività dell'OdV si articolano attraverso l'elaborazione di un piano annuale, definito in coerenza con i contenuti del Modello e in considerazione delle segnalazioni ricevute, degli eventi intercorsi, delle indicazioni emerse nel corso delle riunioni o sulla base di input forniti

dal Presidente, anche in corso d'opera. Tale piano può essere redatto a livello di Gruppo, confluendo nel piano di audit del Chief Audit Executive, in un'ottica di integrazione operativa tra i presidi di controllo.

L'OdV attua interventi di controllo sia programmati che straordinari, assicura un'attività di reporting periodico, in particolare con cadenza annuale, nei confronti del Consiglio di amministrazione e del Collegio Sindacale, e rileva eventuali scostamenti comportamentali tramite l'analisi dei flussi informativi e delle segnalazioni ricevute dai responsabili delle diverse funzioni aziendali. Mantiene inoltre un collegamento funzionale con gli Organismi di Vigilanza delle altre società del Gruppo, e segnala alle funzioni competenti eventuali violazioni del Modello, monitorando attraverso la Direzione Risorse Umane l'effettiva applicazione delle sanzioni disciplinari eventualmente previste o le motivazioni che ne abbiano impedito l'applicazione.

Tra i compiti dell'OdV rientrano anche la valutazione preventiva e il monitoraggio dei piani formativi e informativi aziendali, l'impulso all'aggiornamento continuo del Modello e dei suoi presidi, la formulazione di pareri in merito alla revisione delle politiche e delle procedure aziendali più rilevanti, con l'obiettivo di garantirne la coerenza con i principi del Modello, nonché la proposta di aggiornamenti del Codice Etico, per quanto di competenza. L'OdV può inoltre impartire istruzioni operative alle funzioni aziendali, che sono tenute a darne attuazione entro i termini indicati, nonché trasmettere indicazioni sulle azioni da intraprendere con urgenza per la riduzione del rischio reato, rispetto alle quali le funzioni preposte sono tenute a fornire riscontro sull'esito delle attività svolte.

In materia di whistleblowing (tema che sarà oggetto di approfondimento nel paragrafo successivo), l'Organismo di Vigilanza della capogruppo, unitamente al Collegio Sindacale, esercita un'attività di vigilanza sulla gestione del sistema e della piattaforma dedicata, il cui responsabile è individuato nel Chief Audit Executive. Quest'ultimo ha il compito di gestire le segnalazioni ricevute, inoltrando a ciascuna funzione o organo competente quelle non attinenti alla materia 231, e informando l'Organismo in forma collegiale delle segnalazioni ricevute.

L'Organismo di Vigilanza è nominato con delibera del Consiglio di amministrazione o, laddove previsto, dell'Organo di gestione di ciascuna società, previo parere del Collegio Sindacale. In fase di nomina, le società richiedono ai candidati il consenso alla verifica

del possesso dei requisiti professionali, morali e di indipendenza, ritenuti indispensabili per l'esercizio delle funzioni di vigilanza.

Costituiscono cause di ineleggibilità o decadenza dalla carica eventuali condanne, anche non definitive, per uno dei reati previsti dal D.lgs. 231/2001 e successive modifiche; condanne, con sentenza passata in giudicato, a pene comportanti l'interdizione, anche solo temporanea, dai pubblici uffici o dagli incarichi direttivi in persone giuridiche e imprese; nonché condanne non definitive per delitti non colposi con pena superiore a due anni di reclusione. Rientrano tra le cause di decadenza anche l'assunzione di incarichi ritenuti incompatibili con le funzioni di vigilanza e l'emergere di situazioni di conflitto di interesse, come nel caso in cui un soggetto ricopra contemporaneamente ruoli che possano pregiudicare la necessaria indipendenza o si trovi in rapporti diretti con clienti o partner della società.

Nel contesto dell'Organismo di Vigilanza, il conflitto di interessi è ravvisabile ogniqualvolta sussista una situazione in grado di compromettere l'autonomia e l'indipendenza del componente, o di creare una sovrapposizione tra il ruolo di "vigilato" e quello di "vigilante". Non sono tuttavia considerate incompatibili, per loro natura, né la carica di Sindaco né lo svolgimento di incarichi consulenziali connessi all'analisi dei rischi relativi alla normativa 231, in quanto funzionali all'attività di prevenzione.

I membri dell'OdV sono tenuti a segnalare tempestivamente qualsiasi situazione di conflitto di interessi che dovesse insorgere nel corso del mandato. In caso di composizione collegiale, l'Organismo prende atto della segnalazione e procede a valutarne la sussistenza e la compatibilità con il corretto svolgimento delle funzioni.

La revoca dell'incarico di un singolo componente o dell'intero OdV può avvenire esclusivamente per giusta causa, mediante deliberazione del Consiglio di amministrazione, previo parere del Collegio Sindacale. La proposta di revoca può essere formulata dal Presidente dell'Organismo e trasmessa all'Amministratore Delegato, il quale, salvo giustificato motivo, è tenuto a sottoporla al Consiglio. Nel caso in cui sia il Presidente dell'OdV a essere oggetto della proposta di revoca, l'iniziativa deve provenire dagli altri due componenti dell'Organismo.

Gli Organismi di Vigilanza della capogruppo e delle sue controllate riferiscono periodicamente in merito all'attuazione del Modello 231, all'eventuale emersione di criticità e all'esito delle attività svolte nell'ambito delle funzioni di vigilanza loro attribuite. Tali report vengono indirizzati al Consiglio di amministrazione e al Collegio Sindacale della rispettiva società, in un'ottica di trasparenza e responsabilizzazione diffusa.

A tal fine, ciascun Organismo di Vigilanza predispone una relazione annuale che illustra in modo dettagliato le attività svolte e i risultati conseguiti nel periodo di riferimento. Oltre a tale reporting strutturato, l'OdV provvede a trasmettere, con tempestività, segnalazioni puntuali nel caso di aggiornamenti normativi o giurisprudenziali significativi che rendano necessario un intervento di revisione sul Modello organizzativo, nonché in presenza di gravi violazioni riscontrate nel corso delle attività di verifica e controllo.

Nel caso in cui tali violazioni riguardino membri degli organi sociali, e in particolare uno o più componenti del Consiglio di amministrazione o del Collegio Sindacale, l'Organismo di Vigilanza informa direttamente i rispettivi Presidenti, affinché vengano avviati, secondo le rispettive competenze, eventuali approfondimenti istruttori. Sulla base degli esiti di tali approfondimenti, gli organi preposti valuteranno l'adozione dei provvedimenti opportuni, nel rispetto dei principi di imparzialità, proporzionalità e tutela dell'integrità del sistema di controllo. (Documentazione interna fornita dalla società: Strutturazione del modello organizzativo per la prevenzione dei reati , 2024)

In attuazione di quanto previsto dall'art. 6, comma 2, lettera d) del D.lgs. 231/2001 – secondo cui il Modello di organizzazione, gestione e controllo deve prevedere obblighi di informazione nei confronti dell'organismo deputato alla vigilanza – le società del gruppo hanno istituito un sistema strutturato di flussi informativi a favore dell'Organismo di Vigilanza, suddiviso in due macro-categorie: flussi generali e informazioni non strutturate, e informazioni strutturate, ad evento o periodiche.

a. Flussi informativi generali e informazioni non strutturate

Questa categoria comprende una serie di obblighi informativi generali, volti a garantire il costante presidio dell'efficace attuazione del Modello:

- L’obbligo generale, in capo ai responsabili delle funzioni aziendali, o ai referenti da essi delegati, di comunicare all’Organismo di Vigilanza tutte le informazioni ritenute utili per agevolare le attività di controllo e verifica sull’attuazione del Modello;
- La trasmissione, da parte dei responsabili di funzione, di una relazione contenente:
    - una descrizione dello stato di attuazione dei protocolli di prevenzione delle attività a rischio nell’ambito di propria competenza;
    - una sintesi delle attività di controllo svolte per verificarne l’effettiva applicazione, con indicazione di eventuali azioni di miglioramento intraprese;
    - proposte di aggiornamento o modifica dei protocolli o delle procedure di prevenzione;
- L’obbligo, sempre in capo ai responsabili di funzione, di informare l’Organismo in merito a:
    - l’emissione e/o aggiornamento di disposizioni interne, comunicazioni organizzative, linee guida o procedure aziendali;
    - l’eventuale aggiornamento del sistema delle deleghe e delle procure aziendali;
- L’obbligo, esteso a tutti i dipendenti, di segnalare direttamente all’Organismo, tramite l’indirizzo di posta elettronica dedicato o tramite la piattaforma di whistleblowing, qualsiasi violazione di norme, del Codice Etico o dei principi del D.lgs. 231/2001, nonché qualunque evento che possa costituire un potenziale rischio di responsabilità per l’ente. Tale obbligo riguarda anche comportamenti imputabili a soggetti terzi come organi sociali, agenti, consulenti, partner commerciali e finanziari.

b. Informazioni strutturate, ad evento o periodiche

Accanto ai flussi generali, sono previsti specifici flussi informativi strutturati, riferiti ai processi sensibili, che le funzioni aziendali devono trasmettere all’Organismo di

Vigilanza in base a criteri predefiniti. È compito dell'OdV definire e aggiornare periodicamente, per ciascuna area di rischio, le informazioni rilevanti necessarie all'esercizio delle sue funzioni di controllo. Tali informazioni possono essere:

- **Ad evento**: devono essere trasmesse tempestivamente al verificarsi di determinati eventi, quali ad esempio l'avvio di ispezioni da parte di autorità esterne, il verificarsi di un infortunio grave sul lavoro, oppure l'esito di una procedura di gara;
- **Periodiche**: devono essere comunicate con cadenza regolare (trimestrale, semestrale o annuale) e riguardano dati aggregati su eventi o operazioni rilevanti, come ad esempio l'assenza di infortuni sul lavoro, l'inserimento di nuovi fornitori o l'aggiudicazione di gare.

Per taluni eventi o operazioni, la valutazione ciclica del rischio consente di stabilire se le informazioni debbano essere comunicate in modo immediato oppure con frequenza periodica.

L'Organismo di Vigilanza valuta le segnalazioni ricevute e definisce i conseguenti provvedimenti, in coerenza con le disposizioni contenute nel Modello e secondo quanto previsto dalle procedure aziendali. Inoltre, l'OdV può richiedere ai responsabili di funzione una dichiarazione sottoscritta che attesti, con riferimento a un determinato periodo, l'assenza di eventi che avrebbero richiesto l'invio di informazioni. Nel contesto del Modello 231, le operazioni o decisioni aziendali vengono considerate "in deroga", "fuori procedura" o "fuori sistema" quando sono assunte al di fuori delle procedure aziendali standard o, nel caso di acquisti, quando non risultano tracciate nei sistemi di gestione formalizzati. Sebbene, in talune circostanze, il ricorso a modalità operative non standardizzate possa risultare necessario per evitare un'eccessiva rigidità gestionale e garantire continuità operativa, è comunque richiesto il rispetto di specifiche regole di controllo volte ad assicurare la trasparenza, la tracciabilità e la verificabilità ex post di tali scelte.

In particolare, il ricorso a operazioni in deroga è ammesso esclusivamente al ricorrere di presupposti giustificativi connessi a esigenze aziendali oggettive, tra cui:

- **Necessità e urgenza**, come nel caso di acquisti resi indispensabili da eventi straordinari o incidenti non compatibili con i tempi ordinari di selezione del fornitore;
- **Iperspecializzazione**, quando il fornitore o consulente risulta essere l'unico soggetto in grado di garantire uno specifico servizio o fornitura per via della sua elevata competenza tecnica;
- **Rapporto fiduciario**, in particolare nel caso di incarichi legali o consulenziali, o nella selezione di personale, laddove la fiducia sia riposta nel soggetto segnalante (ad esempio, un altro dipendente);
- **Esistenza di contratti quadro**, che legittimano il ricorso diretto a fornitori già convenzionati.

Ai fini della tracciabilità, ogni operazione in deroga deve essere supportata da un'adeguata documentazione, sia formale che informale, che ne attesti la correttezza e legittimità, in linea con il principio di accountability. A titolo esemplificativo, devono essere conservate le e-mail scambiate con il fornitore o altri documenti utili alla ricostruzione del processo decisionale. Il grado di rigore nella documentazione è proporzionato all'entità e al rischio dell'operazione, secondo quanto previsto dai protocolli relativi ai singoli processi sensibili e dalla regolamentazione interna dei flussi informativi.

L'Organismo di Vigilanza può inoltre richiedere alle funzioni aziendali un livello di tracciabilità più elevato per determinate tipologie di operazioni, nonché un aggiornamento continuo delle informazioni fornite.

Per quanto riguarda l'informativa all'OdV, le operazioni in deroga devono essere comunicate dalle funzioni responsabili all'Organismo, con tempistiche che possono variare in base alla rilevanza dell'operazione: immediatamente (ad evento) oppure con periodicità definita.

Nel caso di acquisti di beni o servizi, o incarichi di consulenza per importi superiori a determinate soglie stabilite periodicamente dall'OdV, è richiesto l'intervento del responsabile della compliance – ove membro dell'Organismo – che, a nome dell'OdV stesso, valida la correttezza del processo di acquisto e ne riferisce formalmente in

occasione della successiva riunione dell'Organismo. Qualora emerga una grave anomalia, il responsabile della compliance è tenuto a segnalare la situazione al Presidente dell'OdV, il quale può convocare una riunione straordinaria per un approfondimento specifico. Nel rispetto dell'autonomia funzionale degli Organismi di Vigilanza delle singole società del Gruppo, l'Organismo di Vigilanza della capogruppo svolge un ruolo di coordinamento, finalizzato a promuovere la diffusione e la condivisione, da parte delle controllate, della metodologia e degli strumenti adottati per l'attuazione del Modello 231. Pur mantenendo piena indipendenza nello svolgimento delle proprie funzioni, gli OdV delle società controllate beneficiano dunque di un presidio centrale che facilita l'allineamento operativo tra le diverse realtà del Gruppo, nel rispetto delle specificità organizzative di ciascuna entità giuridica.

L'Organismo di Vigilanza di ciascuna controllata è tenuto a informare l'Organismo di Vigilanza della capogruppo in merito all'attività svolta, ai fatti rilevati e all'eventuale adozione di provvedimenti disciplinari connessi a violazioni del Modello, nonché agli adeguamenti apportati allo stesso in conseguenza di mutamenti normativi, organizzativi o ambientali. In particolare, la relazione annuale indirizzata all'organo amministrativo della controllata è trasmessa anche all'OdV della capogruppo, a garanzia di un adeguato flusso informativo verticale.

Qualora, nell'esercizio delle proprie funzioni, l'Organismo di Vigilanza della capogruppo rilevi direttamente o riceva segnalazioni su circostanze, eventi o anomalie che possano avere impatto anche sul Modello organizzativo di una controllata, è tenuto a informare tempestivamente l'Organismo competente di quest'ultima, al fine di consentire un intervento puntuale e coordinato.

Per rafforzare l'efficacia del sistema di controllo preventivo e garantire una coerenza metodologica nell'applicazione dei Modelli 231, l'OdV della capogruppo può inoltre convocare riunioni congiunte con gli Organismi di Vigilanza delle società controllate, con finalità di scambio informativo, confronto operativo e allineamento sulle evoluzioni normative o organizzative rilevanti per l'intero Gruppo.

Tutte le informazioni, segnalazioni e documentazioni prodotte o ricevute nell'ambito dell'attuazione del Modello 231 vengono archiviate e conservate dall'Organismo di Vigilanza, con il supporto delle funzioni aziendali incaricate delle attività di segreteria

tecnica e verifica, in un apposito archivio che può essere in formato informatico e/o cartaceo, secondo le modalità previste dai protocolli interni.

Infine, nel trattamento e nella custodia dei dati contenuti nella documentazione di propria competenza, sia l'Organismo di Vigilanza della capogruppo che quelli delle società controllate si conformano integralmente a quanto previsto dal D.lgs. 196/2003 (Codice in materia di protezione dei dati personali) nonché alle ulteriori disposizioni nazionali e internazionali vigenti in materia di privacy e tutela dei dati personali. A tal proposito, l'atto di nomina dei componenti dell'Organismo di Vigilanza e delle figure interne che collaborano stabilisce formalmente la loro designazione quali soggetti autorizzati al trattamento dei dati, in conformità alla normativa sulla protezione dei dati personali, assicurando così la legittimità e la sicurezza delle operazioni di gestione documentale e informativa. (Documentazione interna fornita dalla società: Modello di Organizzazione, di Gestione e Controllo All.7 Flussi informativi verso l'ODV, 2024)

2.2.4 Strumenti di monitoraggio e reporting delle anomalie: Il WHISTLEBLOWING

Il 14 dicembre 2017 è stata pubblicata nella Gazzetta Ufficiale n. 291 la Legge 30 novembre 2017, n. 179, recante "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato". Tale provvedimento, il cui iter legislativo ha preso avvio nel 2015, ha rappresentato una riforma organica della disciplina sul whistleblowing, superando un quadro normativo fino ad allora frammentato e poco incisivo, come evidenziato anche dalla Commissione Europea.

La legge ha introdotto un sistema di tutela "a doppio binario", estendendo le garanzie sia ai lavoratori del settore pubblico — mediante modifiche al Testo Unico sul Pubblico Impiego — sia a quelli del settore privato, intervenendo in modo mirato sul Decreto Legislativo n. 231/2001.

Per il settore privato, in particolare, la riforma ha integrato l'articolo 6 del D.lgs. 231/2001, con l'intento di offrire protezione a dipendenti e collaboratori che, nello

svolgimento delle proprie mansioni, segnalino reati o irregolarità apprese in ambito lavorativo. I Modelli di organizzazione, gestione e controllo devono pertanto includere misure atte a prevenire qualsiasi atto ritorsivo o discriminatorio nei confronti del segnalante e a evitare un uso distorto dello strumento di segnalazione.

Elemento cardine della riforma è l'obbligo, previsto dall'art. 6, comma 2-bis, lettere a) e b), di predisporre canali informativi che consentano l'invio di segnalazioni circostanziate, basate su fatti specifici e riscontrabili, a tutela dell'integrità dell'ente.

Sebbene la norma non individui espressamente l'Organismo di Vigilanza come destinatario delle segnalazioni, la lettura sistematica del nuovo assetto normativo conferma il ruolo centrale che l'OdV è chiamato a svolgere nel sistema di whistleblowing previsto dal Decreto 231. In quanto organo preposto alla vigilanza sull'attuazione del Modello, l'OdV vedrà ampliati i propri poteri e le proprie responsabilità in fase di controllo, a seguito dell'aggiornamento dei modelli alle previsioni introdotte dalla Legge n. 179/2017.

È dovere di ogni dipendente e collaboratore segnalare tempestivamente, al proprio superiore o all'Organismo di Vigilanza della società di appartenenza, con le modalità messe a disposizione dall'ente, qualsiasi violazione, fondata su elementi di fatto concreti, di norme di legge, regolamenti aziendali, Codice Etico o disposizioni contenute nel Modello 231. A titolo esemplificativo e non esaustivo, possono costituire oggetto di segnalazione:

- furto o utilizzo improprio di beni aziendali;
- falsificazione o alterazione di documenti;
- manipolazione di dati contabili o omissione volontaria di registrazioni;
- distruzione, occultamento o uso improprio di documenti, file, attrezzature o archivi aziendali;
- falsa consuntivazione dei dati di commessa;
- atti di corruzione o induzione alla corruzione nei confronti di pubblici ufficiali, incaricati di pubblico servizio, esponenti di enti pubblici o governativi stranieri, oppure di dipendenti di clienti o potenziali clienti privati;

- atti di corruzione nei confronti di dipendenti del gruppo da parte di fornitori o potenziali fornitori;
- falsificazione di note spese;
- falsificazione delle presenze a lavoro;
- divulgazione di informazioni confidenziali a concorrenti;
- manomissione di apparati biomedicali.

Con l'obiettivo di uniformare le procedure trasversali della compliance a livello di gruppo, è stato adottato un servizio centralizzato per le comunicazioni, che consente la tracciabilità delle segnalazioni e rappresenta uno strumento di tutela e monitoraggio delle attività di verifica delle comunicazioni inviate. Tra questi si annoverano, oltre all'indirizzo e-mail dedicato agli Organismi di Vigilanza delle singole società, una piattaforma informatica esterna basata su tecnologia cloud. Tale piattaforma, accessibile tramite link aziendale, garantisce l'anonimato a condizione che la segnalazione non sia stata effettuata con dolo o colpa grave, qualora risultasse infondata. In linea con le best practices internazionali, il sistema prevede inoltre la possibilità di effettuare segnalazioni completamente anonime. È inoltre previsto un canale telefonico: contattando il numero indicato all'interno della piattaforma, un operatore incaricato raccoglie la comunicazione e attiva un ticket, che viene preso in carico dal Local Compliance Officer (nel caso dell'Italia, dall'Organismo di Vigilanza).

La gestione del processo è presidiata dal Chief Audit Executive e dal Group Compliance Committee, cui spetta il compito di assicurare il rispetto delle garanzie di riservatezza dell'identità del segnalante, nonché la protezione dei dati del soggetto segnalato e degli eventuali terzi coinvolti, nel rispetto della normativa vigente.

Costituiscono gravi violazioni disciplinari: i) il compimento di atti ritorsivi o discriminatori, diretti o indiretti, nei confronti del segnalante in buona fede o di coloro che collaborano alle attività di verifica; ii) la violazione delle misure di tutela previste per il segnalante; iii) l'invio doloso o gravemente colposo di segnalazioni infondate. Eventuali provvedimenti ritorsivi, come licenziamenti, demansionamenti, trasferimenti o sanzioni disciplinari adottati a seguito di una segnalazione, sono da ritenersi nulli e configurano altresì una grave violazione disciplinare.

In attuazione dell'art. 6 del Decreto 231, la capogruppo e analogamente la società esaminata, hanno adottato una policy specifica che disciplina il sistema di whistleblowing interno, denominato *Ethics Point*, il cui contenuto è parte integrante del Modello 231. Tale policy è pubblicata sul portale documentale aziendale e deve essere portata a conoscenza di tutti i destinatari del Modello.

Le segnalazioni, anche qualora effettuate in forma anonima, devono essere presentate in modo circostanziato, veritiero e fondato. L'anonimato non può essere utilizzato quale strumento per esprimere dissapori personali o conflitti tra dipendenti. Nelle segnalazioni è espressamente vietato l'utilizzo di espressioni ingiuriose, così come la diffusione di contenuti diffamatori o calunniosi. È inoltre considerato inammissibile il riferimento a fatti riguardanti esclusivamente la sfera privata dei soggetti, qualora non vi sia alcun collegamento, diretto o indiretto, con l'attività aziendale. Tali comportamenti risultano particolarmente gravi se riferiti ad abitudini personali, orientamenti sessuali, convinzioni religiose, politiche o filosofiche. Relativamente al contenuto delle segnalazioni. Il segnalante è tenuto a fornire tutti gli elementi di cui è a conoscenza e che risultino utili a consentire un'adeguata verifica dei fatti riportati. In particolare, la segnalazione deve includere alcuni elementi essenziali. Innanzitutto, è necessario che l'oggetto della segnalazione sia descritto in modo chiaro e preciso, con indicazione, ove conosciute, delle circostanze di tempo e di luogo in cui i fatti segnalati si sarebbero verificati o omessi. Inoltre, deve essere indicato il soggetto presunto autore della condotta illecita, riportandone, se possibile, le generalità oppure elementi utili alla sua identificazione, come la funzione o il ruolo aziendale ricoperto.

Oltre a tali elementi essenziali, il segnalante può facoltativamente fornire ulteriori informazioni, quali le proprie generalità nel caso in cui decida di non avvalersi dell'anonimato, l'indicazione di eventuali soggetti terzi in grado di riferire sui fatti descritti, l'eventuale documentazione a supporto della fondatezza della segnalazione, nonché qualsiasi altra informazione utile a facilitare l'attività di verifica e raccolta delle evidenze. Chiunque riceva una segnalazione, con qualsiasi mezzo, è tenuto a trasmetterla senza indugio all'Organismo di Vigilanza della società di appartenenza, utilizzando l'indirizzo e-mail dedicato o, in alternativa, il canale di whistleblowing predisposto. In tale processo deve essere garantita la riservatezza dell'identità del soggetto che ha fornito l'informazione, a tutela della sua integrità.

Le segnalazioni trasmesse attraverso il canale dedicato sono gestite dal Chief Audit Executive, il quale procede a una valutazione preliminare volta a verificarne la fondatezza e la plausibilità. Nel caso in cui il Chief Audit Executive ritenga che la segnalazione non sia rilevante ai fini del Modello Organizzativo, provvede a inoltrarla al Collegio Sindacale della società. Qualora, invece, la segnalazione riguardi direttamente (ad esempio, un fatto corruttivo) o indirettamente (come una situazione di conflitto di interessi) il Modello Organizzativo, il Chief Audit Executive, in funzione della gravità del contenuto, può eseguire un'istruttoria interna e trasmettere all'Organismo di Vigilanza un report conclusivo contenente i risultati delle verifiche effettuate.

Nel caso in cui la segnalazione riguardi dipendenti di società controllate estere, il Chief Audit Executive provvede a informare il Country Manager competente, trasmettendo comunque copia della segnalazione all'Organismo di Vigilanza della capogruppo.

L'Organismo di Vigilanza, nell'esercizio della propria autonomia e indipendenza, può decidere di svolgere direttamente gli accertamenti oppure di avvalersi del supporto di consulenti esterni. È inoltre compito dell'Organismo di Vigilanza e del Collegio Sindacale garantire che tutte le segnalazioni siano prese in carico, correttamente trattate e che siano adottate misure di tutela adeguate nei confronti del segnalante e degli altri soggetti coinvolti.

La responsabilità della corretta gestione delle segnalazioni pervenute tramite la piattaforma di whistleblowing è attribuita al Compliance Officer di Gruppo, che presiede il Compliance Committee. Si ricorda che la disciplina in materia di protezione dei dati personali, già oggetto di attenzione sin dal 2009, impone di bilanciare la tutela della riservatezza del segnalante con i diritti del soggetto segnalato. In questo senso, la Legge 179/2017, intervenendo anche sul D.lgs. 231/2001, ha richiesto agli enti che adottano un Modello di organizzazione, gestione e controllo di predisporre canali di segnalazione idonei, sicuri e circostanziati, basati su elementi di fatto precisi e concordanti, garantendo al contempo misure volte a prevenire atti ritorsivi o discriminatori. Tali obblighi devono oggi essere letti alla luce del Regolamento (UE) 2016/679 (GDPR), che richiede di definire in modo puntuale ruoli e responsabilità privacy dei soggetti coinvolti, adottare misure tecniche e organizzative per la sicurezza dei dati, regolare eventuali trasferimenti verso Paesi terzi, rispettare i principi di conservazione e disciplinare l'esercizio del diritto

di accesso agli atti da parte del soggetto segnalato. (Documentazione interna fornita dalla società: Modello di Organizzazione, di Gestione e Controllo All.8 Whistleblowing, 2024)

2.3 Analisi dei processi di gestione del rischio di frode

Il presente paragrafo è dedicato all'analisi dei processi attraverso cui la Società gestisce i rischi connessi alla possibilità di frodi, con particolare attenzione agli strumenti, ai controlli e alle responsabilità che concorrono alla loro prevenzione**.** L'analisi si basa sull'esame della documentazione fornita nel corso dell'incarico e su una serie di colloqui condotti con i responsabili delle principali funzioni aziendali, al fine di acquisire una visione chiara e dettagliata delle procedure operative effettivamente adottate. Alla luce di ciò, il capitolo successivo sarà invece interamente dedicato all'illustrazione e all'analisi dell'attività di revisione svolta, finalizzata a verificare in modo sistematico e documentato l'efficacia del sistema di prevenzione delle frodi attualmente in essere. In tale ambito, verranno descritte le fasi operative dell'incarico, le metodologie di audit adottate e i criteri di valutazione utilizzati, con particolare attenzione alla coerenza tra le procedure formalmente previste e le prassi effettivamente applicate.

2.3.1 Il risk management process adottato

È stata condotta un'analisi approfondita del risk management process adottato dalla Società nell'ambito dell'attuazione del Modello 231, con l'obiettivo di comprenderne la struttura, le modalità di applicazione e l'efficacia rispetto alla prevenzione dei reati presupposto. Tale processo, di seguito illustrato, si configura come un sistema strutturato, dinamico e interattivo, articolato in una serie di attività coordinate che si sviluppano lungo due macrofasi principali: la valutazione e la mitigazione del rischio. Questa modalità rispecchia il ciclo logico suggerito dallo standard ISO 31000:2018, che identifica la gestione del rischio come un processo iterativo e continuo, composto da attività integrate di identificazione, analisi, valutazione, trattamento e monitoraggio. Tale impostazione è volta a garantire che il risk management non sia un'attività isolata, ma un processo trasversale e costantemente aggiornato. (International Organization for Standardization, 2018)

La fase di valutazione comprende l'identificazione dei rischi potenziali, l'analisi della loro rilevanza e la pianificazione delle misure preventive necessarie per contenerne gli

effetti. Una volta tracciata la mappa dei rischi, si avvia la fase di mitigazione, che include l'attuazione concreta delle strategie individuate, la valutazione della loro efficacia, un'attività costante di monitoraggio e reporting, nonché la rivalutazione periodica dell'esposizione al rischio, alla luce degli eventuali cambiamenti nel contesto operativo o normativo. (The International Organization for Standardization, 2018)

Tutti i rischi individuati – sia nella fase di avvio, sia nel corso dell'aggiornamento del Modello – sono registrati all'interno della Mappatura dei Rischi, uno strumento operativo che consente di monitorare in modo sistematico eventi e fattori che potrebbero compromettere l'efficacia delle attività aziendali o l'integrità del sistema di controllo interno. Per ogni rischio-reato rilevante ai sensi del D.Lgs. 231/2001, sono stati definiti specifici protocolli preventivi, funzionali sia alla prevenzione, sia alla mitigazione nel caso in cui il reato si verifichi.

La Mappatura dei Rischi è costruita secondo una logica coordinata, che consente una lettura trasversale e coerente tra:

- la natura del rischio (tipologia di illecito presidiato);
- le funzioni aziendali coinvolte;
- i processi interessati;
- i protocolli e le procedure operative predisposte.

Ciascun rischio è identificato mediante una scheda univoca, strutturata secondo i seguenti elementi:

- ID del rischio (identificativo numerico progressivo);
- Riferimenti legislativi (norme applicabili ai sensi del D.Lgs. 231/2001);
- Funzioni aziendali interessate (unità organizzative direttamente coinvolte);
- Descrizione del reato;
- Riferimenti interni (documenti, modulistica o policy rilevanti);
- Valutazione del rischio (alto, medio o basso, sulla base di criteri qualitativi e quantitativi).

L’aggiornamento periodico della mappatura e la verifica dell’efficacia dei presìdi sono attività affidate all’Organismo di Vigilanza, che procede a un riesame ciclico oppure in occasione del verificarsi di nuovi eventi o mutamenti significativi, in conformità con quanto previsto dal Sistema di Gestione Integrato (SGI) adottato dalla Società. Questa impostazione rispecchia le migliori pratiche della letteratura recente, che descrive il risk mapping come uno strumento oggettivo, strutturato e visuale per individuare criticità nei processi aziendali, supportare la definizione delle priorità operative e rafforzare la governance. Disporre di una mappa dei rischi, infatti, non solo promuove un approccio proattivo alla mitigazione, ma contribuisce anche a obiettivi più ampi di miglioramento continuo e di gestione sostenibile del rischio, configurandosi come una necessità imprescindibile per qualsiasi impresa. (Abdelatif, A., Nettour, D., Chaib, R., Verzea, I., Bensehamdi, S., 2023). Nel paragrafo successivo, la mappatura verrà analizzata in maniera dettagliata, con specifico riferimento al processo di valutazione del rischio adottato dalla Società, al fine di evidenziarne criteri, metodologie e risultati. (Documentazione interna fornita dalla società: Modello di Organizzazione, di Gestione e Controllo Parte generale - Sezione Il processo di gestione del rischio, 2024)

2.3.2 Mappatura dei processi critici

L’adozione e il costante aggiornamento del Modello di Organizzazione, Gestione e Controllo da parte della società oggetto di analisi avvengono secondo una metodologia strutturata in fasi, ispirata alle Linee Guida emanate da Confindustria e alle migliori prassi operative promosse dalle principali associazioni di categoria. Tali Linee Guida, aggiornate nel 2021 e approvate dal Ministero della Giustizia, forniscono infatti un quadro metodologico di riferimento che sottolinea l’importanza di integrare i protocolli di prevenzione con sistemi di compliance evoluti, meccanismi di whistleblowing e misure di gestione delle nuove fattispecie di reato introdotte dal D.Lgs. 231/2001. Esse tracciano inoltre un percorso chiaro per la mappatura dei rischi e la progettazione dei presidi specifici, delineando principi operativi fondati sulla riduzione congiunta della probabilità e dell’impatto degli eventi illeciti. Tale approccio metodologico è finalizzato a garantire l’efficacia concreta del sistema, la solidità dei presìdi organizzativi e l’autorevolezza complessiva dell’impianto di prevenzione del rischio-reato, in linea con i principi di

legalità e responsabilità su cui si fonda il D.Lgs. 231/2001. Nel dettaglio, il processo metodologico implementato si compone di passaggi distinti e coerenti, finalizzati alla costruzione di un sistema di controllo efficace e proporzionato al profilo di rischio dell'ente e articolato come segue:

- Identificazione dei reati rilevanti: partendo dal catalogo dei reati presupposto di cui al D.Lgs. 231/2001, sono stati selezionati quelli effettivamente pertinenti rispetto ai processi e alle attività caratteristiche del business aziendale, distinguendo tra condotte finali e comportamenti strumentali (ad esempio, violazioni contabili che possano facilitare condotte corruttive).
- Analisi delle attività sensibili (as-is analysis): è stata effettuata un'analisi dei processi e delle aree aziendali all'interno delle quali è possibile configurare la commissione dei reati individuati, con valutazione del rischio basata su criteri sia quantitativi sia qualitativi.
- Gap analysis: attraverso un confronto tra la situazione attuale e i requisiti di un sistema di controllo interno "ottimale", sono state individuate le azioni di miglioramento necessarie per rafforzare l'idoneità preventiva del Modello 231, con particolare riferimento ai presìdi procedurali, organizzativi e sistemici.
- Valutazione integrata del rischio: oltre al rischio sanzionatorio previsto dal decreto, la valutazione ha tenuto conto anche del potenziale danno reputazionale e degli impatti indiretti, in coerenza con un approccio esteso alla gestione della compliance strategica.

(Confidustria , 2021) (Confindustria Dispositivi Medici, 2024)

All'interno del percorso metodologico sopra descritto si colloca la mappatura dei rischi reato adottata dalla società. A seguito dell'analisi condotta sul contesto organizzativo e operativo, finalizzata a individuare le aree aziendali potenzialmente esposte al rischio di commissione dei reati contemplati dal D.Lgs. 231/2001, la società ha circoscritto le attività a rischio alle seguenti categorie di illecito: reati contro la Pubblica Amministrazione, reati societari e finanziari, reati in materia di salute e sicurezza dei lavoratori, reati informatici (relativi a hardware, software e dati), e reati ambientali.

Tutte le suddette categorie risultano astrattamente applicabili al contesto operativo dell'ente. Tuttavia, in linea con l'obiettivo della presente tesi, l'attenzione sarà rivolta in particolare ai reati societari e finanziari, in quanto strettamente connessi ai temi della frode contabile, dell'informativa economico-finanziaria e della funzione di prevenzione e rilevazione delle irregolarità affidata al fraud audit.

Il documento di mappatura dei rischi oggetto di analisi, reso disponibile nel corso dell'esperienza di revisione svolta presso la società EY, costituisce uno strumento operativo centrale per l'individuazione, la classificazione e la gestione dei profili di rischio connessi alla responsabilità amministrativa dell'ente ai sensi del D.Lgs. 231/2001. La mappatura è organizzata in formato tabellare e consente una lettura sistematica dei reati rilevanti, offrendo per ciascuna fattispecie una serie di informazioni strutturate secondo le seguenti sezioni:

- *riferimento normativo (articolo del Codice Civile e richiamo all'art. del decreto 231),*
- *descrizione della fattispecie di reato così come disciplinata nel modello interno,*
- *funzioni aziendali coinvolte nella gestione o nel rischio,*
- *processi operativi interessati,*
- *descrizione sintetica del rischio concretamente ipotizzato (con esempi operativi),*
- *valutazione qualitativa del rischio (bassa, media, alta),*
- *misure di prevenzione e controllo adottate, che includono protocolli, istruzioni operative, flussi informativi e Codici interni (etico, anticorruzione, ecc.).*

Tale impostazione metodologica risulta coerente con le linee guida in ambito Enterprise Risk Management (ERM), che raccomandano l'utilizzo di template per registrare le informazioni sui rischi. Tali strumenti, che possono assumere la forma di tabelle, registri di rischio, fogli di calcolo o sistemi informatici dedicati, consentono di raccogliere in maniera strutturata i dati necessari e, quando richiesto, di fornire descrizioni dettagliate per facilitare una valutazione completa e per favorire un processo decisionale più consapevole e documentato. (National Institute of Standards and Technology, 2024) (Airmic, Alarm, IRM, 2010).

Di seguito si riporta una sintesi dei principali rischi-reato individuati nella mappatura del Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001 adottato dalla società esaminata, limitatamente a quelli maggiormente rilevanti ai fini dell'analisi del rischio di frode contabile.

Tabella 1 – Elaborazione dai documenti forniti dalla società: fattispecie rilevanti ex D.Lgs. 231/2001, riferimenti normativi e valutazione qualitativa del rischio attribuita dalla società

Fattispecie di reato	Riferimento normativo	Valutazione del rischio
False comunicazioni sociali	Art. 2621 e 2622c.c.	ALTA
Formazione fittizia del capitale	Art. 2632 c.c.	MEDIA
Impedito controllo	Art. 2625 c.c.	ALTA
Illecita influenza sull'assemblea	Art. 2636 c.c.	MEDIA
Ostacolo all'esercizio delle funzioni delle autorità di vigilanza	Art. 2638 c.c.	MEDIA

La tabella è stata elaborata a partire dalla documentazione interna messa a disposizione durante l'incarico di revisione svolto e presenta, per ciascuna fattispecie selezionata, il relativo riferimento normativo e la valutazione qualitativa del rischio attribuita dalla società.

La classificazione riportata nella tabella è il risultato dell'applicazione della matrice di valutazione dei rischi adottata dalla società nell'ambito del proprio Modello 231, così come ricavata dai documenti aziendali analizzati. Tale matrice si fonda sull'incrocio di due dimensioni fondamentali:

- **Probabilità di accadimento**, ossia la stima della possibilità che la specifica fattispecie di reato possa verificarsi, calcolata tenendo conto di variabili quali la

vulnerabilità dei processi, il livello di esposizione al rischio del settore di attività e l'efficacia dei presìdi organizzativi e procedurali già esistenti;

- **Impatto potenziale**, che misura le conseguenze derivanti dall'eventuale verificarsi della condotta illecita, includendo non solo i profili economici e patrimoniali, ma anche quelli legali, reputazionali e di compliance normativa.

L'incrocio di queste due dimensioni genera una griglia di valutazione qualitativa che attribuisce a ciascun rischio un livello sintetico (basso, medio o alto). La matrice permette dunque di trasformare una valutazione descrittiva in un modello comparabile e strutturato, in grado di supportare decisioni operative e strategiche.

Nello specifico:

- un **rischio alto** corrisponde a scenari caratterizzati da un'elevata probabilità di accadimento e da impatti significativi, tali da richiedere l'adozione di controlli rafforzati, meccanismi di monitoraggio continuo e l'eventuale revisione dei protocolli di prevenzione;
- un **rischio medio** rappresenta situazioni in cui la probabilità o l'impatto assumono un livello intermedio: in questi casi, pur non essendo necessari controlli di massima intensità, occorre predisporre presìdi strutturati e un monitoraggio periodico che garantisca la tracciabilità delle attività;
- un **rischio basso** è associato a fattispecie con ridotta probabilità di accadimento e impatti limitati, per le quali risultano proporzionati controlli standard, accompagnati da misure preventive generali.

Questa metodologia di valutazione si inserisce in un quadro ampiamente riconosciuto a livello internazionale. La letteratura recente conferma, infatti, come le matrici probabilità–impatto rappresentino strumenti largamente adottati per classificare i rischi in base alla loro probabilità e alle conseguenze potenziali sugli obiettivi aziendali (Acebes F. , 2024). Allo stesso tempo, gli standard internazionali di riferimento, come la ISO/IEC 31010:2019 – *Risk management e Risk assessment techniques*, sottolineano l'importanza di strumenti che permettano di stimare in modo sistematico la probabilità e l'impatto degli

eventi rischiosi, costituendo un supporto essenziale al processo di valutazione e trattamento del rischio.

In tale prospettiva, la matrice adottata dalla società non ha una funzione meramente descrittiva, ma rappresenta un presidio operativo fondamentale: consente infatti di tradurre l'analisi dei rischi in criteri oggettivi e comparabili, di allineare la valutazione alle priorità organizzative e di fornire all'Organismo di Vigilanza uno strumento concreto per il riesame ciclico e l'aggiornamento della mappatura, in coerenza con i principi della normativa 231 e delle best practices internazionali.

Sulla base della classificazione riportata nella tabella, vengono di seguito illustrate nel dettaglio le singole fattispecie di reato individuate.

In linea con il focus tematico del presente elaborato, una delle fattispecie centrali emerse dalla mappatura dei rischi e oggetto di analisi è rappresentata dal reato di false comunicazioni sociali, disciplinata dagli articoli 2621 e 2622 del Codice Civile. Questo reato rappresenta la forma più diretta e strutturata di frode contabile, in quanto consiste nella comunicazione, sia all'interno dell'impresa che verso l'esterno, di informazioni economico-finanziarie non veritiere, suscettibili di alterare la rappresentazione della realtà aziendale.

Secondo quanto previsto dalla normativa, risultano penalmente perseguibili gli amministratori, i direttori generali, i sindaci e i liquidatori che, con l'intento di ingannare soci o pubblico e di procurare a sé o ad altri un ingiusto profitto, espongano fatti materiali non rispondenti al vero oppure omettono informazioni rilevanti nei bilanci, nelle relazioni o nelle altre comunicazioni obbligatorie previste dalla legge, con riferimento alla situazione economica, patrimoniale o finanziaria della società o del gruppo.

Il reato previsto dall'art. 2621 c.c. si configura anche in assenza di un danno effettivo, mentre l'art. 2622 c.c. ne richiede la realizzazione concreta, sotto forma di pregiudizio patrimoniale per soci o creditori. In entrambi i casi, la punibilità è esclusa se l'effetto della falsità determina una variazione del risultato economico (al lordo delle imposte) non superiore al 5%, o del patrimonio netto non superiore all'1%; oppure se si tratta di valutazioni estimative che si discostano in misura non superiore al 10% rispetto alla stima corretta.

Ai fini della configurabilità del reato, le informazioni false o omesse devono avere un impatto sensibile sulla rappresentazione della situazione aziendale, e possono riguardare anche beni amministrati per conto di terzi. La condotta deve inoltre essere sorretta da dolo specifico, ossia dalla volontà di ingannare i destinatari delle comunicazioni per ottenere un indebito vantaggio. [6]

Nella mappatura dei rischi fornita dalla società, viene riportato, a titolo esemplificativo, il caso in cui un dirigente preposto alla redazione dei documenti contabili ignori intenzionalmente una segnalazione ricevuta dal responsabile amministrativo relativa alla necessità di un accantonamento al fondo svalutazione crediti. L'omissione comporta la sovrastima dell'attivo patrimoniale e un miglioramento artificiale del risultato d'esercizio, con l'effetto di occultare una perdita potenzialmente rilevante, che potrebbe condurre alla violazione di obblighi civilistici in tema di adeguatezza del capitale.

Le possibili modalità realizzative del reato possono includere:

- la manomissione o l'alterazione dei dati contabili presenti nei sistemi informativi aziendali, con l'obiettivo di rappresentare in modo falsato la situazione patrimoniale, economica e finanziaria, ad esempio tramite l'inserimento di voci di bilancio inesistenti o la modifica dei valori reali;
- la determinazione artificiosa di poste valutative in bilancio, quali accantonamenti o rettifiche, in accordo con gli amministratori, come nel caso della sopravvalutazione o sottovalutazione dei crediti e dei relativi fondi;
- l'inserimento in bilancio di poste non valutative non corrispondenti alla realtà, oppure l'occultamento di fatti economicamente rilevanti, che alterano la rappresentazione della situazione aziendale effettiva;
- l'omissione di informazioni obbligatorie, la cui comunicazione è richiesta dalla legge, relative alla condizione economica, patrimoniale o finanziaria dell'impresa.

Il rischio associato a tale condotta è valutato come alto, alla luce della gravità delle conseguenze potenziali sul piano informativo, reputazionale e giuridico, in quanto una falsa rappresentazione dei dati di bilancio compromette l'affidabilità complessiva del

[6] **Codice Civile**, **art. 2621 e art. 2622** – *False comunicazioni sociali*

sistema di reporting, mina la fiducia degli stakeholder interni ed esterni e può determinare rilevanti impatti negativi non solo in termini di responsabilità penali e civili per gli esponenti aziendali coinvolti, ma anche in termini di perdita di credibilità del management e deterioramento delle relazioni con investitori e finanziatori; la classificazione tiene inoltre conto di una probabilità di accadimento non trascurabile, legata alla complessità e al grado di discrezionalità che caratterizzano i processi contabili. I presìdi di controllo interni adottati dalla società comprendono un insieme articolato di misure volte a garantire la correttezza e la trasparenza dei dati contabili. In particolare, sono previsti: programmi di formazione periodica per i responsabili di funzione sui principi contabili e sulle normative di riferimento, con l'obiettivo di assicurare un aggiornamento costante delle competenze; controlli sistematici sui flussi finanziari e sulla documentazione amministrativa, che consentono di rilevare tempestivamente anomalie o discordanze; l'adozione di un sistema procedurale formalizzato basato su protocolli specifici, volto a disciplinare in maniera puntuale i processi di registrazione e rendicontazione; la segregazione delle funzioni chiave per ridurre il rischio di conflitti di interesse e garantire indipendenza nei controlli; l'utilizzo di strumenti informatici che permettano la tracciabilità delle operazioni contabili e la rilevazione di eventuali modifiche sospette ai dati inseriti nei sistemi aziendali; nonché audit interni periodici finalizzati a verificare il rispetto delle procedure e a individuare aree di miglioramento.

Le funzioni aziendali coinvolte nella gestione di tale rischio operano su livelli diversi e con ruoli complementari. Il consiglio di amministrazione, cui spetta la supervisione delle politiche aziendali e l'approvazione dei documenti contabili; gli amministratori delegati, responsabili dell'attuazione operativa delle direttive e del coordinamento delle funzioni interessate; l'ufficio amministrazione e finanza, che cura gli adempimenti contabili e la predisposizione dei prospetti amministrativi e finanziari; il collegio sindacale, con compiti di vigilanza sul rispetto delle normative e delle procedure interne; e la società di revisione, chiamata a fornire un controllo indipendente sull'attendibilità dei bilanci e delle informazioni economico-finanziarie.

A questa fattispecie si affianca il reato di formazione fittizia del capitale, disciplinato dall'articolo 2632 del Codice civile. Secondo quanto riportato nella mappatura, il rischio si concretizza nel caso in cui gli amministratori o i soci conferenti procedano a una sopravvalutazione dolosa dei conferimenti in natura o dei crediti, oppure pongano in

essere pratiche di attribuzione artificiosa del capitale, attraverso, ad esempio, sottoscrizioni reciproche di azioni o quote. Il rischio è valutato come medio, poiché, pur trattandosi di condotte in grado di incidere in maniera rilevante sull'assetto patrimoniale della società e sulla trasparenza della rappresentazione contabile, la probabilità di accadimento è considerata contenuta, in ragione della specificità delle circostanze in cui tali pratiche possono manifestarsi e della presenza di controlli esterni e interni che contribuiscono a mitigarne la realizzazione. La classificazione intermedia riflette quindi la combinazione tra un impatto potenzialmente significativo — con il pericolo di compromettere l'equilibrio tra conferimenti effettivi e capitale dichiarato e di ridurre l'affidabilità complessiva delle informazioni fornite agli stakeholder — e una probabilità ritenuta non molto elevata. I presìdi individuati consistono in una chiara strutturazione delle responsabilità tra le diverse funzioni aziendali coinvolte, volta ad assicurare la tracciabilità delle decisioni e la separazione dei compiti; nello svolgimento di riunioni mensili tra Consiglio di Amministrazione, Collegio Sindacale e Organismo di Vigilanza, finalizzate a garantire un costante monitoraggio delle operazioni di conferimento e delle relative valutazioni; nonché nella predisposizione di rapporti informativi periodici al Consiglio di Amministrazione, al fine di consentire un'analisi puntuale e tempestiva delle operazioni potenzialmente a rischio e favorire l'adozione di eventuali misure correttive.

Il reato di impedito controllo, disciplinato dall'articolo 2625 del Codice civile, è incluso nella mappatura dei rischi reato in quanto potenziale condotta strumentale all'occultamento di irregolarità contabili. Tale fattispecie si configura ogniqualvolta venga ostacolato o impedito lo svolgimento delle attività di controllo e/o di revisione, attribuite per legge ai soci, agli organi di controllo societario o alla società incaricata della revisione legale dei conti.

In particolare, si fa riferimento a condotte poste in essere da parte degli amministratori, che agiscano con intenzione elusiva nei confronti delle richieste avanzate dal Collegio Sindacale o da altri organi di vigilanza, al fine di non fornire la documentazione richiesta, o di presentarla in modo parziale, alterato o incompleto. Rientrano nella fattispecie anche comportamenti non trasparenti, reticenti o dilatori, che, pur non configurando un rifiuto esplicito, finiscono comunque per ostacolare il corretto esercizio dei poteri di verifica.

La condotta può essere integrata mediante l'occultamento di documenti, l'adozione di artifici volti a ostacolare le attività ispettive, o ancora attraverso la mancata risposta a richieste formali. A titolo esemplificativo, rientrano tra i comportamenti rilevanti l'esibizione parziale o manipolata di libri sociali, o l'adozione di prassi ostruzionistiche mirate a rallentare o deviare l'accesso alle informazioni.

L'importanza di questo reato nell'ambito del fraud audit è rilevante, in quanto l'impedimento delle attività di controllo può costituire un chiaro indicatore di rischio rispetto alla volontà di occultare anomalie nei bilanci o violazioni contabili sistemiche. Il comportamento doloso assume una gravità ancor maggiore qualora determini un danno effettivo ai soci, circostanza che comporta un aumento della pena. La procedibilità è subordinata alla querela di parte.

Il rischio associato a tale condotta è valutato come alto all'interno della mappatura, tenuto conto dell'impatto potenzialmente sistemico che un comportamento ostruzionistico verso gli organi di controllo può generare, compromettendo la trasparenza delle informazioni, l'effettività dei meccanismi di vigilanza e la solidità complessiva della governance societaria. La valutazione tiene conto anche del fatto che la probabilità di simili condotte, pur non necessariamente elevata, non può essere esclusa, poiché l'ostacolo all'attività di controllo rappresenta una modalità tipica con cui si tenta di celare irregolarità contabili o gestionali.

Il sistema di prevenzione attivato dalla società si articola in una serie di misure coordinate, che includono: la predisposizione di rapporti periodici al Consiglio di Amministrazione, al fine di garantire un flusso costante e tempestivo di informazioni utili alle decisioni; l'adozione di procedure formalizzate che disciplinano i flussi informativi tra i diversi organi societari, così da ridurre il rischio di interruzioni o manipolazioni nella comunicazione interna; l'applicazione sistematica dei principi espressi nel Codice Etico, quale strumento volto a orientare i comportamenti aziendali e a promuovere la cultura dell'integrità e della collaborazione; nonché la sensibilizzazione del personale attraverso momenti formativi e richiami puntuali alle policy interne, con l'obiettivo di prevenire atteggiamenti reticenti o non collaborativi.

Le funzioni aziendali coinvolte includono il CdA, l'Ufficio Amministrazione e Finanza, il Collegio Sindacale e la Società di Revisione, soggetti tutti potenzialmente limitati

nell'efficacia della loro azione qualora il reato si concretizzi, poiché un comportamento ostruzionistico può ostacolare la piena accessibilità alle informazioni rilevanti, ridurre la trasparenza nei flussi comunicativi interni ed esterni, compromettere la tempestività degli interventi correttivi e, in ultima analisi, indebolire l'effettività dei controlli predisposti dall'assetto di governance.

All'interno della mappatura è inoltre presente il reato di illecita influenza sull'assemblea, disciplinato dall'articolo 2636 del Codice Civile. Il rischio considerato riguarda il caso in cui l'Amministratore Delegato, con il supporto dei propri collaboratori, presenti all'assemblea documenti alterati, incompleti o non veritieri, con lo scopo di influenzarne fraudolentemente le decisioni. Pur non configurandosi necessariamente come una falsificazione del bilancio, questa condotta implica un uso distorto dell'informazione contabile quale leva per manipolare il processo deliberativo. Il rischio è classificato come medio, poiché, pur trattandosi di un comportamento potenzialmente idoneo a compromettere la correttezza e la legittimità delle deliberazioni assembleari, la probabilità di accadimento non è considerata elevata, in quanto circoscritta a specifiche situazioni e mitigata dalla presenza di organi di vigilanza e di procedure di controllo interno. La classificazione intermedia riflette quindi un bilanciamento tra la gravità delle possibili conseguenze — che riguardano la lesione dei diritti degli azionisti, la perdita di fiducia nei confronti degli organi gestionali e la compromissione della trasparenza societaria — e una frequenza stimata come non diffusa. Il presidio individuato si basa su una combinazione di strumenti normativi e organizzativi. Da un lato, la Parte Speciale del Modello 231 disciplina in maniera puntuale i comportamenti da adottare per prevenire condotte manipolative, imponendo regole di tracciabilità e completezza della documentazione assembleare e prevedendo specifici obblighi di collaborazione nei rapporti con gli organi sociali. Dall'altro, il Codice Etico aziendale sancisce i principi di trasparenza, correttezza e lealtà che devono orientare l'azione degli amministratori e dei collaboratori, ponendosi come riferimento per prevenire deviazioni comportamentali.

Infine, la mappatura considera anche il reato di ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza, previsto dall'articolo 2638 del Codice Civile. L'esempio operativo riportato riguarda la trasmissione alla Consob di documenti volontariamente redatti in modo ambiguo o incompleto, soprattutto in occasione di operazioni straordinarie, come l'acquisizione di partecipazioni. Sebbene questa condotta non

determini necessariamente un falso bilancio, essa compromette la trasparenza verso gli organi di vigilanza e può ostacolare l'individuazione di anomalie contabili. Il rischio è valutato come medio, in quanto le conseguenze potenziali di tali condotte possono incidere in maniera significativa sulla regolarità delle operazioni societarie e sulla fiducia delle autorità nei confronti della società, con possibili ripercussioni reputazionali e giuridiche. Tuttavia, la probabilità di accadimento non è considerata elevata, essendo mitigata dalla presenza di procedure di comunicazione formalizzate e da obblighi di legge che impongono trasparenza nei rapporti con gli organismi di vigilanza. La classificazione intermedia riflette quindi un equilibrio tra l'impatto rilevante che la mancata collaborazione con le autorità può generare e il grado di presidio già esistente a livello organizzativo. I presìdi previsti comprendono un insieme di misure volte ad assicurare correttezza, tracciabilità e completezza delle informazioni trasmesse agli organi di vigilanza. Tra questi si annoverano: protocolli anticorruzione, finalizzati a ridurre il rischio di pratiche elusive o opache; controlli documentali, che garantiscono la coerenza e l'integrità dei dati forniti; procedure di gestione delle deleghe, volte a chiarire ruoli e responsabilità interne; attività di vigilanza sui collaboratori esterni , al fine di monitorarne l'affidabilità; e, infine, flussi informativi formalizzati tra Consiglio di Amministrazione, Collegio Sindacale e Organismo di Vigilanza, destinati a favorire la tempestiva condivisione delle informazioni rilevanti e a prevenire omissioni o alterazioni nei rapporti con le autorità.

L'analisi condotta sulle aree aziendali ha permesso poi all'organizzazione di individuare i principali processi e attività operative che risultano maggiormente esposti al rischio di commissione di reati, con particolare attenzione alle fattispecie societarie. L'approccio adottato non si è limitato a un esame formale delle procedure, ma ha considerato la natura delle attività svolte, il grado di discrezionalità connesso alle decisioni operative, nonché l'impatto che eventuali comportamenti irregolari potrebbero avere sulla rappresentazione della realtà economico-finanziaria dell'impresa. Particolare attenzione è stata posta alle aree che incidono direttamente sulla qualità dei dati contabili e sulla trasparenza dei rapporti con gli organi di vigilanza, poiché esse rappresentano i punti più sensibili nel garantire affidabilità e correttezza all'intero sistema di controllo societario. In questa prospettiva, sono considerate ad elevata sensibilità le funzioni che concorrono, anche indirettamente, alla formazione dell'informativa economico-finanziaria e alla gestione

dei flussi comunicativi tra gli organi di governance e di controllo. Tali funzioni assumono un ruolo critico perché, se non presidiate adeguatamente, possono diventare il veicolo principale di condotte illecite, in grado di compromettere la trasparenza gestionale e la fiducia degli stakeholder.

Tra le aree ritenute a rischio sono state segnalate:

- tutti i processi aziendali coinvolti nella gestione e nella produzione dei dati contabili che alimentano il bilancio d'esercizio;
- le attività di redazione del bilancio civilistico e consolidato, della relazione sulla gestione e delle ulteriori comunicazioni previste dalla normativa societaria;
- i flussi informativi tra gli organi societari, in particolare tra Consiglio di amministrazione, Collegio Sindacale, Organismo di Vigilanza e società di revisione;
- le attività di controllo interno, incluse le procedure di rilevazione e registrazione contabile;
- le operazioni straordinarie o gestionali che incidono direttamente sulla struttura e sull'integrità del capitale sociale.

In relazione a queste aree poi sono state individuate una serie di attività operative definite come "sensibili", in quanto potenzialmente esposte a condotte illecite di natura societaria. Esse comprendono:

- la gestione anagrafica dei fornitori e dei clienti;
- la contabilità fornitori e clienti;
- la gestione dei rapporti infragruppo, inclusi i finanziamenti interni;
- la definizione e aggiornamento del piano dei conti;
- l'intera gestione della contabilità generale;
- la predisposizione e approvazione del bilancio d'esercizio;
- la gestione delle relazioni con i soci, la società di revisione, il Collegio Sindacale e l'Organismo di Vigilanza.

Si precisa che l'elenco delle attività sensibili sopra riportato è oggetto di costante aggiornamento, nell'ambito delle attività periodiche di risk mapping e risk assessment condotte dalla società, anche su iniziativa dell'Organismo di Vigilanza. Eventuali modifiche o integrazioni, dovute a variazioni organizzative, evoluzioni normative o nuove fattispecie di reato rilevanti ai sensi del D.Lgs. 231/2001, comportano un aggiornamento del Modello stesso e sono quindi sottoposte all'approvazione del Consiglio di amministrazione.

L'individuazione delle aree e delle attività sensibili costituisce dunque il punto di partenza per la definizione di un sistema di prevenzione strutturato, volto a ridurre l'esposizione dell'organizzazione ai rischi emersi. Una volta mappati i processi più critici, si è resa necessaria l'adozione di misure organizzative, gestionali e comportamentali capaci di assicurare trasparenza, tracciabilità e correttezza nello svolgimento delle attività aziendali. In quest'ottica, la società ha sviluppato un quadro organico di principi guida, divieti e procedure operative, destinati a presidiare in maniera mirata le aree a rischio e ad orientare i comportamenti di tutti i soggetti coinvolti, come sarà illustrato nel paragrafo seguente. (Documentazione interna fornita dalla società: Modello di Organizzazione, di Gestione e Controllo All. 2 Mappatura dei processi critici) (Documentazione interna fornita dalla società: Modello di Organizzazione, di Gestione e Controllo Parte Speciale "Reati Societari")

2.3.3 Principi guida, divieti e procedure operative implementate a presidio delle aree a rischio

Ai fini del rispetto delle Linee Guida di riferimento, il sistema di controllo interno della società, nelle aree operative a rischio e in quelle strumentali, deve ispirarsi a una serie di principi fondamentali, volti a garantire l'efficacia, la trasparenza e la coerenza dei meccanismi di prevenzione. La letteratura e la prassi più recenti confermano infatti che l'efficacia dei modelli organizzativi richiede l'adozione di procedure interne formalizzate, la tracciabilità delle attività e la definizione di flussi informativi chiari verso gli organi di controllo, così da assicurare un reale presidio dei rischi e una concreta funzione preventiva. (Cassa Depositi e Prestiti , 2025)

In primo luogo, si richiede un'adeguata separazione delle responsabilità: le attività operative, le funzioni autorizzative e i controlli devono essere attribuiti a soggetti differenti, al fine di evitare concentrazioni decisionali e garantire la reciproca indipendenza tra chi esegue, chi approva e chi verifica.

Il sistema dei poteri di firma deve risultare formalmente definito e coerente con le responsabilità assegnate, sia sotto il profilo organizzativo che gestionale, ed esercitato entro soglie di valore prestabilite, in modo da assicurare il rispetto dei limiti autorizzativi.

Un ulteriore principio guida è rappresentato dalla chiarezza e semplicità organizzativa: ruoli, compiti e responsabilità devono essere definiti in modo univoco e comprensibile, così da permettere una corretta esecuzione delle attività e dei controlli correlati.

Altro elemento essenziale è l'imparzialità operativa: i destinatari del Modello 231 sono tenuti a operare con diligenza e neutralità, evitando ogni situazione che possa generare conflitti di interesse, anche solo potenziali, rispetto agli interessi della società o dei suoi stakeholder.

Fondamentale è infine il principio di tracciabilità delle attività: ogni operazione significativa e ogni controllo effettuato devono poter essere ricostruiti a posteriori, attraverso una documentazione adeguata, preferibilmente in formato digitale. La corretta archiviazione dei documenti assume, pertanto, un ruolo centrale nella gestione della conformità.

Si raccomanda, infine, di ridurre il più possibile l'incidenza dei controlli manuali, favorendo sistemi automatizzati e procedure informatizzate che aumentino l'affidabilità del controllo stesso e ne riducano la dipendenza dall'errore umano.

In linea con i principi guida sopra enunciati, il Modello di Organizzazione, Gestione e Controllo adottato dalla società definisce precise regole comportamentali applicabili alle aree aziendali considerate a rischio, con particolare riferimento ai reati societari. Tali disposizioni sono vincolanti per tutti i soggetti coinvolti nella governance e nella gestione dell'ente, tra cui gli organi sociali, il Country Manager, l'Amministratore Delegato, i componenti del Consiglio di amministrazione, i Direttori e Dirigenti responsabili, nonché i dipendenti e collaboratori, in relazione alle rispettive funzioni e responsabilità. A tali

soggetti, nel rispetto delle normative vigenti e delle politiche aziendali interne, è richiesto di attenersi costantemente ai seguenti principi e alle procedure:

- Piena conoscenza e rispetto delle regole di corporate governance vigenti nella Società e nel Gruppo di appartenenza;
- Padronanza della struttura organizzativa, delle linee gerarchiche e del sistema di controllo di gestione;
- Conformità alle normative e alle procedure che disciplinano il sistema amministrativo, contabile e di reporting interno;
- Assunzione delle decisioni aziendali in linea con le norme di legge, lo statuto societario, il Modello 231 e il Codice Etico;
- Corretta segregazione delle responsabilità operative e decisionali, al fine di evitare concentrazioni di potere e sovrapposizioni di ruoli nelle attività sensibili;
- Formalizzazione delle responsabilità di gestione, coordinamento e controllo, accompagnata da una chiara definizione delle linee di dipendenza e delle mansioni;
- Tracciabilità del processo decisionale e documentazione delle fasi autorizzative;
- Coerenza tra i poteri di firma conferiti e le responsabilità effettivamente attribuite, garantendo una trasparente comunicazione verso l'esterno;
- Assegnazione dei poteri in funzione della rilevanza economica e della criticità delle operazioni da autorizzare;
- Separazione tra le funzioni operative, contabili e di controllo, affinché le attività siano sempre soggette a verifica indipendente;
- Selezione dei consulenti esterni sulla base di criteri di competenza, autonomia e affidabilità, con motivazione documentata della scelta;
- Coerenza tra sistemi di incentivazione e obiettivi effettivamente raggiungibili, in rapporto al ruolo e alle responsabilità assegnate;

- Conformità al complesso normativo interno, comunitario e internazionale applicabile.

Accanto ai principi generali di comportamento, il modello adottato prevede un insieme di divieti espressamente formulati al fine di prevenire condotte che possano anche solo potenzialmente integrare fattispecie di reato. Tali divieti, che riguardano sia le attività direttamente sensibili sia quelle strumentali, si configurano come presidi fondamentali a tutela dell'integrità dei processi aziendali e della correttezza dell'informazione societaria. L'obiettivo del Modello non è tanto quello di elencare in maniera esaustiva tutte le condotte vietate, quanto piuttosto quello di delineare un quadro chiaro e condiviso di comportamenti attesi. All'interno di tale perimetro, ciascun soggetto, in base al proprio ruolo e alle proprie responsabilità, è chiamato ad agire in modo conforme alle normative vigenti e alle procedure interne, contribuendo così alla costruzione di una cultura aziendale improntata alla compliance e all'integrità. In questa prospettiva, i divieti si configurano come uno strumento di tutela preventiva, non solo nei confronti delle fattispecie penalmente rilevanti, ma anche rispetto a condotte solo potenzialmente illecite o opache, che potrebbero compromettere l'affidabilità dell'informativa societaria e la credibilità dell'ente nel suo complesso. Infine, è posto un forte accento sul dovere di garantire un flusso informativo chiaro, tempestivo e completo nei confronti dell'Organismo di Vigilanza. In questo ambito, costituiscono condotte vietate:

- l'omissione o la mancata comunicazione di informazioni rilevanti, comprese eventuali modifiche al sistema delle deleghe e dei poteri;
- la violazione delle procedure previste dal Modello;
- qualsiasi azione finalizzata ad ostacolare o eludere l'attività di controllo esercitata dagli organi preposti.

Il Modello evidenzia inoltre che, sebbene alcune attività aziendali non siano direttamente esposte al rischio di commissione di reati societari, esse potrebbero comunque rappresentare ambiti nei quali si creano disponibilità economiche o condizioni favorevoli a finalità illecite, come atti corruttivi o pratiche gestionali opache. Per questo motivo, è previsto un rafforzamento dei controlli anche su tali aree, in un'ottica di prevenzione

estesa e coerente con i principi di legalità, trasparenza e responsabilità che ispirano l'intero sistema 231.

Nel contesto delle procedure adottate dalla società per prevenire il rischio di illeciti contabili o l'occultamento di risorse extracontabili, particolare attenzione è riservata alla regolamentazione dei principali cicli operativi, con specifico riferimento ai processi di acquisto e approvvigionamento (ciclo passivo) e alla gestione dei ricavi da attività contrattuali e servizi (ciclo attivo). Entrambi i cicli sono oggetto di dettagliate procedure interne che prevedono controlli a più livelli, con l'obiettivo di garantire tracciabilità, correttezza documentale e segregazione delle responsabilità.

Per quanto concerne il ciclo passivo, tutte le fasi relative agli approvvigionamenti e ai pagamenti sono rigidamente disciplinate. In particolare, dopo l'emissione dell'ordine, la fornitura viene sottoposta a un primo controllo fisico da parte dell'area ricevente, che attesta l'effettiva ricezione della merce. Segue una seconda verifica di tipo documentale da parte dell'area contabile, la quale confronta ordine, documenti di trasporto e fattura. In caso di incongruenze, il pagamento viene automaticamente sospeso, e potrà essere riattivato soltanto previa autorizzazione del responsabile dell'area logistica e approvvigionamenti.

Anche il processo di gestione della fatturazione passiva è regolato da procedure stringenti, che prevedono l'intervento di almeno due soggetti, impedendo che una singola persona – anche se in posizione apicale – possa disporre da sola un pagamento. È inoltre esclusa ogni deroga alle procedure previste, salvo per importi minimi definiti.

Tali cautele hanno l'obiettivo di prevenire la formazione di fondi extracontabili o l'effettuazione di uscite non autorizzate, presidiando così in modo efficace uno degli ambiti più vulnerabili rispetto al rischio di frode. A rafforzare ulteriormente il sistema concorre l'attività continuativa dell'area Amministrazione e Finanza, che effettua controlli secondo il modello di controllo contabile e amministrativo previsto a livello di gruppo.

Nonostante la solidità del sistema, il Modello ribadisce l'obbligo per tutti i soggetti aziendali di segnalare tempestivamente qualsiasi anomalia o sospetto riconducibile a condotte illecite. Le eventuali segnalazioni devono essere indirizzate al Consiglio di

amministrazione e, per conoscenza, trasmesse all'Organismo di Vigilanza, a conferma della centralità del flusso informativo interno nel prevenire fenomeni fraudolenti. Parallelamente, anche il ciclo attivo è disciplinato secondo modalità che mirano a garantire la correttezza della rilevazione dei ricavi e l'affidabilità dell'informativa economico-finanziaria. I ricavi della società (come verrà approfondito nel capitolo seguente) si articolano in due categorie principali: quelli ricorrenti da canone, connessi a contratti pluriennali per la gestione integrata delle apparecchiature biomediche, e quelli spot, legati a interventi straordinari richiesti dal cliente.

Nel caso dei ricavi da canone, il processo ha inizio con l'aggiudicazione di una gara e la successiva approvazione dell'offerta da parte del cliente. Tale approvazione costituisce il presupposto per la stipula contrattuale e per l'avvio della fatturazione. Operativamente, i Capi Area dislocati sul territorio inseriscono, tramite un'applicazione web, i dati relativi alle commesse di propria competenza, che vengono poi trasmessi al Responsabile della Fatturazione Attiva. L'Ufficio Contratti e Contabilità provvede alla verifica delle informazioni inserite, controllando la coerenza tra tariffe, canoni e condizioni contrattuali. In questa fase si intende prevenire il rischio di errata fatturazione, attraverso il confronto tra contratto, anagrafica cliente e fattura generata.

Una volta validati i dati, questi vengono caricati nel gestionale di fatturazione. Per i clienti della Pubblica Amministrazione, la registrazione contabile può avvenire solo dopo la ricezione dell'avviso di consegna tramite SDI. La contabilizzazione è accompagnata da un controllo formale volto ad assicurare la corretta imputazione contabile dei ricavi. A fine mese, viene inoltre calcolato l'accantonamento per fatture da emettere (FDE), che durante l'anno resta extracontabile, mentre nel mese di dicembre è rilevato contabilmente. L'intera procedura si conclude con una quadratura mensile tra il gestionale e la contabilità generale, effettuata con il supporto della funzione di Controllo di Gestione.

L'adozione di controlli chiave formali, la presenza di più livelli autorizzativi e la sistematizzazione delle fasi di emissione, contabilizzazione e verifica dei ricavi hanno dunque l'obiettivo di garantire la trasparenza del processo e minimizzare il rischio di anomalie contabili. Allo stesso tempo tali presidi mirano a rafforzare l'idoneità del Modello 231 nel prevenire condotte fraudolente nell'ambito della gestione.

Nel presente capitolo è stato analizzato il sistema di controllo interno implementato dalla società, così come descritto nei documenti aziendali forniti e approfondito attraverso specifici colloqui con il management. L'obiettivo è stato quello di ricostruire l'impianto organizzativo e procedurale adottato in relazione alle aree a rischio, con particolare riferimento alle fattispecie rilevanti ai sensi del D.Lgs. 231/2001. Il capitolo successivo è invece dedicato all'applicazione delle metodologie di *fraud audit* al caso aziendale, con l'obiettivo di esaminare in che modo il sistema di controllo interno, descritto fino a questo momento sulla base della documentazione e delle valutazioni interne fornite dalla società, trovi concreta attuazione sul piano operativo. Se in questa fase l'analisi si è concentrata sui rischi individuati dall'azienda stessa, la trattazione prosegue ora assumendo la prospettiva del revisore esterno. In tale ottica vengono esaminati i processi contabili e i cicli aziendali maggiormente esposti, al fine di valutare la capacità dei presidi di controllo di gestire le aree di vulnerabilità rilevate. (Documentazione interna fornita dalla società: Linee Guida di Gruppo per il Modello 231 - Sezione Principi di comportamento nelle principali aree di rischio, 2024)

CAPITOLO 3 – ATTIVITA' DI FRAUD AUDIT SUL CASO AZIENDALE: VERIFICHE, RISULTATI E OPPORTUNITÀ DI MIGLIORAMENTO

3.1 Descrizione dell'attività di revisione condotta

L'analisi sviluppata in questa sezione si concentra sull'applicazione operativa dei principi di fraud audit al caso aziendale oggetto di studio. Nel capitolo precedente è stato ricostruito il sistema di controllo interno sulla base della documentazione aziendale e delle informazioni fornite dalla società, al fine di restituire un quadro il più possibile fedele alla configurazione formale dei presìdi organizzativi. In tale ricostruzione si è posto un accento particolare sugli aspetti maggiormente coerenti con l'obiettivo della tesi, ossia la valutazione dell'efficacia del sistema di controllo interno nella prevenzione delle frodi, così da predisporre il necessario punto di partenza per le verifiche illustrate nelle pagine che seguono.

In questa prospettiva, lo studio intende ora colmare il divario tra la dimensione teorica e quella pratica, verificando in che misura le strutture di governance e i protocolli interni siano effettivamente in grado di contrastare comportamenti opportunistici o pratiche distorsive. Il lavoro è stato condotto adottando la prospettiva del revisore esterno, secondo un approccio metodologico articolato in tre fasi: (i) identificazione delle aree e dei processi maggiormente esposti a rischi di frode, (ii) analisi delle modalità di controllo e dei presìdi adottati, (iii) formulazione di un giudizio sull'affidabilità complessiva del sistema di controllo interno e individuazione di possibili opportunità di miglioramento.

Le verifiche sono state condotte applicando le procedure tipiche della revisione contabile – che verranno di seguito esaminate in dettaglio – comprendenti l'analisi dei processi aziendali più sensibili, l'esame delle aree a maggior rischio di frode, la valutazione dell'adeguatezza dei controlli interni e il riscontro delle informazioni contabili. A queste attività si sono affiancati colloqui con i referenti aziendali e un costante confronto con il team di revisione, che hanno consentito di approfondire criticità operative e di valutare la reale efficacia dei controlli adottati. Questo percorso ha permesso di superare una lettura meramente formale delle policy, ricostruendo un quadro più realistico e dinamico delle modalità con cui l'organizzazione affronta i rischi di frode.

In definitiva, l'obiettivo perseguito è stato quello di fornire un'analisi quanto più aderente alla realtà organizzativa e alle prassi effettivamente adottate, evidenziando sia i punti di forza sia le aree suscettibili di miglioramento, così da contribuire a una valutazione critica e costruttiva del sistema di controllo interno in ottica antifrode.

Alla luce di queste premesse, il paragrafo che segue (3.1.1) illustra nel dettaglio le metodologie di revisione adottate, mentre il successivo (3.1.2) descrive le fasi operative del processo di audit, fornendo una rappresentazione ordinata e completa del percorso seguito nello svolgimento delle attività.

3.1.1 Metodologie di revisione adottate

L'incarico di revisione contabile, conferito per il triennio 2024–2026, è stato impostato come una revisione full scope, ossia un'attività estesa a tutte le principali aree di bilancio e finalizzata a garantire una copertura completa e sistematica dell'intero set informativo. Questo approccio, che si distingue dalle revisioni limitate o dalle review per l'ampiezza e la profondità delle verifiche, consente al revisore di ottenere una ragionevole sicurezza sull'assenza di errori significativi, siano essi derivanti da frodi o da comportamenti non intenzionali.

L'attività si è svolta in conformità agli International Standards on Auditing (ISA), che impongono al revisore di adottare un approccio risk-based audit. In particolare, lo standard ISA 315 (Revised 2019) – Identifying and Assessing the Risks of Material Misstatement stabilisce che la pianificazione della revisione deve basarsi sulla comprensione del contesto aziendale, del modello di business, dei processi rilevanti e del sistema di controllo interno, così da identificare e valutare i rischi di errori materiali a livello di bilancio e di singole asserzioni. (IAASB, 2019) Lo standard ISA 330 – The Auditor's Responses to Assessed Risks disciplina invece le modalità con cui il revisore deve rispondere ai rischi individuati, prevedendo l'applicazione di test di controllo e di procedure sostanziali calibrati in base alla probabilità e alla gravità degli errori stimati. (IAASB, 2015) Infine, l'ISA 200 – Overall Objectives of the Independent Auditor chiarisce che l'obiettivo complessivo della revisione, ossia fornire una ragionevole sicurezza sull'assenza di errori materiali, si consegue proprio attraverso l'adozione di un approccio basato sul rischio, che rende la pianificazione e l'esecuzione delle verifiche proporzionata ai rischi individuati. (IAASB, 2020)

In coerenza con tali principi, la metodologia di revisione ha previsto in primo luogo una fase di comprensione del business e dei principali cicli aziendali, che ha consentito di acquisire una conoscenza approfondita dell'impresa sotto il profilo operativo, organizzativo e di governance. Tale fase preliminare si è rivelata essenziale non solo per inquadrare correttamente l'attività svolta, ma anche per comprendere la natura delle transazioni tipiche, l'ambiente di controllo e i potenziali fattori di vulnerabilità connessi alla gestione dei processi chiave. Dall'analisi dei cicli aziendali sono stati inoltre estrapolati i *What Could Go Wrong* (WCGW), ossia i potenziali scenari di errore che possono verificarsi nei diversi passaggi operativi. Tale attività ha permesso di valutare in che misura i controlli interni fossero effettivamente in grado di presidiare i rischi emersi, fornendo così indicazioni utili per la determinazione del livello di *control risk* nei diversi processi. In conformità a quanto previsto dallo ISA 330 – *The Auditor's Responses to Assessed Risks*, questa valutazione del rischio di controllo riveste un ruolo essenziale poiché consente di calibrare la portata delle verifiche sostanziali, modulandone natura ed estensione in funzione dell'affidabilità dei presidi. Nel contesto del presente elaborato, l'analisi dei controlli interni è stata utilizzata con una finalità specifica: fornire elementi per esprimere un giudizio sull'efficacia complessiva del sistema di controllo interno in ottica antifrode. A valle di tale analisi, sono stati definiti i principali parametri quantitativi di revisione, che costituiscono un passaggio imprescindibile nella pianificazione dell'attività: la *significatività di pianificazione (planning materiality, PM)*, *l'errore tollerabile (tolerable error, TE)* e la *soglia di rilevazione (SAD nominal amount)*. La *planning materiality* rappresenta la soglia oltre la quale un errore, considerato singolarmente o in aggregato, può ragionevolmente ritenersi in grado di influenzare le decisioni degli utilizzatori del bilancio; il *tolerable error* definisce l'ammontare massimo di errore accettabile per ciascun conto significativo, senza che ciò comprometta la correttezza complessiva del bilancio; infine, il *SAD nominal amount* costituisce la soglia minima oltre la quale ogni anomalia deve essere comunicata, anche qualora non sia materialmente rilevante. (Documentazione interna di revisione: PM TE and SAD nominal amount, 2024) L'integrazione tra parametri quantitativi e considerazioni qualitative sui rischi ha consentito di individuare i conti significativi, vale a dire quelle poste di bilancio che, oltre a superare determinate soglie di materialità, presentano un più elevato livello di *inherent risk*. Quest'ultimo rappresenta il rischio intrinseco di errori materiali, legato alla

natura delle operazioni, alla complessità delle valutazioni o al grado di soggettività insito in specifiche stime contabili, indipendentemente dall'esistenza di controlli interni. Su queste aree, oggetto di successiva analisi, si è quindi concentrata l'attività di audit in coerenza con la logica rischio–risposta prevista dagli ISA; nel presente elaborato, tuttavia, l'esame è stato condotto con l'obiettivo specifico di valutare i profili di esposizione a possibili fenomeni fraudolenti e di verificare, in tale prospettiva, l'efficacia del sistema di controllo interno. Le aree di bilancio selezionate non sono quindi considerate soltanto per la loro rilevanza quantitativa e qualitativa ai fini della revisione contabile, ma vengono analizzate soprattutto per comprendere se i presidi di controllo siano idonei a ridurre il rischio di manipolazioni o anomalie nelle registrazioni contabili.

Le attività di audit si sono quindi sviluppate secondo un approccio integrato, che ha combinato la valutazione dei controlli interni con procedure sostanziali volte a verificare la correttezza delle scritture contabili e la loro adeguata rappresentazione in bilancio. Tale impostazione è stata condotta in linea con le linee guida contenute nell'*Handbook of International Quality Management, Auditing, Review, Other Assurance, and Related Services Pronouncements*, che costituisce uno dei principali corpus normativi e tecnici di riferimento a livello internazionale per l'attività di revisione, volto a promuovere uniformità, coerenza e qualità delle verifiche. In questo modo si è garantita coerenza metodologica, tracciabilità e qualità dell'intero processo di revisione. (IAASB, 2024)

In questa cornice metodologica, un riferimento specifico di rilievo è stato rappresentato dal Group Accounting Manual (GAM), che costituisce la guida per le unità di reporting nella predisposizione del reporting package consolidato in conformità alle politiche contabili di gruppo. Le disposizioni del manuale, coerenti con i principi contabili internazionali IAS/IFRS emanati dallo IASB e adottati dall'Unione Europea, garantiscono uniformità nei criteri di rilevazione e valutazione, richiedendo in assenza di norme specifiche l'applicazione del giudizio professionale. Ciò consente di assicurare che le informazioni contabili rappresentino fedelmente la situazione patrimoniale, economica e finanziaria, riflettano la sostanza delle operazioni e siano redatte secondo principi di neutralità, prudenza e completezza, risultando così utili e affidabili per gli utilizzatori finali. (Documentazione interna di revisione: Group Accounting Manual, 2024) In sintesi, la metodologia adottata ha permesso di collocare l'attività di revisione entro un quadro solido e comparabile, capace di integrare principi internazionali, parametri di

pianificazione e strumenti operativi di gruppo. Tale approccio ha favorito una più efficace focalizzazione sulle aree a maggiore rilevanza e, nel contesto del presente elaborato, ha posto le basi per un'analisi volta a verificare l'efficacia del sistema di controllo interno in ottica antifrode. Le attività descritte nei paragrafi successivi, pertanto, non ricostruiscono l'intero processo di revisione contabile, ma comprendono le fasi preliminari di analisi del contesto aziendale e del modello di business, insieme alle procedure ritenute più significative per valutare i rischi e l'adeguatezza dei controlli. In questo modo è stato possibile mantenere una visione complessiva dell'impresa e, al tempo stesso, perseguire l'obiettivo specifico dell'elaborato, ossia formulare un giudizio sull'efficacia dei presidi di controllo interno nella prevenzione e rilevazione di frodi. (Documentazione interna di revisione: SRM_Summary Review Memorandum, 2024) (Documentazione interna di revisione: Group Accounting Manual, 2024)

3.1.2 Fasi operative del processo di audit

Come di consueto negli incarichi di revisione, l'attività ha preso avvio con la fase di interim, sviluppata sulla base dell'impianto normativo e metodologico delineato in precedenza, che ha rappresentato il quadro di riferimento per la pianificazione e per l'impostazione delle procedure di verifica. In tale contesto, è stata acquisita una conoscenza approfondita della realtà aziendale, considerata passaggio preliminare necessario per definire un approccio di revisione coerente e fondato. L'analisi si è concentrata innanzitutto sulla comprensione del business profile e sulla valutazione delle leggi e dei regolamenti applicabili, potenzialmente in grado di influenzare direttamente o indirettamente la predisposizione del bilancio e la relativa informativa.

Tra i principali riferimenti normativi è emerso il ruolo dei principi contabili internazionali IAS/IFRS, la cui continua evoluzione, attraverso l'emanazione di nuovi standard e l'aggiornamento di quelli esistenti, è suscettibile di determinare modifiche nella rappresentazione contabile dei fatti di gestione e, conseguentemente, nelle disclosure fornite agli stakeholders. Un ulteriore aspetto di rilievo è costituito dal Codice degli Appalti. Pur non operando in un mercato rigidamente regolamentato, la Società, intrattenendo rapporti con enti pubblici, deve attenersi alle prescrizioni normative in materia di appalti, disciplinate dal D. Lgs. n. 50/2016, con successive modifiche. Tale normativa, relativa all'aggiudicazione dei contratti di concessione, degli appalti pubblici e di quelli nei settori speciali dell'acqua, dell'energia, dei trasporti e dei servizi postali,

ha introdotto un quadro volto a razionalizzare e ridurre le molteplici disposizioni pregresse, con l'obiettivo di accrescere la certezza del diritto, semplificare i procedimenti e ridurre i tempi delle procedure di gara e di realizzazione delle opere pubbliche. Al tempo stesso, essa ha perseguito l'obiettivo di garantire maggiore certezza del diritto, favorendo la digitalizzazione dei processi, l'accesso delle piccole e medie imprese, nonché una più puntuale disciplina degli appalti legati a situazioni di emergenza, alla sicurezza e alla tutela dei beni culturali. Particolare attenzione è stata inoltre rivolta alla sostenibilità ambientale ed energetica, attraverso l'introduzione di criteri premiali per i progetti a minore impatto. Nel complesso, il Codice mira a rendere le procedure più trasparenti e tracciabili, rafforzando gli strumenti di prevenzione e contrasto dei fenomeni corruttivi. Accanto a tali disposizioni, sono stati considerati anche i regolamenti che incidono indirettamente sul bilancio e sull'informativa, tra cui i principi emanati dallo IASB e il D. Lgs. 231/2001 in materia di responsabilità amministrativa degli enti. Come già descritto nel capitolo precedente, la normativa introduce una responsabilità che, sebbene formalmente qualificata come amministrativa, presenta in realtà una natura sostanzialmente penalistica, poiché la colpevolezza dell'ente si configura nei casi in cui un reato commesso da organi o dipendenti sia riconducibile a scelte imprenditoriali, all'assenza di un modello organizzativo idoneo o a un deficit di vigilanza da parte degli organi di controllo. Alla luce di ciò, l'impresa oggetto di revisione si è dotata di un Modello Organizzativo coerente con le linee guida elaborate dalle associazioni di categoria, successivamente aggiornato a seguito di operazioni straordinarie e sottoposto a costante revisione per recepire le nuove disposizioni normative. Con riferimento alle policies and procedures aziendali, è stato rilevato che l'impresa dispone di un ufficio tecnico deputato a garantire il rispetto della normativa sugli appalti pubblici, mentre il CFO presidia costantemente l'evoluzione dei principi contabili internazionali, valutando i potenziali impatti che eventuali modifiche agli standard potrebbero produrre sul bilancio. (Documentazione interna di revisione: Form laws and regulations, 2024) Nell'ambito della fase conoscitiva è stata dedicata particolare attenzione alla comprensione delle attività principali e della strategia aziendale. L'impresa analizzata si configura come operatore di riferimento a livello nazionale nella gestione integrata delle tecnologie biomediche ed è parte di un gruppo di dimensione paneuropea che riveste un ruolo primario nel settore dei servizi destinati all'healthcare. La capillare presenza sul

territorio, unita alla costante interazione con i clienti e con le istituzioni di settore, consente di consolidare una posizione competitiva di rilievo e di fungere da interlocutore privilegiato nello sviluppo di nuovi modelli di business legati all'erogazione di servizi. La struttura dimensionale e organizzativa permette inoltre la partecipazione a tutte le principali gare pubbliche, la cui sistematica mappatura offre un quadro dettagliato dell'andamento del mercato, sia sotto il profilo dei volumi sia con riferimento alla tipologia di servizi offerti.

Un'attenzione particolare è stata rivolta alla direzione tecnica, la cui impostazione è orientata non solo a soddisfare in modo sempre più completo le esigenze della clientela, ma anche a perseguire l'efficientamento dei processi interni, con l'obiettivo di salvaguardare e incrementare la redditività complessiva. La Società ha 5 sedi in Italia (Sede Legale ed amministrativa a Roma, Sedi Operative a Milano, Torino, Gualdo Tadino, Bologna e Vicenza), 1 Centro di Eccellenza orientato al *training & testing* sulle apparecchiature ad alto contenuto tecnologico, 2 Centri altamente specializzati nelle riparazioni endoscopiche e radiologiche e centinaia di laboratori specialistici attivi direttamente presso le strutture sanitarie. La forza lavoro, costituita da oltre milleseicento dipendenti, garantisce la gestione, la manutenzione e la sicurezza di un parco tecnologico di più di novecentomila apparecchiature medicali, che spaziano dai dispositivi più semplici fino alle tecnologie più complesse, distribuite in oltre trecento strutture sanitarie localizzate sia in Italia sia in altri Paesi europei. L'offerta dell'impresa si articola in un ventaglio ampio e diversificato di servizi, che coprono l'intero ciclo di vita delle tecnologie biomediche e si estendono fino allo sviluppo di soluzioni innovative per la sanità digitale. Una componente centrale è rappresentata dall'ingegneria clinica, che comprende la manutenzione multivendor delle apparecchiature biomediche, svolta sia in forma preventiva sia correttiva e straordinaria, nonché le verifiche di sicurezza pianificate o successive alle riparazioni. Rientrano inoltre in quest'area la gestione e il controllo delle apparecchiature ad alto contenuto tecnologico, l'erogazione di consulenza tecnica a supporto delle decisioni gestionali e strategiche delle strutture sanitarie, l'implementazione di sistemi informatizzati per la gestione del parco tecnologico e delle attività manutentive, oltre alla formazione specialistica rivolta a tecnici e operatori sanitari.

Accanto a ciò, un ruolo rilevante è svolto dai servizi di radiodiagnostica, che spaziano dalla progettazione e realizzazione di reparti di diagnostica per immagini fino alla fornitura, installazione e manutenzione di apparecchiature radiologiche ad elevata complessità tecnologica, con l'aggiunta di un supporto gestionale che prevede la messa a disposizione di personale qualificato, sia per attività operative sia per programmi di formazione.

Un ulteriore ambito operativo è costituito dai workshop specialistici, che trovano la loro sede principale nell'hub centrale dedicato alla manutenzione on call. Tali laboratori sono caratterizzati da un'elevata specializzazione, in particolare nella riparazione di dispositivi e componenti di meccanica pneumatica ospedaliera, comprendendo strumenti complessi quali tavoli operatori, turbine odontoiatriche, manipoli e trapani elettrici, nonché l'intera gamma di strumentazione chirurgica.

A queste attività si affianca lo sviluppo di sistemi e processi innovativi per la sanità digitale, volti a favorire l'evoluzione dei modelli di gestione dei servizi sanitari attraverso l'integrazione di nuove tecnologie. L'impresa eroga inoltre servizi di telemedicina mediante centri altamente specializzati, operativi in modalità continuativa 24 ore su 24, in grado di fornire assistenza domiciliare telematica. Tali centri si avvalgono di soluzioni tecnologiche avanzate che assicurano continuità di servizio, affidabilità, capacità di scalabilità e costante innovazione.

Infine, l'azienda dispone di un background completo a supporto dei blocchi operatori e delle sale operatorie integrate, mettendo a disposizione servizi avanzati e soluzioni tecnologiche che consentono di rispondere efficacemente alle esigenze cliniche e gestionali delle strutture ospedaliere più complesse.

Nell'ambito dell'analisi preliminare, particolare attenzione è stata rivolta ai cambiamenti intervenuti nella natura dell'impresa e nel suo contesto operativo, al fine di valutarne i potenziali effetti sull'attività di revisione. In questa prospettiva, sono stati esaminati gli eventi di business che hanno caratterizzato l'esercizio in esame, con l'obiettivo di comprendere le operazioni straordinarie e gli sviluppi organizzativi che possono avere un impatto sul profilo di rischio e, conseguentemente, sull'attività di revisione. È emersa in particolare la costituzione, avvenuta nel corso del 2024, di una società consortile a responsabilità limitata con capitale sociale pari a 10.000 euro, finalizzata a consentire ai

soci di ottimizzare le proprie capacità tecniche, amministrative e gestionali attraverso una gestione congiunta. L'oggetto sociale è ampio e riguarda l'organizzazione e la gestione di operazioni commerciali, industriali, finanziarie e immobiliari ritenute necessarie per il perseguimento delle finalità consortili. La ripartizione delle quote sociali ha visto l'impresa oggetto di revisione assumere la partecipazione di maggioranza relativa, affiancata da altri soci con quote proporzionali al capitale sottoscritto. Successivamente, l'attenzione è stata rivolta all'analisi delle condizioni di mercato del periodo. È emerso che l'impresa mantiene una forte presenza sia a livello nazionale che europeo, grazie alla partecipazione sistematica a numerose gare pubbliche. Oltre alle attività ricorrenti, sono in corso progetti innovativi che prevedono la realizzazione di partenariati pubblico-privati in diverse aree del Paese, con quote di partecipazione variabili in funzione delle singole iniziative. Tali operazioni, ancora in fase di implementazione, rappresentano un elemento significativo della strategia di sviluppo, orientata a consolidare il posizionamento nel mercato e a diversificare i modelli di business. Sono stati successivamente esaminati i principali rischi di business a cui l'impresa risulta esposta. Un primo profilo riguarda il rischio di mercato e di prezzo, strettamente connessi alla partecipazione alle gare pubbliche e alla successiva gestione delle commesse aggiudicate. La società ha predisposto un sistema di mitigazione fondato su una struttura interna solida, composta da un ufficio gare e da un ufficio legale di consolidata esperienza, chiamati a presidiare le verifiche preliminari di natura tecnica e legale, nonché la predisposizione di offerte congrue dal punto di vista economico. A ciò si affianca una direzione tecnica altamente qualificata, che assicura la corretta esecuzione delle commesse in corso, garantendo il rispetto degli obblighi contrattuali e riducendo l'esposizione a potenziali contestazioni. La presenza di un modello di organizzazione, gestione e controllo e di un codice etico aggiornato costituisce un ulteriore presidio volto a rafforzare i meccanismi di prevenzione dei rischi. Un secondo profilo rilevante è rappresentato dal rischio di credito, legato ai ritardi nei pagamenti che caratterizzano, in particolare, la clientela pubblica. Per fronteggiare tale criticità, l'impresa ha implementato un articolato sistema di monitoraggio e recupero dei crediti e ha fatto ricorso a strumenti finanziari quali contratti di factoring stipulati con diversi istituti. È stato inoltre considerato il rischio di liquidità, che risulta mitigato sia dall'appartenenza al gruppo di riferimento sia dal ricorso a operazioni di factoring pro-soluto, le quali garantiscono risorse finanziarie sufficienti a

coprire i fabbisogni correnti e prospettici. A ciò si aggiunge la predisposizione di analisi periodiche sui flussi di cassa, finalizzate a un monitoraggio puntuale delle entrate e delle uscite finanziarie. Sono stati poi valutati anche altri profili di rischio, quali il rischio di cambio, considerato marginale poiché solo una quota minima delle transazioni avviene in valuta estera, e il rischio di tasso, ritenuto residuale in ragione della natura prevalentemente infragruppo dei debiti finanziari. (Documentazione interna di revisione: SRM_Summary Review Memorandum, 2024)

Dopo l'esame del contesto operativo e dei principali rischi di business, l'attenzione è stata successivamente rivolta all'approfondimento dei processi aziendali ritenuti più significativi ai fini della revisione, con l'obiettivo di predisporre le narrative dei principali cicli contabili e di integrarle nel processo di valutazione complessiva. La scelta dei cicli da analizzare è stata effettuata sulla base della rilevanza contabile e della significatività delle transazioni ad essi collegate, nonché del livello di rischio associato ai relativi processi. Sono stati pertanto privilegiati i cicli che incidono direttamente sulle principali voci di bilancio e che presentano una maggiore esposizione a rischi di errore o di frode. A tal fine sono stati organizzati incontri con i responsabili di processo, grazie ai quali è stato possibile ricostruire in maniera puntuale le modalità di gestione delle aree operative individuate come prioritarie. Di seguito si riportano i cicli analizzati e le principali caratteristiche emerse.

- **Ciclo attivo**

L'analisi del ciclo attivo ha evidenziato la presenza di due principali tipologie di ricavi: quelli derivanti da contratti a canone e quelli riconducibili a prestazioni straordinarie o spot (c.d. HBS – Hourly Based Services, ossia attività fatturate a consumo, sulla base di ore effettivamente erogate o di specifici preventivi).

- *Ricavi da canone*

  Una volta ottenuta l'aggiudicazione di una gara per l'affidamento dei servizi integrati di gestione e manutenzione delle apparecchiature biomediche, il cliente procede con l'approvazione dell'offerta e ne comunica formalmente l'accettazione all'impresa, consentendo così la stipula del contratto. Successivamente, i responsabili di area presenti sul territorio inseriscono, tramite un applicativo web, i dati relativi alla fatturazione delle commesse di loro competenza, trasmettendoli al responsabile della fatturazione attiva. Quest'ultimo, supportato dall'ufficio contratti e contabilità, provvede a verificare la correttezza delle informazioni immesse, con particolare attenzione alle tariffe applicate e ai canoni pattuiti contrattualmente o aggiornati mediante apposite delibere. Una volta completato il controllo, i dati vengono caricati nel gestionale della fatturazione e le fatture sono contabilizzate. Parallelamente, viene calcolato l'accantonamento relativo al fatturato da emettere: tale accantonamento, durante l'anno, viene gestito extra contabilmente e iscritto in contabilità soltanto nel mese di dicembre. Mensilmente, con il supporto del team di controllo di gestione, viene inoltre effettuata la quadratura tra i dati del gestionale e le registrazioni contabili, così da garantire coerenza e completezza delle rilevazioni.

- *Ricavi HBS (prestazioni spot)*

  Accanto ai ricavi a canone, l'impresa può generare entrate derivanti da attività straordinarie o richieste specifiche da parte dei clienti, esterne al contratto principale. Si tratta, ad esempio, di interventi a chiamata o della fornitura urgente di materiali. In tali circostanze, il cliente presenta una richiesta di preventivo, solitamente trasmessa via e-mail o attraverso una richiesta formale di intervento. Una volta ricevuta la richiesta, l'impresa elabora il preventivo e lo invia al cliente per approvazione. Quest'ultima può avvenire tramite l'emissione di un ordine firmato oppure attraverso un'autorizzazione scritta di intervento o, in alcuni casi, anche verbale. Solo a seguito di tale conferma si procede con l'esecuzione della prestazione e con la relativa registrazione contabile. Dal punto di vista procedurale, tale fase segue regole analoghe a quelle previste per i ricavi da canone, pur differenziandosi per la natura degli input iniziali, che derivano da

preventivi o ordini specifici del cliente. (Documentazione interna di revisione: narrative ciclo attivo, 2024)

- **Ciclo passivo**

Con riferimento al ciclo passivo, ogni richiesta di materiale (*Ri.Ma.*) o di intervento (*Ri.De.*) dà origine a un ordine di acquisto (ODA). Tale ordine viene inserito a sistema dall'ufficio acquisti e, una volta autorizzato, avvia il processo di approvvigionamento. Successivamente, quando l'ODA risulta autorizzato ed evaso, viene determinata la quota di accantonamento relativa al fatturato da ricevere. Al momento della ricezione della merce, il documento di trasporto (DDT) viene archiviato e la fattura del fornitore viene contabilizzata, completando così la registrazione contabile dell'operazione. Tale registrazione si fonda sulla disponibilità congiunta dell'ordine di acquisto, del DDT e della fattura, che rappresentano la documentazione formale a supporto del processo. Con cadenza mensile, il controller interno estrae dal sistema un report che distingue tra fatturato contabilizzato e fatturato ancora da ricevere, verificando la congruità degli importi e la correttezza delle rilevazioni relative agli accantonamenti. (Documentazione interna di revisione: narrative ciclo passivo, 2024)

- **Ciclo tesoreria**

Il ciclo di tesoreria ricopre un ruolo centrale nella gestione dei flussi finanziari aziendali e si articola attraverso procedure strutturate che garantiscono il monitoraggio costante di incassi e pagamenti. Gli incassi derivano sia da rapporti commerciali con la Pubblica Amministrazione sia da commesse stipulate con clienti privati, e la loro corretta gestione è presidiata dalla funzione di tesoreria, responsabile della verifica di accuratezza e completezza delle operazioni.

Per quanto concerne gli incassi, sono previste due modalità operative:

- *Incasso diretto*, che si realizza prevalentemente tramite bonifici bancari, ma che può avvenire anche attraverso RID, RIBA attivi, bollettini o cambiali. La gestione è supportata dal software PITECO, interfacciato con il sistema contabile D365.

Quotidianamente i movimenti bancari vengono scaricati da UniWeb, piattaforma di digital banking centralizzata di Unicredit, e importati in PITECO. Una volta consolidati, i dati vengono trasferiti in D365, che genera automaticamente la prima nota contabile. I conti utilizzati per la gestione degli incassi diretti sono di natura transitoria e sono oggetto di riconciliazione periodica, che viene svolta con cadenza settimanale al fine di garantire l'assenza di scostamenti o residui non giustificati. Sul piano operativo, invece, il processo viene gestito quotidianamente tramite PITECO. Nella schermata *"Gestione Incassi"* del sistema vengono riportati, da un lato, i dettagli degli incassi bancari e, dall'altro, le fatture importate automaticamente da D365 ogni sera, con la possibilità, se necessario, di procedere anche a un'importazione manuale. Gli incassi possono assumere due stati: *"Da abbinare"* e *"Riconciliati"*. Nel primo caso, l'addetto di tesoreria utilizza i dati contenuti nel mandato di pagamento (ad esempio importo, causale e cliente) per individuare la corrispondente fattura nella sezione dedicata e, una volta verificata la corrispondenza, procede a selezionarla ("flaggarla"), determinando così l'abbinamento e il passaggio dell'incasso allo stato di *"Riconciliato"*. Al termine della giornata, attraverso la funzione *"Consolidamento movimenti"* di PITECO, gli incassi riconciliati e le relative scritture contabili vengono trasferiti a D365, completando l'allineamento tra i movimenti bancari e la contabilità generale. Le scritture tipiche prevedono movimenti tra il conto banca, il conto transitorio incassi e i crediti verso clienti. Nel caso di RID e Ri.Ba., una volta presentato l'effetto (o autorizzato l'addebito automatico), il credito viene trasferito dal cliente al conto effetti presso banca, che viene successivamente chiuso all'atto dell'incasso tramite la movimentazione del conto banca. In caso di insoluto, l'importo viene rilevato sul conto transitorio insoluti, che deve essere successivamente riallocato manualmente al cliente in D365 per ripristinare la corretta esposizione del credito. Le cambiali seguono un iter analogo, pur senza predisposizione manuale di distinte bancarie (su D365 si alimentano le sole scritture contabili). Gli incassi non riconciliati restano sospesi in apposita sezione e vengono abbinati una volta ricevuto il mandato bancario. In presenza di difficoltà di riconciliazione, l'ufficio tesoreria si avvale del supporto della funzione vendite.

- *Incasso indiretto tramite factoring*, utilizzato in particolare per i crediti vantati nei confronti della Pubblica Amministrazione. In questo caso, i crediti vengono ceduti pro soluto a società di factoring, con contratti stipulati a livello di gruppo e gestiti tramite PITECO. Le cessioni hanno frequenza mensile e possono avvenire in più soluzioni, anche in base alle esigenze di liquidità della società. Una volta individuate le fatture cedibili, ossia quelle relative a clienti già contrattualizzati con il factor, il credit manager ne cura l'estrapolazione e la trasmette al responsabile bancario centrale e si procede alla cessione. L'incasso da parte del factor avviene in un intervallo di due-quattro giorni. Qualora il cliente effettui erroneamente un pagamento direttamente alla società anziché al factor, l'importo deve essere riversato al factor entro i termini contrattuali previsti (la principale controparte in termini di factoring, prevede che l'incasso ricevuto debba essere girato al factor entro 45 giorni). Con cadenza mensile, la funzione di tesoreria provvede inoltre al pagamento verso le società di factoring, partendo dalle fatture più datate ancora insolute.

Per quanto concerne i pagamenti invece, la gestione è interamente centralizzata tramite UniWeb, la piattaforma di e-banking di Unicredit, che consente di operare anche sui conti correnti di altri istituti collegati come "banche passive". Sono previste tre modalità di pagamento: anticipato, differito (a 30, 60, 90 o 120 giorni dalla data fattura) e, più raramente, pagamento a vista. Nel caso di pagamento anticipato, su segnalazione e autorizzazione dell'ufficio acquisti, la tesoreria provvede a disporre il bonifico contestualmente all'emissione dell'ordine di acquisto, trasmettendo al fornitore la prova del pagamento per accelerare la consegna. Per tutte le altre modalità, invece, è previsto che nessun pagamento possa essere effettuato in assenza della relativa fattura autorizzata e contabilizzata in D365. Nei pagamenti differiti le scadenze sono regolate contrattualmente e si collocano, in via generale, a 60-90 giorni dalla data della fattura. Ciascun operatore di tesoreria, tramite PITECO, predispone le distinte di pagamento per i fornitori di propria competenza e le carica su UniWeb. L'autorizzazione definitiva e la validazione spettano esclusivamente al vertice aziendale, che dispone delle credenziali di accesso (token) necessarie a rendere effettive le disposizioni. Tutti i pagamenti vengono poi processati e registrati tramite D365, che consente di selezionare le fatture da saldare

e di generare le relative scritture contabili. (Documentazione interna di revisione: narrative ciclo tesoreria, 2024)

- **Ciclo magazzino**

Il ciclo di magazzino si articola su più livelli organizzativi e logistici e comprende un magazzino centrale, diversi magazzini periferici e depositi collocati direttamente presso le strutture ospedaliere, suddivisi per commessa. Le movimentazioni delle merci avvengono sulla base di richieste formalizzate e vengono gestite secondo procedure standardizzate che garantiscono tracciabilità e controllo. La gestione delle movimentazioni prevede che ogni richiesta venga elaborata dalla sede centrale, che provvede a trasferire la merce al magazzino richiedente. L'uscita viene registrata al momento dell'effettivo utilizzo del bene.

Le uscite di magazzino possono assumere diverse configurazioni, riconducibili principalmente a quattro casistiche:

- *Prestazione contrattuale*: attività comprese nel canone, per le quali non viene emessa una fattura specifica, in quanto già incluse nel contratto di servizio.
- *Addebito periodico*: operazioni soggette a rendicontazione ciclica, anch'esse prive di fattura dedicata.
- *Intervento extra*: attività straordinarie per le quali viene emessa fattura, ma non è presente un documento di trasporto (DDT), in quanto non si tratta di una fornitura di beni.
- *Vendita*: la casistica tradizionale, che segue l'iter completo composto da preventivo, ordine e successiva fatturazione.

Per quanto riguarda le entrate di magazzino, queste riguardano principalmente due tipologie di beni:

- *Merci di consumo*, oggetto di ordini cumulativi predisposti dalla sede centrale per far fronte a richieste ripetitive o cicliche. Queste possono essere acquistate ed ordinate esclusivamente dal magazzino centrale.

- *Merci spot*, per le quali i magazzini periferici o i responsabili delle singole commesse inoltrano una richiesta di autorizzazione all'acquisto alla sede centrale. Solo a seguito dell'approvazione è possibile procedere con l'acquisto diretto da parte del magazzino periferico o della commessa stessa.

Con cadenza periodica, e comunque in occasione della chiusura annuale al 31 dicembre, vengono effettuate le conte inventariali. Tali attività seguono procedure formalizzate e standardizzate, volte a garantire l'accuratezza delle quantità rilevate e la corrispondenza con le registrazioni contabili. Inoltre, su base mensile, l'addetto al magazzino predispone un report di valorizzazione delle giacenze, utile ai fini del reporting gestionale. In questa sede vengono indagati ed eventualmente corretti i disallineamenti che dovessero emergere tra dati fisici e contabili. (Documentazione interna di revisione: narrative ciclo magazzino, 2024)

Oltre all'analisi dei principali cicli aziendali, un ulteriore aspetto di rilievo ha riguardato la valutazione delle *Information Provided by the Entity (IPE)*, ossia dei report e delle estrazioni generate dai sistemi informativi aziendali e messe a disposizione dei revisori. Tali informazioni rappresentano un elemento essenziale dell'evidenza di revisione, in quanto costituiscono la base sia per l'esecuzione dei test di controllo sia per le procedure sostanziali.

Affinché possano essere considerate affidabili, è necessario verificarne preliminarmente l'accuratezza, la completezza e l'adeguatezza. Il processo di predisposizione e utilizzo delle IPE può infatti presentare diversi profili di rischio, tra cui: la possibilità che i dati elaborati risultino incompleti o inesatti; il rischio che i parametri di estrazione non riflettano fedelmente le informazioni richieste, generando dati parziali; l'eventualità che errori nelle elaborazioni o riclassificazioni operate dal sistema producano distorsioni; la possibilità che il trasferimento dei dati verso strumenti di *end user computing* (ad esempio fogli di calcolo) comporti modifiche non tracciabili; e infine il rischio che eventuali interventi manuali da parte dell'utente introducano imprecisioni o alterazioni nei dati. Alla luce di tali criticità, è stato eseguito un test of IPE, finalizzato ad accertare che le informazioni utilizzate nel corso della revisione fossero complete, accurate e coerenti con gli obiettivi delle procedure di audit. In questo modo è stato possibile considerarle

evidenze probative affidabili, in conformità con quanto previsto dagli standard internazionali di revisione, e in particolare dall'ISA 500. (Documentazione interna di revisione: test IPE – Information Provided by Entity (Excel), 2024)

In aggiunta alle attività descritte, sono stati impiegati specifici strumenti operativi finalizzati ad ottenere una mappatura preliminare delle principali applicazioni gestionali e delle infrastrutture tecnologiche a supporto dei processi aziendali più rilevanti. Tale ricognizione ha consentito di collocare le attività di revisione in un contesto operativo completo, includendo anche gli aspetti tecnologici che concorrono al funzionamento dei presidi di controllo e alla gestione dei rischi. (Documentazione interna di revisione: Mappatura applicazioni gestionali e infrastrutture tecnologiche (Excel), 2024)

Dopo aver completato l'analisi dei principali cicli aziendali e dell'ambiente informatico di supporto, e sulla base della conoscenza del cliente maturata nel corso delle precedenti attività di revisione del bilancio, l'attenzione si è spostata sulla definizione dell'approccio di revisione da adottare. In questa fase sono stati determinati il valore del Tolerable Error (TE), ossia la soglia massima di errore accettabile nei bilanci senza che ciò comprometta la correttezza complessiva dell'informativa finanziaria, e il SAD Nominal Amount, parametro utilizzato per individuare l'ammontare minimo degli errori da comunicare[7]. Tali grandezze risultano fondamentali per orientare la successiva pianificazione delle procedure di revisione, consentendo di calibrare la natura, l'estensione e la tempistica dei test di audit. (Documentazione interna di revisione: PM TE and SAD nominal amount, 2024) Il passaggio successivo ha riguardato la selezione dei conti significativi, effettuata attraverso un approccio che combina criteri quantitativi e qualitativi. Sono stati innanzitutto qualificati come significativi i conti con saldo superiore al valore del TE; a questi si sono aggiunti ulteriori conti selezionati in base a:

- **elevato volume delle transazioni**, che aumenta la probabilità di errori o anomalie;

[7] ***ISA Italia 320*** *– Significatività nella pianificazione e nello svolgimento della revisione contabile* e ***ISA Italia 450*** *– Valutazione delle distorsioni identificate nel corso della revisione contabile*, emanati da IAASB e recepiti in Italia dal MEF e dal CNDCEC.

- **complessità delle operazioni sottostanti**, in quanto caratterizzate da trattamenti contabili articolati o da stime soggettive;
- **maggiore esposizione a rischi intrinseci**, legati alla natura delle voci di bilancio e alla possibilità di distorsioni materiali;
- **professional judgement del revisore**, quale valutazione qualitativa fondata sull'esperienza e sulla conoscenza del contesto aziendale.[8]

Complessivamente, sono stati così individuati venticinque conti significativi, che hanno costituito il perimetro principale dell'analisi.

Per approfondire la comprensione dei processi aziendali collegati a tali conti, sono stati organizzati incontri con i referenti della società. In particolare, l'attenzione si è concentrata sui principali cicli aziendali e sul Financial Statement Closing Process (FSCP), inteso come l'insieme delle attività di chiusura contabile e predisposizione del bilancio. Per ciascun processo è stato eseguito un Walk-Through (WT), procedura che consiste nel seguire un'intera transazione dalla sua origine fino alla rilevazione contabile finale, con l'obiettivo di verificare la corrispondenza tra le procedure formalmente descritte e le modalità operative effettivamente adottate, in linea con quanto previsto dall'ISA 315 (IAASB, 2019).

A completamento delle attività interinali, è stata inoltre predisposta e inviata la corrispondenza di circolarizzazione verso le principali controparti, quali banche, consulenti legali e fiscali, società di factoring, consulenti del lavoro, società di leasing, depositari, nonché clienti e fornitori. Nei casi di mancata risposta, sono state attivate procedure alternative per acquisire adeguata evidenza probativa.

Nell'ambito delle procedure di revisione svolte sui conti significativi, sono emerse alcune aree particolarmente sensibili che hanno richiesto un'attenzione specifica da parte del revisore. Le principali *audit issues* hanno riguardato:

[8] Il concetto di ***professional judgement*** trova fondamento nei principi internazionali di revisione (in particolare ISA 200 – *Overall Objectives of the Independent Auditor*), che richiedono al revisore di applicare le proprie competenze, l'esperienza professionale e la conoscenza del contesto aziendale per assumere decisioni appropriate in situazioni caratterizzate da incertezza o discrezionalità. In questo senso, il giudizio professionale integra gli elementi quantitativi e qualitativi, costituendo uno strumento essenziale per valutare rischi, definire procedure e formulare conclusioni di revisione.

► il corretto riconoscimento dei ricavi;
► la rilevazione e valutazione delle rimanenze di magazzino;
► la stima del fondo svalutazione crediti;
► la contabilizzazione delle operazioni di cessione di crediti pro-soluto.

Tali aree sono state ritenute sensibili in quanto caratterizzate da un'elevata esposizione al rischio di errore o frode: i ricavi rappresentano una delle voci più significative del bilancio e frequentemente oggetto di possibili manipolazioni; le rimanenze incidono in modo diretto sul risultato d'esercizio e possono prestarsi a errori di valutazione; il fondo svalutazione crediti comporta l'esercizio di giudizi soggettivi circa la recuperabilità delle esposizioni; infine, le operazioni di cessione di crediti presentano profili di complessità contabile e contrattuale che richiedono un esame accurato. L'analisi di tali aree, per la loro rilevanza in ottica antifrode, verrà approfondita dettagliatamente nei paragrafi successivi.

L'analisi è stata quindi estesa alle stime contabili incluse in alcune di queste voci, in conformità a quanto previsto dallo ISA 540 – Auditing Accounting Estimates and Related Disclosures (IAASB, 2019). Questo principio pone particolare enfasi sul fatto che le stime rappresentino un'area ad alto rischio di distorsioni materiali, in quanto fondate su giudizi discrezionali del management e quindi suscettibili di manipolazioni intenzionali. Lo standard richiede al revisore di acquisire una comprensione dei processi utilizzati dall'impresa per la formulazione delle stime, di valutarne la ragionevolezza alla luce delle assunzioni adottate, di verificare la coerenza dei dati impiegati e, infine, di considerare l'eventualità che il management abbia fatto ricorso a pratiche opportunistiche finalizzate ad alterare le risultanze contabili.

Proprio per questo, la revisione delle stime non è finalizzata unicamente a verificarne la correttezza formale, ma anche a testare l'efficacia del sistema di controllo interno nel ridurre il rischio che tali poste vengano sfruttate come strumenti di frode contabile.

Le stime rilevanti per l'impresa sono state oggetto di classificazione in funzione del grado di incertezza insito nei processi di valutazione, della complessità delle assunzioni formulate dal management e della rilevanza potenziale delle poste sul bilancio. Pur essendo teoricamente individuabili tre livelli di rischio (basso, medio ed elevato), nel caso concreto l'analisi ha condotto a una distribuzione su sole due categorie: stime a basso

rischio, caratterizzate da un livello contenuto di soggettività e da un ridotto margine di variabilità nei risultati, e stime a rischio elevato, contraddistinte invece da una maggiore esposizione a possibili errori materiali o a manipolazioni intenzionali. Ciò riflette il fatto che le poste analizzate presentavano profili di rischio chiaramente polarizzati: da un lato stime considerate solide e ben supportate, dall'altro stime maggiormente esposte a potenziali manipolazioni o a margini di soggettività rilevanti. La mancanza della categoria "medio" non rappresenta quindi un'anomalia metodologica, ma il risultato di un giudizio professionale basato sulle caratteristiche del caso concreto. La seguente tabella riassume le principali valutazioni ed è di seguito dettagliatamente analizzata:

Tabella 2 – Elaborazione dai documenti di revisione: Stime contabili e relativa categoria di rischio individuata.

Stima contabile	Categoria di rischio
Imposte anticipate	BASSO
Passività legali e fiscali	BASSO
Imposte differite passive	BASSO
Fondo svalutazione crediti	ELEVATO
Valutazione delle rimanenze	ELEVATO

Le imposte anticipate (Deferred Tax Assets – DTA) sono state classificate come stime a basso rischio. Tale valutazione trova fondamento nel fatto che la loro iscrizione è supportata da un piano fiscale annuale predisposto dall'area finance e approvato dal management, con assunzioni pienamente coerenti con il piano industriale della società. La base documentale risulta quindi solida e trasparente, riducendo la discrezionalità connessa al processo valutativo. Inoltre, i riscontri effettuati negli esercizi precedenti non hanno evidenziato significativi scostamenti rispetto alle previsioni, né anomalie che possano far ipotizzare pratiche opportunistiche o errori sistematici. La combinazione di

coerenza prospettica, controllo formale delle ipotesi e storicità positiva dei risultati ha reso ragionevole collocare tale voce in una categoria di rischio contenuto.

Le passività legali e fiscali sono state anch'esse considerate a basso rischio. La valutazione si basa sulla presenza di una funzione interna specificamente dedicata alla gestione dei contenziosi e sulla prassi consolidata di acquisire regolarmente pareri da consulenti legali e fiscali esterni di comprovata competenza. Questo duplice livello di presidio, interno ed esterno, consente di ridurre sensibilmente il margine di incertezza tipicamente connesso a tali poste. I dati storici confermano questa valutazione: negli esercizi precedenti, infatti, non sono emerse variazioni inattese negli importi accantonati, né utilizzi dei fondi che potessero far sospettare approcci opportunistici da parte del management. Tale stabilità rafforza la conclusione circa il basso livello di rischio attribuibile a questa voce.

Infine, le imposte differite passive (Deferred Tax Liabilities – DTL**)** sono state collocate nella medesima categoria di rischio ridotto. La loro origine deriva principalmente dall'applicazione dell'IFRS 16 e dall'avviamento, aree che comportano effetti differiti nel tempo ma che presentano un grado molto limitato di discrezionalità nelle modalità di calcolo. L'applicazione standardizzata dei principi contabili e la natura sostanzialmente tecnica delle rilevazioni riducono infatti il margine di soggettività, rendendo poco probabile la presenza di manipolazioni intenzionali o errori significativi. Anche in questo caso, l'assenza di scostamenti rilevanti negli esercizi precedenti ha consolidato la valutazione di un rischio basso.

Le due ultime stime – il fondo svalutazione crediti e la valutazione delle rimanenze – meritano un'attenzione particolare, in quanto sono state individuate come aree a rischio elevato sia per la rilevanza quantitativa delle poste sia per il grado di discrezionalità insito nella loro determinazione.

Il fondo svalutazione crediti rappresenta una delle aree più sensibili sotto il profilo del rischio di frode, poiché strettamente collegato alle valutazioni sulla recuperabilità dei crediti commerciali ed infatti è collocata nella categoria di rischio più elevato. La determinazione del fondo richiede l'applicazione di criteri di stima che possono variare in funzione di parametri quali l'anzianità del credito, l'andamento storico degli incassi o la solidità finanziaria della controparte. Proprio per il carattere discrezionale di tali criteri,

questa posta può prestarsi a utilizzi opportunistici da parte del management, ad esempio per incrementare o ridurre arbitrariamente gli accantonamenti in funzione degli obiettivi di bilancio. In ottica antifrode, la revisione ha quindi previsto controlli mirati a verificare la coerenza delle percentuali di svalutazione applicate, la corrispondenza con le esperienze storiche di recupero, nonché il rispetto delle procedure interne di monitoraggio dei crediti in sofferenza. L'ISA 540 (IAASB, 2019) richiama esplicitamente l'attenzione del revisore sul rischio che le stime contabili possano essere influenzate da bias gestionali o da pressioni finalizzate a manipolare i risultati; il fondo svalutazione crediti ne costituisce un esempio paradigmatico.

Analogamente, la valutazione delle rimanenze si configura come un'area ad elevata esposizione al rischio di errore materiale o di frode. Le rimanenze assumono un ruolo rilevante nella rappresentazione della situazione aziendale, poiché influenzano in modo diretto sia l'andamento economico dell'esercizio, incidendo sulla determinazione del risultato, sia la dimensione patrimoniale, concorrendo a delineare il valore complessivo delle risorse disponibili. Per questo motivo, la loro corretta rilevazione e valutazione è un aspetto centrale nei processi di redazione e revisione del bilancio. L'impresa adotta il criterio dell'ultimo prezzo di acquisto per attribuire valore alle giacenze, ma la corretta applicazione di tale criterio richiede un monitoraggio continuo dei flussi di approvvigionamento e un adeguato sistema di registrazione dei movimenti di magazzino. Errori nella rilevazione delle entrate o delle uscite di merce, omissioni nei caricamenti a sistema o valutazioni discrezionali non giustificate possono condurre a una rappresentazione non fedele della voce. Inoltre, la natura diffusa e territorialmente articolata della gestione dei magazzini accresce la complessità dei controlli e aumenta il rischio che anomalie non vengano prontamente rilevate. Anche in questo caso, l'ISA 540 sottolinea come la valutazione delle rimanenze, trattandosi di un'area basata su stime e assunzioni, richieda una particolare attenzione da parte del revisore per individuare eventuali indicatori di manipolazione.

La revisione di queste due poste non ha quindi solo lo scopo di accertarne la correttezza formale e la conformità ai principi contabili, ma assume un significato più ampio in relazione alla finalità del presente elaborato. Esse costituiscono infatti un banco di prova per valutare l'efficacia del sistema di controllo interno nella prevenzione e rilevazione di possibili fenomeni fraudolenti, in quanto sono aree in cui il rischio di utilizzo distorto

delle stime contabili risulta particolarmente elevato. Per tale motivo, l'analisi dettagliata del fondo svalutazione crediti e della valutazione delle rimanenze sarà sviluppata in un paragrafo successivo, al fine di evidenziare come i presidi di controllo interno si dimostrino effettivamente in grado – o meno – di mitigare i rischi connessi a comportamenti opportunistici del management.

Alla luce di quanto esposto, l'analisi prosegue con l'esame mirato delle aree a rischio e con la valutazione dei relativi presidi, con l'obiettivo di verificare in che misura il sistema di controllo interno sia in grado di garantire un'adeguata tutela rispetto a possibili fenomeni fraudolenti. (Documentazione interna di revisione: SRM_Summary Review Memorandum, 2024)

3.2 Analisi integrata dei rischi identificati e dei controlli interni in chiave antifrode

L'attività di fraud audit non può ridursi a una mera ricognizione dei controlli formalmente adottati, ma richiede necessariamente un'integrazione con l'analisi dei rischi cui l'organizzazione è esposta e con la valutazione del grado di copertura garantito dai presìdi esistenti. Solo attraverso un approccio integrato, che metta in relazione i punti di vulnerabilità con le misure di mitigazione adottate, è infatti possibile cogliere la reale solidità del sistema di controllo interno in chiave antifrode.

In questa prospettiva, la sezione che segue si propone di offrire un quadro organico che, muovendo dall'analisi dei principali rischi riscontrabili nei processi aziendali, si concentri successivamente sulle aree che presentano i profili di maggiore esposizione e, infine, sulle modalità di presidio adottate dalla società attraverso i controlli interni. L'analisi si articola quindi in tre momenti tra loro complementari: nel primo (par. 3.2.1) viene condotta una ricognizione dei principali rischi nei processi aziendali e delle attività di verifica svolte in relazione ad essi; nel secondo (par. 3.2.2) l'approfondimento si concentra sulle aree critiche che evidenziano i più elevati livelli di esposizione, inquadrandole all'interno del relativo quadro metodologico di riferimento; nel terzo (par. 3.2.3) l'attenzione si sposta sulle modalità di presidio implementate dalla società, con l'obiettivo di valutarne la coerenza e l'efficacia rispetto ai rischi individuati.

In questo modo, la sezione si configura come un passaggio intermedio cruciale tra la descrizione del sistema di controllo interno e la successiva valutazione critica, offrendo

una visione strutturata del rapporto tra rischi e controlli e ponendo le basi per una riflessione più ampia sulla capacità dell'organizzazione di prevenire e individuare tempestivamente possibili condotte fraudolente.

3.2.1 Principali rischi identificati nei processi aziendali e attività di verifica svolte

Nell'ambito delle attività di revisione, come finora descritto, una volta individuati i conti significativi l'attenzione si è concentrata sulle classi significative di transazioni ad essi collegate (*Significant Classes of Transactions – SCOTs*), al fine di analizzare i cicli operativi sottostanti e individuare i relativi punti di vulnerabilità. L'esame dei cicli ha consentito di estrapolare i *What Could Go Wrong* (WCGW), ossia i possibili scenari di errore o frode che possono verificarsi nei diversi passaggi processuali. Tali rischi rappresentano il punto di partenza per valutare l'adeguatezza dei controlli interni e, conseguentemente, il livello di *control risk*.

I cicli aziendali, già descritti in precedenza con riferimento al loro funzionamento complessivo, vengono quindi in questa sede ripercorsi secondo un approccio più schematico, volto a isolare i principali WCGW connessi a ciascuna fase e a documentare le attività di verifica svolte. Tale impostazione selettiva consente di mettere in evidenza le aree maggiormente esposte e di predisporre la base metodologica per la successiva valutazione dell'efficacia dei presidi di controllo interno in ottica antifrode.

La valutazione ha tenuto conto sia dei fattori di rischio intrinseco – quali complessità, soggettività delle stime, cambiamenti normativi o gestionali, incertezza operativa e vulnerabilità a possibili distorsioni legate a bias manageriali o a fattori di rischio di frode – sia delle aree di processo maggiormente esposte a potenziali inesattezze. In questo modo è stato possibile identificare i punti del processo che potevano dare origine a rischi di errori materiali.

Una volta individuati i rischi più significativi all'interno delle classi di transazioni (SCOTs), essi sono stati collegati alle pertinenti asserzioni di bilancio dei conti interessati. Nell'analisi dei cicli critici, è stata inoltre verificata l'adeguatezza delle policy aziendali, con particolare attenzione al rispetto del quadro normativo di riferimento in materia di informativa finanziaria. Nei casi in cui tali policy non risultassero adeguatamente definite,

sono state rilevate deficienze di controllo, documentate come potenziali indicatori di rischio di errori materiali.

Per confermare la corretta comprensione di ciascun processo, sono state condotte procedure di walkthrough [9]e richieste di chiarimenti puntuali al management, al fine di verificare la completezza della documentazione e accertare l'identificazione di tutti i rischi rilevanti (WCGWs). Ogni eventuale aggiornamento delle modalità operative ha comportato un aggiornamento della mappatura dei rischi.

L'analisi dei percorsi critici delle SCOTs ha consentito di valutare se l'insieme delle procedure aziendali fosse idoneo a garantire la corretta rappresentazione delle transazioni nei prospetti finanziari, in conformità al quadro normativo di riferimento. (Documentazione interna di revisione: Identify significant classes of transactions (SCOTs), 2024)

L'analisi è stata avviata con riferimento al ciclo attivo, considerato particolarmente rilevante per la generazione dei ricavi e per l'impatto che esso esercita sulla rappresentazione del bilancio. In tale ambito, sono state mappate le principali fasi del processo, individuando per ciascuna di esse i rischi connessi (*WCGW – What Could Go Wrong*) e le attività di verifica svolte dal team di revisione.

- **Fase di avvio del servizio (initiation phase)**

  La prima fase del ciclo attivo riguarda l'attivazione delle prestazioni nei confronti dei clienti. Il rischio principale (WCGW) individuato in questo passaggio è la possibilità che vengano erogati servizi non autorizzati, ossia non supportati da un contratto formalmente sottoscritto o da un ordine regolarmente approvato. Tale scenario si qualifica come WCGW in quanto l'esecuzione di attività prive di titolo potrebbe comportare il riconoscimento di ricavi non giustificati, esponendo il bilancio a inesattezze materiali. Per mitigare questo rischio, è stata svolta un'attività di verifica documentale, volta ad accertare la presenza di un contratto valido o, in alternativa, di un ordine di servizio o di un verbale di intervento

[9]Le **procedure di walkthrough**, disciplinate dall'ISA 315 (*Identifying and Assessing the Risks of Material Misstatement*), prevedono il tracciamento di una transazione dall'origine fino alla sua rilevazione finale nei registri contabili. Tale attività consente al revisore di ottenere una comprensione diretta del processo, verificando sia il disegno dei controlli interni sia la loro effettiva applicazione.

corredato da preventiva autorizzazione scritta. Questo presidio è risultato essenziale per garantire che l'avvio delle prestazioni avvenisse esclusivamente sulla base di accordi vincolanti e tracciabili.

- **Fase di registrazione (recording phase)**

  Una volta avviato il servizio, il processo prosegue con la registrazione dei dati necessari per l'emissione della fattura. Il rischio (*WCGW*) individuato in questo passaggio consiste nella possibile emissione di fatture errate, derivanti da errori di trascrizione, incongruenze nelle anagrafiche o mancato allineamento con le condizioni contrattuali. Tali errori potrebbero tradursi in una rappresentazione non corretta dei ricavi e incidere sulla completezza e sull'accuratezza delle rilevazioni contabili. A presidio di questo rischio, il team di revisione ha eseguito controlli di coerenza tra i dati presenti nei contratti, le informazioni registrate a sistema e i dettagli riportati in fattura, verificando la corrispondenza tra le condizioni economiche pattuite e la documentazione prodotta.

- **Fase di contabilizzazione (processing phase)**

  In questa fase il rischio principale (*WCGW*) riguarda la possibilità di una non corretta contabilizzazione dei ricavi, con conseguente compromissione della rappresentazione veritiera della performance economica e finanziaria della società. Tale rischio si collega in particolare all'asserzione di *cut-off*, ossia alla corretta imputazione dei ricavi al periodo di competenza. Per presidiare questo aspetto, l'attività di revisione ha incluso la verifica puntuale della registrazione delle fatture emesse, accertando che fossero imputate ai corretti esercizi contabili e conformi alle regole stabilite dal principio di competenza economica.

- **Fase di rendicontazione (reporting phase)**

  Infine, nella fase di chiusura e rendicontazione, il rischio principale (*WCGW*) è stato individuato nella non corretta determinazione degli accantonamenti al fondo svalutazione crediti. Tale area è particolarmente sensibile, in quanto caratterizzata da un elevato grado di discrezionalità da parte del management. Per presidiare questo rischio, è stata condotta un'analisi approfondita delle metodologie adottate dalla società per la determinazione del fondo, verificandone la coerenza con le

policy interne e con i principi contabili di riferimento, nonché la congruità delle assunzioni utilizzate.

Parallelamente all'analisi delle singole fasi, sono stati condotti colloqui e *walkthrough* con i responsabili di processo, al fine di approfondire il funzionamento delle procedure, verificare l'effettiva applicazione dei controlli e rilevare eventuali variazioni rispetto agli esercizi precedenti. Dalle verifiche svolte non sono emerse modifiche sostanziali né nei processi operativi né negli strumenti informatici utilizzati a supporto, confermando la stabilità complessiva dell'impianto procedurale. (Documentazione interna di revisione: narrative ciclo attivo, 2024)

L'analisi è proseguita con il ciclo passivo, che riveste un ruolo centrale nella gestione degli approvvigionamenti e dei rapporti con i fornitori, incidendo in maniera significativa sulla corretta rappresentazione dei costi e dei debiti in bilancio. Anche in questo caso, il processo è stato scomposto nelle sue principali fasi operative, per ciascuna delle quali sono stati individuati i rischi potenziali (*WCGW – What Could Go Wrong*) e le relative attività di verifica.

- **Fase di avvio dell'ordine (initiation phase)**

  La fase iniziale riguarda la generazione dell'ordine di acquisto in risposta a una richiesta di materiale o di intervento. Il rischio principale (WCGW) è che vengano emessi ordini non coerenti con i fabbisogni effettivi o privi di un'adeguata autorizzazione, con conseguente possibilità di generare costi impropri o non pertinenti. Per mitigare tale rischio, l'attività di revisione ha previsto verifiche documentali finalizzate ad accertare la corrispondenza tra la richiesta di approvvigionamento e l'ordine formalizzato, verificando al contempo che quest'ultimo fosse debitamente autorizzato.

- **Fase di registrazione (recording phase)**

  Successivamente, la ricezione della merce o del servizio comporta la registrazione dei documenti a sistema. In questo passaggio il rischio principale (WCGW) è rappresentato dalla mancata corrispondenza tra ordine di acquisto, documento di trasporto e fattura del fornitore, con possibili effetti sulla corretta imputazione dei costi e sul rischio di passività non esistenti o non correttamente rilevate. Per

presidiare questa criticità, l'attività di verifica ha previsto un confronto sistematico tra i tre documenti, volti ad assicurare la coerenza e la completezza delle informazioni prima della registrazione contabile.

- **Fase di contabilizzazione (processing phase)**

  Questa fase riguarda la determinazione e la contabilizzazione degli accantonamenti per fatture da ricevere. In questo passaggio, il rischio (WCGW) riguarda la determinazione e la contabilizzazione degli accantonamenti per fatture da ricevere. Una gestione non corretta potrebbe infatti comportare una rappresentazione distorta delle passività e dei costi a bilancio. L'attività di verifica ha incluso controlli mirati al ricalcolo delle quote di competenza e alla quadratura con i dati contabili, con l'obiettivo di verificare l'accuratezza e la correttezza della rilevazione.

- **Fase di rendicontazione (reporting phase)**

  Nella fase di reporting, l'attenzione si sposta dal singolo documento alla rappresentazione aggregata in bilancio. Il rischio principale (WCGW) consiste nella possibilità di errori o omissioni nella contabilizzazione complessiva dei costi derivanti dalle fatture ricevute, con impatti sulla completezza e correttezza dell'informazione contabile. Per affrontare tale criticità, sono state effettuate riconciliazioni tra fatture contabilizzate e documentazione di supporto, così da garantire la corretta imputazione dei costi in bilancio e la completezza dell'informazione contabile.

Parallelamente all'analisi delle singole fasi, sono stati svolti colloqui e walkthrough con i responsabili di processo, al fine di acquisire una comprensione dettagliata delle procedure, verificare l'applicazione effettiva dei controlli e valutare la stabilità del sistema rispetto agli esercizi precedenti. Anche in questo caso, le verifiche hanno confermato l'assenza di variazioni sostanziali nel processo operativo e negli strumenti informatici utilizzati, a dimostrazione della continuità e della coerenza delle prassi adottate. (Documentazione interna di revisione: narrative ciclo passivo, 2024)

È stato poi analizzato il ciclo di tesoreria, che riveste un'importanza cruciale nella gestione finanziaria della società, in quanto attiene sia alla corretta rilevazione degli

incassi derivanti dai rapporti commerciali con la Pubblica Amministrazione e con soggetti privati, sia alla gestione dei pagamenti verso i fornitori. L'analisi ha consentito di identificare i principali rischi potenziali (*WCGW – What Could Go Wrong*) e di documentare le attività di verifica svolte per presidiare tali aspetti, con riferimento alle diverse articolazioni del ciclo di tesoreria.

- **Incassi diretti**

  Il rischio principale (WCGW) riguarda il mancato o inesatto incasso delle somme dovute dai clienti a causa di errori, malfunzionamenti o disallineamenti nei sistemi informativi di tesoreria (PITECO/UniWeb), con conseguente rischio di mancata rilevazione nel sistema degli incassi effettivamente avvenuti. Per ridurre tale possibilità, è stato verificato che il personale di tesoreria effettui quotidianamente un controllo su PITECO, accertando la corretta ricezione nel sistema degli incassi transitati attraverso UniWeb. Un ulteriore rischio (*WCGW*) concerne la mancata riconciliazione degli incassi con le fatture emesse. Per mitigarlo, è stata verificata l'attività dell'addetto alla tesoreria, che provvede ogni giorno ad abbinare manualmente i movimenti bancari importati da UniWeb alle corrispondenti fatture registrate in D365, assicurando che lo stato dell'incasso passi da "da abbinare" a "riconciliato".

- **Incassi tramite factoring**

  Per i crediti ceduti pro soluto a società di factoring, il rischio (*WCGW*) è che i clienti effettuino per errore il pagamento direttamente alla società anziché al factor, con conseguente mancata regolarizzazione dei flussi. Le verifiche hanno riguardato la correttezza delle procedure interne predisposte per riversare tempestivamente gli importi al factor entro i termini contrattuali, nonché la coerenza dei controlli operati dal credit manager sulle fatture oggetto di cessione.

- **Pagamenti**

  Relativamente alla gestione dei pagamenti i rischi principali (*WCGW*) sono due: da un lato, l'esecuzione di pagamenti relativi a fatture non correttamente autorizzate; dall'altro, la possibilità che i pagamenti vengano processati da soggetti non abilitati. Per presidiare il primo rischio, sono state verificate le

> procedure adottate dagli addetti alla tesoreria, che provvedono a controllare la presenza dell'autorizzazione su D365 prima di includere le fatture nelle distinte di pagamento. Con riferimento al secondo rischio, è stata accertata la procedura che prevede l'intervento esclusivo del CEO, unico soggetto autorizzato a validare i pagamenti tramite accesso al sistema UniWeb con token personale. (Documentazione interna di revisione: narrative ciclo tesoreria, 2024)

È stato infine analizzato il ciclo di magazzino, che assume particolare rilievo per la corretta rilevazione delle movimentazioni di materiali e per la loro incidenza sul bilancio attraverso le rimanenze finali. La società dispone di un magazzino centrale ubicato a Roma, di diversi magazzini periferici e di ulteriori magazzini collocati presso strutture ospedaliere, suddivisi per singola commessa. Ogni richiesta di materiale (Ri.Ma) viene elaborata dalla sede centrale, che provvede a spedire la merce al magazzino richiedente mediante un trasferimento; l'uscita di magazzino viene registrata al momento dell'effettivo utilizzo del materiale.

Le principali casistiche operative sono quattro:

- **Prestazioni contrattuali incluse nel canone (PRC),** per le quali l'uscita di magazzino corrisponde a un intervento di manutenzione non accompagnato da fatturazione;
- **Addebiti periodici (PER)**, attività soggette a rendicontazione ma anch'esse non correlate a fattura dedicata;
- **Interventi extra (EXT)**, per i quali è prevista la fatturazione dell'attività senza l'emissione di un DDT, poiché non si tratta di fornitura di beni;
- **Vendite (VEN)**, che seguono l'iter tradizionale con preventivo, ordine e successiva fatturazione.

In relazione a tali operazioni, il rischio principale (*WCGW*) è quello di un'errata o non giustificata registrazione dell'uscita di merce. L'attività di verifica ha previsto il confronto incrociato (match) tra il Documento di Trasporto, l'ordine – quando presente – e la fattura, ove prevista.

Per quanto riguarda le entrate di magazzino, si distinguono due tipologie:

- **Merci di consumo**, ordinate dalla sede centrale, che effettua acquisti cumulativi per soddisfare richieste ricorrenti o cicliche, mantenendo uno stock presso il magazzino principale.
- **Merci spot**, acquistate a seguito di specifiche richieste avanzate dai magazzini periferici o dalle singole commesse, previa autorizzazione della sede centrale.

Anche in questo caso, il rischio (*WCGW*) è quello di una registrazione errata o non adeguatamente giustificata dell'entrata di merce. Per fronteggiarlo, è stata effettuata una verifica della corrispondenza tra l'entrata registrata e i documenti giustificativi (ordine, DDT, fattura).

Un rischio ulteriore (*WCGW*) riguarda il mancato carico o scarico delle merci in magazzino. L'attività di verifica è consistita nel confronto tra i documenti di trasporto o le fatture e la corrispondente registrazione effettuata a sistema.

Con riferimento alla fase di chiusura e rendicontazione, è stata posta attenzione al rischio (*WCGW*) di un'errata contabilizzazione delle rimanenze. Per ridurre tale rischio, sono state effettuate conte inventariali periodiche (in particolare al 31 dicembre), seguendo procedure standardizzate e formalizzate, nonché verifiche di coerenza tra i report di giacenza predisposti mensilmente dall'addetto al magazzino e i valori registrati in contabilità.

Infine, ai fini della valorizzazione delle rimanenze, è stato verificato che la società adotti il criterio dell'ultimo prezzo di acquisto, che consente di attribuire alle merci un valore coerente con le condizioni correnti di approvvigionamento. (Documentazione interna di revisione: narrative ciclo magazzino, 2024)

Nel complesso, l'analisi dei cicli aziendali ha permesso di ricostruire i principali rischi potenziali connessi alle diverse fasi operative, individuando per ciascuno i relativi *What Could Go Wrong (WCGW)* e documentando le attività di verifica svolte. Tale mappatura ha consentito di collegare i rischi ai conti significativi e alle pertinenti asserzioni di bilancio, fornendo così la base metodologica per l'approfondimento successivo, incentrato sulla valutazione dei presidi di controllo interno predisposti dalla società per fronteggiare i WCGW e ridurre l'esposizione a possibili anomalie o manipolazioni.

3.2.2 Analisi del rischio di frode: quadro metodologico e aree critiche

L'analisi dei rischi di frode è stata sviluppata nel pieno rispetto degli standard internazionali di revisione. In particolare, l'ISA 240 evidenzia come il revisore sia tenuto a considerare, in ogni incarico, la possibilità che il bilancio presenti inesattezze materiali derivanti da frodi, distinguendole dagli errori non intenzionali per la loro natura dolosa e per il grado di complessità che spesso le caratterizza. Tra i rischi presi in esame, un'attenzione particolare è riservata al cosiddetto *management override of controls*, ossia all'eventualità che la direzione aziendale, sfruttando la propria posizione, possa eludere o aggirare i controlli interni, manipolando i dati contabili attraverso scritture arbitrarie, modifiche alle stime o omissioni informative. Tale rischio è qualificato come rischio significativo perché, indipendentemente dall'efficacia del sistema di controllo interno, il management si trova in una posizione che gli consente di esercitare un potere discrezionale in grado di compromettere l'attendibilità del bilancio. (IAASB, 2009)

Accanto all'ISA 240, l'ISA 500 stabilisce i criteri relativi all'acquisizione delle evidenze di revisione, specificando che esse debbano essere sufficienti e appropriate. L'adeguatezza e la qualità delle evidenze raccolte sono fondamentali per supportare il giudizio professionale dell'auditor, soprattutto in relazione a rischi di frode, che per loro natura si caratterizzano per un più elevato grado di complessità e di intenzionalità rispetto agli errori non fraudolenti. Pertanto, nella valutazione dei rischi di frode, il revisore non solo è chiamato a identificare le aree più esposte, ma deve anche calibrare le procedure di verifica in modo da acquisire evidenze robuste e non ambigue, capaci di contrastare l'eventuale presenza di manipolazioni dolose. (IAASB, 2009)

Su questo impianto normativo si innesta l'applicazione del modello del triangolo della frode, elaborato da Donald Cressey (1953) e già introdotto nel Capitolo 1. Tale modello, richiamato anche all'interno della EY Global Audit Methodology (GAM) – il manuale che guida le società del Gruppo nella predisposizione del Reporting Package secondo le Group Policies, coerenti con gli standard contabili internazionali IAS/IFRS – costituisce un riferimento essenziale per l'analisi delle dinamiche fraudolente. Esso individua tre condizioni principali che, quando coesistono, possono incentivare la commissione di una frode:

- **Opportunità**, ossia la possibilità oggettiva per un individuo di porre in essere comportamenti fraudolenti, generalmente favorita da debolezze nei controlli interni o da un accesso privilegiato alle informazioni;
- **Incentivi o pressioni**, legate a fattori economici, finanziari o organizzativi che spingono il soggetto a perseguire comportamenti illeciti (ad esempio il raggiungimento di obiettivi di performance, il rispetto di covenant contrattuali o la volontà di mantenere una certa immagine verso il mercato);
- **Atteggiamenti o razionalizzazioni**, che rappresentano il processo psicologico mediante cui il soggetto giustifica a sé stesso la frode, minimizzandone la gravità o legittimandola come risposta a condizioni percepite come ingiuste.

L'interazione di questi tre elementi consente di spiegare perché, anche in presenza di controlli apparentemente adeguati, possano emergere condotte fraudolente. La loro applicazione in ambito di revisione permette quindi di mappare i contesti più esposti al rischio, identificando le aree di bilancio o i processi in cui si concentrano maggiormente le opportunità di manipolazione, le pressioni legate ai risultati economici e le possibili giustificazioni da parte del management o dei dipendenti. In tal modo, l'auditor è in grado di sviluppare procedure di verifica mirate e proporzionate, coerenti con i rischi individuati. (Donald R. Cressey, 1953)

Muovendo da tale cornice metodologica, l'attenzione è stata indirizzata in primo luogo sull'area del riconoscimento dei ricavi, ritenuta intrinsecamente esposta per la combinazione di due fattori: da un lato, la presenza di stime contabili (in particolare nella determinazione delle fatture da emettere), che possono costituire un canale privilegiato per anticipazioni o simulazioni di ricavi; dall'altro, l'elevato volume di registrazioni che caratterizza la classe, con conseguente accrescimento del rischio che errori o manipolazioni non vengano intercettati dai controlli di routine. In tale contesto sono stati formalmente identificati due rischi principali di frode:

- Il taglio improprio dei ricavi, ossia il riconoscimento in un periodo diverso da quello di competenza;
- Il riconoscimento "over time" dei ricavi di commessa disciplinato dall'IFRS 15, che consente di rilevare i ricavi progressivamente lungo la durata del contratto

sulla base dello stato di avanzamento delle prestazioni. Tale modalità, pur garantendo una rappresentazione più fedele dell'andamento economico, comporta un elevato grado di discrezionalità nella stima delle percentuali di completamento e dei costi residui. In ottica antifrode, ciò può tradursi nel rischio che il management anticipi il riconoscimento dei ricavi o sottostimi i costi futuri, ritardando l'emersione di perdite e alterando artificiosamente i risultati economici dell'esercizio.

Sul versante dei presìdi organizzativi e procedurali, l'analisi ha considerato i meccanismi di tracciabilità contrattuale e di coerenza documentale alla base della contabilizzazione: la formalizzazione delle prestazioni (contratti e ordini), l'allineamento con i documenti di erogazione (verbali d'intervento, documenti di consegna, installazioni) e i processi di registrazione e riconciliazione con la contabilità generale. Con specifico riguardo alle stime delle fatture da emettere, l'attenzione si è focalizzata sul collegamento tra criteri di determinazione ed evidenze a supporto (stato di avanzamento, servizi effettivamente resi, documentazione probatoria), in modo da ridurre gli spazi di discrezionalità che potrebbero alimentare rischi di riconoscimento prematuro o sovrastima dei ricavi.

In risposta ai rischi di frode identificati e documentati, sono state sviluppate procedure di audit mirate, articolate su più livelli e coerenti con la logica rischio-risposta:

- **Analisi contrattuale e corretto cut-off dei ricavi.**

  È stata svolta una revisione puntuale dei nuovi contratti stipulati nell'esercizio, provenienti sia da gare pubbliche sia da negoziazioni private. L'analisi ha riguardato in particolare le clausole economiche, le condizioni di fornitura, i termini temporali e le fasi contrattuali, rilevanti per la corretta imputazione dei ricavi a bilancio. Successivamente sono stati eseguiti test di *cut-off*, ossia procedure di verifica finalizzate ad accertare che i ricavi siano registrati nel corretto esercizio di competenza, in linea con il principio contabile della competenza economica. L'obiettivo è stato quello di evitare, da un lato, l'anticipazione artificiosa dei ricavi (*overstatement*), dall'altro il loro rinvio ingiustificato (*understatement*), garantendo così la corretta rappresentazione del risultato d'esercizio.

- **Ispezione mirata delle transazioni e riscontri documentali.**

  Su un campione selezionato di operazioni di ricavo è stata condotta un'ispezione analitica delle fatture emesse, con verifica della corrispondenza temporale tra la data di erogazione dei servizi (ad esempio data di installazione o di manutenzione, momento del trasferimento dei rischi e benefici) e la relativa registrazione contabile. Per ciascuna transazione è stata richiesta documentazione di supporto (contratti, ordini di vendita, documenti di trasporto, verbali di intervento), in modo da confermare la sostanza economica delle operazioni. Particolare attenzione è stata riservata alle transazioni a cavallo della chiusura, considerate più esposte al rischio di errori di cut-off e manipolazioni.

- **Procedure analitiche sostanziali e analisi di trend.**

  Sono state effettuate procedure analitiche sostanziali sui ricavi, con specifico focus sui mesi prossimi alla chiusura dell'esercizio. Le analisi hanno incluso confronti rispetto ai trend storici, alle previsioni di budget e ai dati di settore, al fine di intercettare eventuali andamenti anomali, picchi di fatturazione o cadute non giustificate. L'approccio ha consentito di disporre di elementi di riscontro aggiuntivi rispetto alle verifiche di dettaglio e di rafforzare la capacità di individuare possibili anomalie, anche in un'ottica di prevenzione di comportamenti fraudolenti.

- **Test di cut-off su popolazioni a basso valore e alto volume.**

  Considerata la natura *low-value/high-volume* delle transazioni di ricavo, che aumenta la probabilità di errori diffusi non intercettabili con sole verifiche mirate, è stato predisposto un test di cut-off specifico. Tale test ha riguardato un campione di operazioni registrate immediatamente prima e dopo la data di chiusura, con l'obiettivo di verificare che la loro imputazione fosse coerente con la competenza economica. Questo presidio ha permesso di cogliere tempestivamente eventuali scivolamenti temporali, riducendo il rischio che piccoli errori ripetuti su larga scala producessero effetti materiali complessivi.

- **Conferme esterne e incassi successivi.**

  Per i saldi clienti di importo significativo sono state inviate richieste di conferma esterna, al fine di acquisire evidenze indipendenti circa l'esistenza e l'accuratezza dei crediti. Nei casi di mancata risposta, la validazione è stata svolta tramite la verifica degli incassi successivi alla data di bilancio, così da accertare che le posizioni risultassero effettivamente esigibili. Qualora neppure tali riscontri fossero disponibili, l'esistenza e la correttezza dei crediti sono state corroborate attraverso contratti e ordini firmati. Questo approccio multilivello ha consentito di rafforzare l'affidabilità delle evidenze probative raccolte.

- **Verifica delle rettifiche post-chiusura.**

  È stato analizzato un campione di note di credito emesse dopo la chiusura dell'esercizio, al fine di intercettare eventuali storni di vendite che potessero rivelare la registrazione di ricavi fittizi o prematuri. La procedura ha consentito di verificare la sostanza economica delle operazioni e di rilevare tempestivamente eventuali comportamenti volti ad alterare artificiosamente il risultato d'esercizio. L'analisi ha incluso il confronto con la documentazione di supporto e con le prassi contrattuali in essere.

- **Analisi delle scritture contabili (JE).**

  Sono state analizzate le journal entries con particolare attenzione alle registrazioni anomale o prive di chiara giustificazione economica, in particolare se concentrate in prossimità della chiusura dell'esercizio. Questa attività ha rappresentato la risposta specifica al rischio, sempre presunto, di *management override of controls*, con un focus mirato sulle aree in cui la discrezionalità contabile è maggiore. In particolare, le scritture relative a stime, riclassificazioni e rettifiche di periodo sono state considerate maggiormente sensibili, poiché in esse il margine di giudizio manageriale risulta più ampio e, di conseguenza, più suscettibile di essere utilizzato in modo opportunistico per alterare l'andamento dei risultati o la posizione patrimoniale.

L'impianto così delineato consente di collegare puntualmente i rischi di frode individuati con risposte di audit proporzionate e documentate: il taglio improprio viene affrontato

con l’asse combinata contratti–cut-off–analitiche–credit notes; il rischio “over time”/perdite è presidiato tramite verifiche documentali sullo stato di esecuzione, conferme/incassi successivi e test mirati sulle stime. (Documentazione interna di revisione: Risks of material misstatement, 2024)

Accanto all’area dei ricavi, ulteriori profili di rischio di frode sono stati individuati nel magazzino e nella gestione del portafoglio crediti. Con riferimento al magazzino, la particolare configurazione della Società – caratterizzata dalla presenza di un deposito centrale, di magazzini periferici e di circa 130 siti presso ospedali e centri assistiti – comporta un’elevata esposizione in termini di volume e complessità delle movimentazioni. Al 31 dicembre 2024 il valore complessivo delle rimanenze ammontava a circa 29 milioni di euro. In considerazione della rilevanza quantitativa e della natura intrinsecamente rischiosa di quest’area, l’attività di revisione ha previsto, oltre alla comprensione e alla valutazione dei controlli interni, anche l’esecuzione di procedure sostanziali dirette, necessarie a ottenere evidenze probative sufficienti e appropriate in merito all’“existence” e alla corretta valutazione delle scorte. Tali procedure, note come *substantive procedures*, comprendono test di dettaglio e verifiche di coerenza sui dati contabili e documentali, finalizzate a raccogliere evidenze indipendentemente dall’affidabilità del sistema di controllo interno. A tal fine, il team ha partecipato a conte fisiche in un campione di magazzini significativi e ha svolto ulteriori substantive procedures, tra cui il *tracing* delle merci contate durante le osservazioni, test di cut-off alla data del 31.12.2024 e verifiche sulla valorizzazione delle giacenze in accordo con la policy aziendale. L’attenzione si è concentrata sul rischio di sopravvalutazione delle scorte, tipicamente connesso a possibili manipolazioni finalizzate a migliorare artificiosamente i risultati economici.

Un ulteriore ambito di rilievo nell’analisi dei rischi di frode è costituito dalla valutazione del fondo svalutazione crediti, che per la società esaminata rappresenta una delle aree più sensibili in termini di discrezionalità gestionale. Come già evidenziato, la Società opera in un mercato caratterizzato da ritardi nei pagamenti, soprattutto da parte della clientela pubblica. Per contenere tale rischio finanziario, sono state implementate diverse attività di controllo, monitoraggio e recupero dei crediti, che comprendono la gestione ordinaria delle sollecitazioni, il ricorso ad azioni legali e la sottoscrizione di contratti di factoring, per la cessione pro-soluto di crediti commerciali. Tali attività sono state oggetto di

specifico approfondimento attraverso colloqui con i responsabili aziendali coinvolti, al fine di valutarne l'effettiva applicazione e l'efficacia operativa.

Con riferimento ai crediti non ceduti, il management stima l'ammontare del fondo svalutazione attraverso un'analisi basata sulle posizioni creditizie dei clienti. La policy adottata prevede tre modalità principali:

1. **Valutazione specifica** dei crediti in contenzioso (extra-giudiziale o legale), effettuata con il coinvolgimento periodico dell'ufficio legale interno e dei consulenti esterni, per definire la corretta percentuale di recupero.
2. **Svalutazione al 100%** dei crediti di importo inferiore a 5.000 euro e con anzianità superiore a 720 giorni, pur restando soggetti a tentativi di recupero.
3. **Valutazione in base all'IFRS 9** per i crediti rimanenti relativi a fatture emesse (non svalutati e non intercompany).

Più nello specifico, la policy distingue tra fatture da emettere e fatture emesse. Nel primo caso, durante l'anno vengono effettuate valutazioni specifiche in occasione degli incontri mensili tra CFO e capi area per la verifica dei ricavi maturati e della recuperabilità delle posizioni creditorie. Se emerge l'impossibilità di recupero di determinate poste, si procede allo stanziamento specifico del fondo. Nel caso delle fatture già emesse, oltre alla valutazione specifica basata sullo status del credito, viene applicata la regola della svalutazione integrale per i crediti "under 5.000 euro" e con "aging over 720 giorni", mentre per le restanti posizioni (non svalutate e non intercompany) viene effettuata una valutazione generica in base ai criteri IFRS 9. La popolazione oggetto di analisi (Exposure at Default – EAD) comprende fatture emesse e fatture da emettere, suddivise tra clientela pubblica e privata. Sono escluse le posizioni già oggetto di valutazione specifica, le note di credito, i crediti coperti da assicurazioni, quelli oggetto di accordi di compensazione, i rapporti intercompany, i crediti ceduti o cedibili (in virtù dei contratti di factoring in essere), nonché le posizioni incassate nei mesi di gennaio e febbraio successivi alla chiusura. Alla popolazione così determinata vengono applicati i parametri previsti dall'IFRS 9: una Probability of Default (PD), distinta tra settore pubblico (rischio Paese Italia) e settore privato (principali società quotate), ponderata in base al peso percentuale delle due componenti sul totale, e una Loss Given Default (LGD) calcolata con criteri

specifici. Le attività di audit hanno incluso diverse *substantive procedures*, sviluppate con l'obiettivo di ottenere evidenze probative sufficienti e appropriate sulla corretta determinazione del fondo svalutazione crediti:

- **Quadratura tra monte crediti, partitario e contabilità generale**

  È stato eseguito un riconcilio dettagliato tra i saldi esposti in bilancio, i valori risultanti dal partitario clienti e quelli presenti in contabilità generale. Tale procedura ha consentito di verificare la coerenza interna dei dati, escludendo la presenza di scostamenti non giustificati e garantendo che la base di partenza per la stima del fondo fosse completa e affidabile.

- **Analisi della ragionevolezza degli accantonamenti specifici**

  Sono stati esaminati i principali crediti oggetto di svalutazione individuale (in contenzioso o di recuperabilità incerta), valutando la congruità delle percentuali di perdita stimate dal management. Questa attività ha incluso colloqui con l'ufficio legale interno e il confronto con le evidenze fornite dai consulenti esterni, così da verificare che le stime riflettessero correttamente lo stato delle procedure di recupero in corso.

- **Confronto con gli esercizi precedenti**

  È stata effettuata un'analisi retrospettiva delle percentuali di recupero dei crediti già svalutati negli esercizi passati, con lo scopo di valutare l'affidabilità storica del modello adottato e individuare eventuali scostamenti sistematici tra previsioni e risultati effettivi. Questa procedura ha rappresentato un elemento di giudizio sulla coerenza e la continuità applicativa della policy aziendale.

- **Verifica della valutazione effettuata secondo IFRS 9 mediante ricalcolo di PD e LGD**

  Il team di revisione ha ricostruito, su un campione significativo di posizioni, il calcolo della *Probability of Default* (PD) e della *Loss Given Default* (LGD), verificando la corretta applicazione delle metodologie previste dall'IFRS 9 e la coerenza delle assunzioni utilizzate. Particolare attenzione è stata riservata alla

distinzione tra clientela pubblica e privata, nonché all'adeguatezza delle fonti esterne utilizzate per determinare i parametri di rischio.

- **Monitoraggio delle modalità di accantonamento connesse alle operazioni di cessione pro-soluto**

  Sono stati analizzati i crediti oggetto di factoring pro-soluto, verificando che fossero correttamente esclusi dal perimetro della popolazione di analisi (EAD) e che gli effetti delle operazioni fossero contabilizzati in conformità ai principi contabili di riferimento. Questa attività ha permesso di accertare che il fondo svalutazione non includesse posizioni già trasferite al factor e che le cessioni fossero correttamente rappresentate in bilancio.

In stretta connessione con la gestione del fondo svalutazione crediti, anche le operazioni di cessione pro-soluto sono state ritenute meritevoli di specifica attenzione in ottica antifrode. Pur configurandosi come uno strumento ordinario di gestione della liquidità e di mitigazione del rischio di insolvenza, tali operazioni possono infatti prestarsi a utilizzi distorsivi finalizzati a migliorare artificiosamente la situazione finanziaria o a occultare posizioni deteriorate. In questo contesto, l'attività di revisione si è concentrata sulla verifica della corretta applicazione dei requisiti di *derecognition* previsti dall'IFRS 9, condizione necessaria per procedere alla cancellazione dei crediti dal bilancio. Le procedure di audit hanno incluso:

- **Circolarizzazione alle società di factoring**

  Sono state inviate richieste di conferma esterna agli intermediari con cui sono stati stipulati i contratti di cessione, per verificare l'effettiva esistenza delle operazioni, i termini contrattuali applicati e la corretta contabilizzazione degli importi ceduti.

- **Analisi della documentazione contrattuale e di supporto**

  È stata esaminata la documentazione relativa ai contratti di factoring e agli allegati di dettaglio, comprendenti l'elenco delle fatture emesse e da emettere oggetto di trasferimento, nonché eventuali modifiche o integrazioni contrattuali. Questa procedura ha consentito di verificare la coerenza tra gli accordi sottoscritti e la contabilizzazione effettuata.

- **Riconciliazione dei flussi finanziari**

  Sono stati confrontati i flussi finanziari registrati dalle società di factoring con gli incassi effettivi provenienti dai clienti terzi, al fine di accertare la corretta attribuzione degli importi e l'assenza di scostamenti non giustificati.

Tali controlli hanno permesso di verificare che le operazioni di cessione rispettassero integralmente le condizioni contrattuali e che fossero contabilizzate in conformità ai requisiti previsti dall'IFRS 9, con particolare riferimento al trasferimento sostanziale dei rischi e dei benefici. In questo modo è stato possibile accertare che i crediti oggetto di factoring fossero correttamente esclusi dal bilancio e che i flussi finanziari generati dalle operazioni trovassero adeguato riscontro nella documentazione di supporto e nelle registrazioni contabili.

Accanto ai rischi specifici emersi nelle singole aree di bilancio, è stato preso in considerazione anche il profilo del *management override of controls*, che rappresenta un rischio trasversale e, come precedentemente richiamato con riferimento all'ISA 240, deve essere valutato in ogni incarico di revisione in quanto potenzialmente incidente su qualsiasi posta contabile o processo aziendale. A differenza di altri rischi, infatti, l'override trae origine non da carenze strutturali del sistema di controllo interno, ma dalla posizione privilegiata che la direzione ricopre, che le consente di aggirare o neutralizzare i presìdi esistenti. In tale prospettiva l'attenzione si è concentrata in particolare sulle modalità attraverso cui la direzione potrebbe eludere i presìdi esistenti, ponendo in essere registrazioni contabili fittizie, modificando arbitrariamente le assunzioni e i giudizi utilizzati nelle stime o omettendo informazioni rilevanti. Ulteriori scenari analizzati hanno riguardato la possibilità di posticipare o anticipare la rilevazione di operazioni, nonché di intervenire sui termini economici di transazioni significative e inusuali, con l'effetto di incidere sulla rappresentazione del risultato d'esercizio e della posizione finanziaria. Per fronteggiare tali rischi, il presidio sull'override è stato sviluppato attraverso un insieme di procedure specifiche, calibrate sulle aree maggiormente esposte a discrezionalità. Tra queste, la revisione mirata delle *journal entries* ha rappresentato un passaggio centrale: l'analisi si è focalizzata sulle registrazioni effettuate in prossimità della chiusura del periodo, sugli importi atipici o privi di chiara giustificazione economica e sulle scritture aventi impatto significativo sul risultato d'esercizio. A supporto, è stata

condotta una ricomposizione critica delle evidenze giustificative, finalizzata a verificare la coerenza tra le registrazioni contabili e la documentazione sottostante.

Le verifiche hanno inoltre incluso l'esame di operazioni straordinarie, la valutazione delle riclassificazioni di poste rilevanti e l'analisi delle stime contabili significative, tutte aree caratterizzate da un elevato grado di discrezionalità gestionale e quindi particolarmente vulnerabili a possibili manipolazioni. L'insieme di tali procedure ha permesso di sviluppare una risposta mirata al rischio, sempre presunto, di management override, garantendo un approccio coerente con quanto richiesto dagli standard internazionali di revisione.

(Documentazione interna di revisione: SRM_Summary Review Memorandum, 2024) (Documentazione interna di revisione: Planned responses to significant risks and higher risk estimates)

3.2.3 Modalità di presidio attuate dalla società attraverso i controlli interni

Nel Capitolo 2 è stato analizzato il sistema di controllo interno così come descritto dalla società, con riferimento alle componenti strutturali, ai ruoli e alle funzioni coinvolte. In questa sede, invece, l'attenzione è rivolta alla concreta applicazione operativa dello stesso nei principali processi aziendali. L'obiettivo non è ancora quello di esprimere un giudizio di efficacia – che sarà oggetto di valutazione autonoma nel paragrafo successivo – bensì di illustrare come i presidi previsti dal framework trovino concreta applicazione nei principali cicli operativi, attraverso modalità organizzative, regole procedurali e controlli sistematici adottati dall'organizzazione. Di seguito vengono quindi descritte le modalità di presidio riscontrate, con particolare attenzione alle aree qualificate in sede di revisione come maggiormente esposte a rischio di frode – ossia il riconoscimento dei ricavi, la gestione del fondo svalutazione crediti e delle cessioni pro-soluto, la valutazione delle rimanenze di magazzino e, in via trasversale, il rischio di *management override of controls* – nonché ai principali *What Could Go Wrong* (WCGW) emersi dall'analisi dei cicli aziendali, ossia i potenziali scenari di errore o frode che i presidi sono chiamati a mitigare. A completamento dell'esposizione, tali collegamenti tra rischi e controlli sono sintetizzati nella tabella riportata, che presenta in forma schematica i presidi rilevati per ciascun WCGW in ciascun ciclo analizzato: la successiva trattazione li sviluppa invece in

maniera analitica e discorsiva, evidenziandone il funzionamento concreto nei processi aziendali.

Tabella 3 – Elaborazione dai documenti di revisione: sintesi dei principali WCGW e dei presidi di controllo individuati.

Ciclo	Fase	WCGW identificato	Presìdi di controllo rilevati
Attivo	Avvio servizio	Erogazione di servizi non autorizzati	Segregazione funzioni
Attivo	Registrazione	Emissione di fatture errate	Formalizzazione documentale
Attivo	Contabilizzazione	Errata contabilizzazione dei ricavi (cut-off)	Sistemi gestionali integrati + riconciliazioni e quadrature periodiche
Attivo	Rendicontazione	Errata determinazione del fondo svalutazione crediti	Procedure standardizzate e policy interne + controlli periodici e verifiche sostanziali
Passivo	Avvio ordine	Ordini non coerenti/non autorizzati	Formalizzazione documentale
Passivo	Registrazione	Mancata corrispondenza ODA–DDT–fattura	Formalizzazione documentale
Passivo	Contabilizzazione	Errata contabilizzazione accantonamenti fatture da ricevere	Riconciliazioni e quadrature periodiche

Passivo	Rendicontazione	Errori nella contabilizzazione dei costi da fatture ricevute	Riconciliazioni e quadrature periodiche
Tesoreria	Incassi diretti	Mancata rilevazione a sistema degli incassi già transitati sui conti bancari	Sistemi gestionali integrati
Tesoreria	Incassi diretti	Mancata riconciliazione incassi–fatture	Sistemi gestionali integrati
Tesoreria	Incassi factoring	Mancato riversamento al factor	Sistemi gestionali integrati
Tesoreria	Pagamenti	Pagamenti non autorizzati o da soggetti non abilitati	Segregazione funzioni + procedure standardizzate e policy interne
Magazzino	Movimentazioni	Uscite non giustificate/errate	Procedure standardizzate e policy interne
Magazzino	Movimentazioni	Entrate non giustificate/errate	Procedure standardizzate e policy interne
Magazzino	Movimentazioni	Mancato carico/scarico delle merci	Controlli periodici e verifiche sostanziali
Magazzino	Rendicontazione	Errata contabilizzazione delle rimanenze	Controlli periodici e verifiche sostanziali

Un primo presidio di carattere generale è rappresentato dalla formalizzazione documentale, che accompagna ogni fase rilevante dei processi e costituisce il presupposto per lo svolgimento delle attività successive. Nel ciclo attivo, ad esempio, l'avvio delle prestazioni è subordinato alla sottoscrizione di un contratto o a un ordine formale del

cliente: ciò riduce il rischio, particolarmente sensibile in quest'area, di riconoscere ricavi privi di titolo. In questa prospettiva, la formalizzazione documentale non solo funge da filtro preliminare all'erogazione dei servizi, ma diventa anche un presidio essenziale nella fase di registrazione contabile, poiché assicura la coerenza tra contratti, ordini e documentazione di supporto, limitando così la possibilità di errori nella fatturazione e di emissione di documenti incompleti o non corretti *(WCGW: emissione di fatture errate)*. (Documentazione interna di revisione: narrative ciclo attivo, 2024) Anche nel ciclo passivo, la formalizzazione documentale rappresenta un presidio chiave: ogni richiesta di materiale (Ri.Ma.) o di intervento (Ri.De.) deve essere trasformata in un ordine di acquisto (ODA) formalizzato, registrato a sistema e debitamente autorizzato, al quale devono corrispondere i documenti di supporto (ODA, documento di trasporto e fattura). Questo meccanismo garantisce che gli acquisti siano sempre tracciati e autorizzati, riducendo il rischio di emissione di ordini non coerenti con i fabbisogni o privi della necessaria approvazione *(WCGW: ordini di acquisto non coerenti/non autorizzati)*, e al tempo stesso assicura che la registrazione contabile avvenga solo sulla base di documentazione completa e coerente, limitando la possibilità di rilevare costi impropri o passività inesistenti *(WCGW: mancata corrispondenza ODA–DDT–fattura)*. (Documentazione interna di revisione: narrative ciclo passivo, 2024). Analogamente, nella gestione dei crediti la tracciabilità documentale di ogni posizione costituisce un presidio essenziale, poiché consente non soltanto di monitorare l'effettiva esigibilità delle somme, ma anche di fondare le stime sul fondo svalutazione su evidenze oggettive e verificabili. La disponibilità di contratti, ordini, solleciti e riscontri di pagamento permette infatti di ridurre significativamente la discrezionalità del management nella determinazione degli accantonamenti, contenendo il rischio che vengano mantenute a bilancio posizioni sopravvalutate o che non siano tempestivamente rilevate perdite attese. In quest'ottica, la base documentale non rappresenta un mero adempimento formale, bensì uno strumento sostanziale di presidio, che rafforza l'affidabilità complessiva delle valutazioni e limita gli spazi di possibili manipolazioni in un'area tradizionalmente esposta a rischio di frode.

Accanto alla formalizzazione documentale, un ruolo centrale è svolto dalla segregazione delle funzioni, che impedisce a un singolo soggetto di gestire in autonomia fasi critiche del processo e riduce, di conseguenza, il rischio di errori o comportamenti opportunistici.

Nel ciclo attivo, ad esempio, il processo di generazione dei ricavi è scandito da più livelli di responsabilità: i responsabili territoriali inseriscono i dati di fatturazione relativi alle commesse di propria competenza tramite un applicativo dedicato, ma la loro validazione è affidata all'ufficio contratti e alla funzione amministrativa, che verificano la coerenza delle informazioni immesse con i contratti sottoscritti e con le delibere di aggiornamento dei canoni. Tale presidio consente di ridurre il rischio che vengano avviati servizi non supportati da adeguata autorizzazione contrattuale, assicurando così che le attività erogate siano sempre giustificate da un titolo valido *(WCGW: erogazione di servizi non autorizzati).* Analoghi meccanismi di segregazione si riscontrano nel ciclo di tesoreria, dove le attività operative di predisposizione dei pagamenti sono affidate agli operatori della funzione, che attraverso PITECO elaborano le distinte e le caricano sulla piattaforma bancaria UniWeb. Le disposizioni diventano esecutive solo a seguito dell'autorizzazione finale, riservata al vertice aziendale, unico soggetto dotato delle credenziali personali necessarie per rendere effettivi i pagamenti presso la banca. In questo modo si mitiga il rischio che vengano processati pagamenti privi di autorizzazione o non coerenti con le fatture contabilizzate *(WCGW: pagamenti non autorizzati o da soggetti non abilitati)* (Documentazione interna di revisione: narrative ciclo tesoreria, 2024). In termini trasversali, la segregazione delle funzioni rappresenta un presidio essenziale non solo contro errori o anomalie operative, ma anche rispetto al rischio di management override. La frammentazione dei poteri decisionali lungo la catena autorizzativa, infatti, impedisce che un singolo soggetto possa gestire in maniera autonoma l'intero processo, riducendo le possibilità che la direzione aziendale o altri ruoli chiave possano aggirare i controlli stabiliti. La presenza di più livelli di verifica introduce un controllo reciproco permanente, che rende tracciabili le responsabilità e limita la discrezionalità individuale, rafforzando così l'affidabilità complessiva del sistema.

Un ulteriore livello di presidio è garantito dall'impiego di sistemi gestionali integrati (D365, PITECO, UniWeb), che assicurano tracciabilità e automazione dei flussi, riducendo la possibilità di interventi discrezionali non giustificati. Nel ciclo attivo, l'interfaccia tra il gestionale di fatturazione e la contabilità generale assicura che i dati caricati confluiscano direttamente nelle registrazioni contabili, senza passaggi intermedi suscettibili di errori o manipolazioni. In questo modo si riduce il rischio di discrepanze o di imputazioni non corrette dei ricavi a bilancio *(WCGW: errata contabilizzazione dei*

ricavi). Nel ciclo di tesoreria, l'integrazione tra i sistemi PITECO e UniWeb consente un monitoraggio quotidiano dei flussi finanziari, assicurando che ogni incasso transitato sul conto bancario venga correttamente recepito e registrato nel gestionale. In questo modo si riduce sia il rischio che somme effettivamente riscosse non vengano rilevate e rimangano erroneamente esposte come crediti in bilancio *(WCGW: mancata rilevazione a sistema degli incassi già transitati sui conti bancari)*, sia il rischio che gli incassi non vengano riconciliati con le relative fatture e restino sospesi *(WCGW: mancata riconciliazione incassi- fatture)*. Anche per le operazioni di cessione pro-soluto, l'interconnessione dei sistemi consente di tracciare in maniera coerente le fatture cedute e i relativi flussi finanziari. In questo modo, qualora un cliente effettui il pagamento direttamente alla società invece che al factor, il sistema permette di intercettare tempestivamente l'anomalia e di attivare la procedura di riversamento prevista contrattualmente. La possibilità di monitorare costantemente la corrispondenza tra incassi registrati e posizioni cedute consente quindi di mitigare il rischio che i crediti non vengano correttamente riversati al factor. *(WCGW: mancato riversamento al factor)*. L'evidenza applicativa, in questo senso, è che la tracciabilità intrinseca garantita dai sistemi gestionali integrati e l'automatizzazione dei passaggi chiave riducono significativamente i margini di intervento manuale non motivato, costituendo un ulteriore freno a potenziali condotte di override. La centralizzazione dei dati e la loro elaborazione all'interno di piattaforme uniche e interconnesse (D365, PITECO, UniWeb) assicurano infatti che ogni registrazione sia riconciliata con le fonti originarie e resa tracciabile, rendendo più difficile l'inserimento o la modifica arbitraria delle operazioni. In tal modo, l'impiego dei sistemi integrati non solo riduce il rischio di errori materiali, ma rappresenta anche un presidio strutturale contro possibili pratiche di management override, poiché le operazioni restano vincolate a un flusso standardizzato e verificabile in ogni fase.

Di particolare rilievo risultano anche i meccanismi di riconciliazione e quadratura periodica, che costituiscono un presidio trasversale volto a intercettare tempestivamente errori o anomalie. Nel ciclo attivo, ad esempio, viene effettuata una quadratura mensile tra gestionale e contabilità per i ricavi a canone: questo controllo assicura la coerenza tra le fonti informative e garantisce la corretta imputazione temporale delle entrate, riducendo il rischio di registrare ricavi in periodi non corretti *(WCGW: errata contabilizzazione dei ricavi).* Nel ciclo passivo, con cadenza mensile il controller interno

estrae dal sistema un report che distingue tra fatturato contabilizzato e fatturato ancora da ricevere, procedendo a una verifica della congruità degli importi e della correttezza delle rilevazioni relative agli accantonamenti. Questo presidio periodico consente di intercettare eventuali scostamenti rispetto ai dati attesi e di correggere tempestivamente errori di imputazione. In tal modo viene ridotto il rischio che vengano iscritti accantonamenti eccessivi o insufficienti *(WCGW: Errata contabilizzazione accantonamenti fatture da ricevere)*, ma anche che si verifichino errori nella contabilizzazione dei costi derivanti dalle fatture ricevute *(WCGW: errori nella contabilizzazione dei costi da fatture ricevute)*, con conseguente maggiore attendibilità della rappresentazione contabile delle passività.

La società ha inoltre definito procedure standardizzate e policy interne che regolano in maniera puntuale le diverse fasi operative, fornendo un quadro di riferimento uniforme che riduce il rischio di errori o comportamenti discrezionali. Nel ciclo di magazzino, ad esempio, la policy che distingue fra merci di consumo – gestite centralmente – e merci spot – acquistabili solo previa autorizzazione rappresenta un presidio fondamentale. Questa regola interna, imponendo modalità di approvvigionamento differenziate e sottoposte a controlli preventivi, rappresenta un presidio volto a garantire che ogni movimentazione sia giustificata e registrata secondo procedure codificate. In tal modo, la policy contribuisce a ridurre il rischio che vengano effettuati carichi o scarichi privi di adeguato supporto o erroneamente contabilizzati *(WCGW: Entrate e Uscite non giustificate/errate)*. Nel ciclo di tesoreria, la policy che vieta l'esecuzione di pagamenti in assenza della relativa fattura contabilizzata in D365 si configura come una barriera diretta contro l'effettuazione di uscite non autorizzate. Tale meccanismo assicura che ogni pagamento sia fondato su un titolo contabile valido e autorizzato, riducendo il rischio che somme vengano erogate in modo improprio o senza giustificazione *(WCGW: pagamenti non autorizzati o da soggetti non abilitati)*. Un ulteriore ambito presidiato riguarda la gestione dei crediti. La società ha formalizzato regole di svalutazione che prevedono, tra l'altro, l'integrale svalutazione dei crediti di importo inferiore a 5.000 euro o con anzianità superiore a 720 giorni. Questa policy contribuisce a contenere il rischio che vengano mantenute a bilancio posizioni prive di reali prospettive di incasso e, allo stesso tempo, riduce la discrezionalità del management nella determinazione degli accantonamenti. Ne deriva una maggiore affidabilità delle stime e una valutazione prudente del portafoglio

crediti, che limita l'eventualità di accantonamenti non coerenti con il reale grado di rischiosità delle esposizioni *(WCGW: Errata determinazione del fondo svalutazione crediti).*

Infine, un presidio ulteriore è costituito dai controlli periodici e dalle verifiche sostanziali, strumenti che rafforzano l'affidabilità complessiva del sistema. A differenza delle riconciliazioni e delle quadrature, che operano in maniera sistematica sulle registrazioni contabili, questi controlli si caratterizzano per un approccio selettivo e sostanziale, volto a validare con evidenze dirette – come verifiche fisiche e analisi mirate – la correttezza dei dati riportati nei sistemi. Nel magazzino, ad esempio, i controlli periodici comprendono sia le conte inventariali, svolte con cadenza annuale e in momenti intermedi, sia la valorizzazione periodica delle giacenze, che consente di monitorarne l'andamento e di individuare eventuali scostamenti da approfondire. Questi strumenti concorrono a garantire la correttezza dei dati relativi alle rimanenze e rappresentano una difesa significativa contro possibili fenomeni di sopravvalutazione *(WCGW: errata contabilizzazione delle rimanenze)*. Le medesime attività permettono inoltre di individuare eventuali omissioni nei carichi o scarichi, consentendo di riallineare tempestivamente i dati contabili alle risultanze fisiche *(WCGW: mancato carico/scarico delle merci)*. (Documentazione interna di revisione: narrative ciclo magazzino, 2024) Parallelamente, il monitoraggio periodico del fondo svalutazione crediti, effettuato tramite incontri mensili tra la direzione amministrativa (CFO) e i capi area, consente di valutare la recuperabilità delle fatture da emettere e di aggiornare le stime sulla base di evidenze concrete. Questo approccio riduce il rischio che vengano mantenuti accantonamenti inadeguati o non coerenti con lo stato effettivo dei crediti *(WCGW: errata determinazione del fondo svalutazione crediti)*.

Nel complesso, i presidi interni si delineano come un sistema articolato e trasversale, fondato su una pluralità di strumenti – quali la formalizzazione documentale, la segregazione delle funzioni, l'impiego di sistemi gestionali integrati, i meccanismi di riconciliazione periodica, le policy operative e le attività di verifiche periodiche – che governano in maniera sistematica le diverse fasi dei principali cicli aziendali. La loro applicazione contribuisce a garantire tracciabilità, coerenza e uniformità nelle procedure, riducendo gli spazi di discrezionalità nella gestione quotidiana e ponendo particolare attenzione alle aree di bilancio considerate più sensibili sotto il profilo del rischio di frode,

quali il riconoscimento dei ricavi, la gestione del portafoglio crediti e la valorizzazione delle rimanenze di magazzino. La ricostruzione condotta in questa sede ha avuto l'obiettivo di descrivere le modalità di presidio attuate dalla società, senza formulare valutazioni sul relativo grado di efficacia: tale giudizio sarà oggetto del paragrafo successivo, al termine della sistematica analisi delle attività di revisione svolte in ottica antifrode. (Documentazione interna di revisione: SRM_Summary Review Memorandum, 2024)

3.3 Risultati dell'analisi e implicazioni per il miglioramento del sistema antifrode

L'analisi ha preso in esame i processi aziendali e le aree considerate maggiormente esposte al rischio di frode, con l'obiettivo di verificare in che misura il sistema di controllo interno sia strutturato e applicato in modo da garantire un'adeguata prevenzione delle irregolarità. In questo contesto, è stato osservato non soltanto l'assetto formale dei presidi, ma anche il loro funzionamento operativo, così da comprendere se i controlli siano effettivamente integrati nelle attività quotidiane e idonei a ridurre i rischi residui.

La valutazione si è sviluppata lungo due direttrici complementari: da un lato, l'identificazione dei punti di forza del sistema, ovvero di quelle procedure e di quei presidi che, per livello di formalizzazione e grado di applicazione, contribuiscono a rendere il modello complessivamente robusto; dall'altro lato, l'individuazione di possibili aree di miglioramento o di aspetti che, se adeguatamente rafforzati, potrebbero incrementare ulteriormente l'efficacia del sistema stesso.

I risultati che ne derivano assumono quindi un carattere duplice: essi forniscono un quadro dell'effettiva efficacia del sistema di controllo interno nella prevenzione delle frodi, ma al tempo stesso costituiscono la base informativa per l'individuazione di margini di miglioramento. In tale prospettiva, le considerazioni che seguono saranno articolate in due sottoparagrafi: il primo (3.3.1) volto a esprimere un giudizio sull'efficacia del sistema, il secondo (3.3.2) dedicato allo svolgimento di una gap analysis, finalizzata a mettere in luce le principali aree di miglioramento e le opportunità di rafforzamento.

3.3.1 Giudizio sull' efficacia del sistema di controllo interno in ottica antifrode

Nella fase conclusiva del lavoro di revisione, il team ha condotto una riflessione sistematica volta a verificare la coerenza tra i rischi identificati in fase di pianificazione e le procedure effettivamente eseguite, con particolare riferimento ai rischi significativi e ai rischi di frode, incluso il rischio presunto di *management override of controls*. Tale analisi ha avuto l'obiettivo di valutare se gli interventi svolti fossero adeguati a fornire evidenze sufficienti e appropriate in risposta ai rischi di errori significativi identificati, in coerenza con quanto previsto dall'ISA 330 – *Auditor's Responses to Assessed Risks*, che impone al revisore di progettare e implementare procedure di revisione mirate in funzione dei rischi valutati. (IAASB, 2015)

Un punto particolarmente rilevante di tale riflessione consiste nel raccordo con quanto emerso dal Capitolo 2. In quella sede, è stata descritta la mappatura dei rischi-reato ex D.Lgs. 231/2001, predisposta dalla società come parte integrante del proprio Modello di Organizzazione, Gestione e Controllo. Tale strumento si colloca in una prospettiva tipicamente endogena, in quanto individua le aree aziendali a rischio di reato (con particolare attenzione ai reati societari e finanziari), ne valuta l'esposizione sulla base delle attività sensibili e definisce presidi organizzativi, procedurali e informativi destinati a prevenirne la commissione. La logica sottesa è quella di un sistema di compliance preventiva, volto a ridurre l'esposizione dell'ente a responsabilità amministrativa, danni reputazionali e conseguenze patrimoniali derivanti da condotte illecite.

Diverso è l'angolo prospettico adottato nel Capitolo 3, che riflette l'attività di revisione esterna svolta sul sistema di controllo interno. Qui l'attenzione non si concentra sul rischio-reato in senso giuridico, ma sulla capacità dei presidi effettivamente attuati di garantire la correttezza e l'attendibilità dell'informativa economico-finanziaria e di ridurre il rischio di frodi contabili, come previsto dall'ISA 240 – *The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements.* (IAASB, 2009) In altre parole, mentre la società – attraverso la mappatura dei rischi – persegue un obiettivo di prevenzione generale e di conformità normativa, il revisore verifica se i controlli siano concretamente operativi ed efficaci nel ridurre il rischio di errori significativi e manipolazioni nei bilanci.

La scelta di presentare dapprima la mappatura dei rischi e i presìdi delineati nei documenti aziendali, e successivamente i controlli effettivamente riscontrati in sede di revisione, risponde all'esigenza di valutare l'efficacia complessiva del sistema di controllo interno. Solo attraverso il confronto tra il disegno formale dei protocolli di prevenzione e la loro concreta applicazione operativa è infatti possibile cogliere il grado di coerenza e di affidabilità del sistema in ottica antifrode.

In primo luogo, è stata valutata la capacità delle procedure sostanziali di fornire evidenze affidabili in relazione ai rischi caratterizzati da un livello più elevato di stima, così da assicurare la copertura delle aree a maggiore sensibilità informativa. Particolare attenzione è stata riservata alle aree caratterizzate da giudizi discrezionali del management, come la determinazione del fondo svalutazione crediti, la valutazione delle rimanenze e la gestione delle operazioni di cessione pro-soluto, nelle quali la discrezionalità gestionale può costituire un fattore di rischio in ottica antifrode. Parallelamente, sono state esaminate le aree con rischio intrinseco maggiore – ad esempio la corretta rilevazione dei ricavi a canone e delle prestazioni spot – per accertare che i presidi operativi descritti fossero in grado di garantire un tracciamento completo e verificabile dei flussi, riducendo così la possibilità di registrazioni fittizie o anticipate.

Un ulteriore momento di valutazione ha riguardato la qualità e l'affidabilità delle evidenze raccolte. Il team di revisione ha discusso l'eventuale presenza di dubbi sull'attendibilità dei dati acquisiti e ha verificato la coerenza tra le diverse fonti probative, concludendo che eventuali incongruenze sono state affrontate e risolte in modo soddisfacente. È stato inoltre verificato che le informazioni messe a disposizione dalla società fossero supportate da un'adeguata documentazione, tale da consentire la ricostruzione puntuale dei processi e la verifica dell'operatività dei controlli interni, come richiesto dall'ISA 500 – *Audit Evidence*. (IAASB, 2009) In questa prospettiva, è stato accertato che la documentazione predisposta descrivesse accuratamente il funzionamento dei processi (SCOT), evidenziando i *What Could Go Wrong* (WCGW) e i relativi presidi di mitigazione. (Documentazione interna di revisione: Conclude on audit evidence for significant risks and estimates, 2024)

Oltre all'analisi dei cicli operativi, un elemento di rilievo è stato il test of IPE (Information Provided by the Entity). Considerato che i report e le estrazioni prodotte dai sistemi

informativi rappresentano la base delle verifiche, è stato necessario accertarne preliminarmente completezza, accuratezza e affidabilità. Il test ha riguardato la correttezza dei parametri di estrazione, la coerenza dei dati trasferiti nei sistemi di *end user computing* e l'assenza di manipolazioni manuali non tracciate. L'esito positivo ha permesso di considerare le IPE come evidenze probative affidabili, confermando l'affidabilità dei sistemi informativi aziendali e rafforzando indirettamente l'efficacia complessiva del sistema dei controlli interni. (Documentazione interna di revisione: test IPE – Information Provided by Entity (Excel), 2024)

Con riferimento ai singoli cicli, l'analisi ha confermato che: nel ciclo attivo, non sono emersi indicatori di debolezza nelle policy aziendali, che hanno supportato il corretto flusso delle transazioni dalla stipula contrattuale fino alla contabilizzazione dei ricavi; nel ciclo passivo, i controlli a presidio della corrispondenza tra richieste di acquisto, ordini, documenti di trasporto e fatture hanno assicurato la corretta imputazione dei costi e l'assenza di passività occulte; nel magazzino, la combinazione tra verifiche di cut-off, conte fisiche e policy di valorizzazione ha ridotto il rischio di sopravvalutazione delle scorte, area tradizionalmente sensibile in ottica antifrode; nel ciclo di tesoreria, i meccanismi di riconciliazione dei movimenti bancari e la segregazione dei ruoli nelle autorizzazioni di pagamento hanno costituito un presidio efficace contro errori e transazioni non autorizzate.

Un aspetto trasversale emerso riguarda il rischio di management override. Pur trattandosi di un rischio insito in qualunque sistema di controllo interno, la presenza di procedure formalizzate, la tracciabilità garantita dai sistemi gestionali integrati e la separazione delle funzioni riducono sensibilmente i margini di intervento discrezionale non autorizzato. L'emersione di tale rischio risulta coerente con quanto previsto dalla mappatura 231, che già individuava nei reati di false comunicazioni sociali e di impedito controllo un ambito specificamente legato a possibili condotte elusive da parte della dirigenza.

Infine, particolare rilievo ha assunto il dialogo con gli organi di governance. Nel corso della revisione, sono stati condivisi i rischi significativi individuati, le aree di maggiore esposizione a frodi e i risultati preliminari delle verifiche, anche con riferimento alle potenziali aree qualificabili come Key Audit Matters (KAM). Tali aspetti, definiti dall'ISA 701 – *Communicating Key Audit Matters in the Independent Auditor's Report*,

corrispondono a quelle aree che, a giudizio del revisore, hanno richiesto la maggiore attenzione nel corso dell'audit e che vengono quindi comunicate nella relazione di revisione per accrescere la trasparenza informativa verso gli stakeholder. (IAASB, 2016) Questo flusso informativo ha garantito la piena consapevolezza da parte degli organi preposti alla supervisione, rafforzando il ruolo di accountability e il presidio complessivo sul sistema antifrode.

Nel complesso, la revisione ha consentito di esprimere un giudizio positivo sull'efficacia del sistema di controllo interno in ottica antifrode. Non sono state rilevate frodi effettive o sospette, né carenze significative nei controlli. I presidi attuati dalla società – documentazione formale, segregazione delle funzioni, riconciliazioni sistematiche, policy operative, monitoraggi periodici e affidabilità delle IPE – si sono dimostrati coerenti con i rischi individuati e hanno fornito un quadro di governance solido. Le verifiche condotte sulle aree più sensibili – ricavi, fondo svalutazione crediti, operazioni di cessione pro-soluto e magazzino – non hanno fatto emergere anomalie significative, confermando l'affidabilità delle rilevazioni e la capacità preventiva del sistema di controllo interno. Il confronto con la mappatura dei rischi-reato esaminata nel Capitolo 2 evidenzia che i presidi descritti non si esauriscono in un adempimento formale, ma trovano effettivo riscontro nelle procedure operative e nelle verifiche di revisione, delineando un sistema di prevenzione multilivello che integra la compliance normativa con le esigenze di attendibilità del bilancio. L'approccio di revisione è stato così improntato al *reliance sui controlli*[10], riconoscendo la loro capacità preventiva e calibrando di conseguenza l'estensione delle verifiche sostanziali, come previsto dall'ISA 330. (IAASB, 2015) Tale scelta non rappresenta un mero aspetto metodologico, ma costituisce la naturale conseguenza dell'efficacia dei presidi in ottica antifrode, che si configurano come strumenti concreti di mitigazione dei rischi e non come semplici formalità. Pur in un quadro complessivamente positivo, l'analisi ha tuttavia evidenziato alcuni margini di miglioramento, non tanto in termini di carenze strutturali, quanto piuttosto di opportunità di rafforzamento dei controlli e di maggiore tempestività nel monitoraggio. Tali aspetti, che verranno approfonditi nel paragrafo successivo,

[10] Per ***reliance sui controlli*** si intende l'approccio di revisione che attribuisce rilevanza ai controlli interni dell'azienda, ritenendoli sufficientemente affidabili da ridurre l'estensione delle verifiche sostanziali. In tal modo, il revisore calibra la propria attività considerando i presidi interni come strumenti efficaci di prevenzione e rilevazione di errori o frodi.

riguardano l'ottimizzazione dell'efficienza dei presidi e l'ulteriore potenziamento della capacità preventiva del sistema in ottica antifrode. (Documentazione interna di revisione: SRM_Summary Review Memorandum, 2024) (Documentazione interna di revisione: bilancio società , 2024)

3.3.2 Gap Analysis: principali debolezze e aree di miglioramento

L'analisi svolta ha confermato la sostanziale efficacia del sistema di controllo interno in ottica antifrode, ma ha anche permesso di individuare alcuni profili di debolezza residua e potenziali aree di miglioramento. Questi aspetti non inficiano la solidità complessiva del modello, ma suggeriscono margini di evoluzione, soprattutto in termini di tempestività dei presidi, adattabilità alle mutevoli condizioni operative e capacità di gestione del rischio residuo.

Una prima criticità riguarda la frequenza dei controlli, che in molti casi si sviluppano su base periodica (mensile, trimestrale o annuale). Sebbene tale impostazione sia coerente con gli standard tradizionali di revisione e di controllo interno, essa introduce inevitabilmente un margine temporale in cui eventuali anomalie o tentativi di manipolazione possono non essere immediatamente intercettati. Ad esempio, la quadratura dei ricavi a canone viene eseguita con cadenza mensile, la valorizzazione del magazzino è effettuata mensilmente ma accompagnata da una verifica fisica solo al 31 dicembre, mentre le valutazioni sul fondo svalutazione crediti vengono discusse in incontri mensili tra il CFO e i capi area. Questo intervallo temporale tra una verifica e l'altra rappresenta un potenziale punto debole: anomalie di rilievo, se commesse in periodi intermedi, potrebbero restare inosservate fino al controllo successivo, riducendo la capacità preventiva del sistema e aumentando il rischio che manipolazioni deliberate o errori materiali abbiano effetti rilevanti sul bilancio. In contesti caratterizzati da complessità operativa crescente e da un'elevata esposizione al rischio di frode, la sola periodicità può quindi rivelarsi insufficiente.

Una seconda area di debolezza riguarda la dipendenza, seppur residua, dal controllo manuale. Nonostante l'ampio utilizzo di sistemi gestionali integrati (D365, PITECO, UniWeb), che garantiscono un livello elevato di automazione e tracciabilità, alcune attività di verifica restano affidate al personale amministrativo. Un esempio significativo è rappresentato dalla quadratura mensile dei ricavi a canone, condotta manualmente dal

controller attraverso il confronto tra dati gestionali e registrazioni contabili. Pur trattandosi di una fase inserita in un contesto informatizzato e destinata a garantire coerenza, la presenza di un margine di discrezionalità lascia aperto uno spazio di rischio, legato tanto a possibili errori involontari quanto a interventi opportunistici. In ottica antifrode, infatti, anche una componente manuale residuale può costituire un punto di vulnerabilità, in quanto aumenta la possibilità che il management possa incidere sulle registrazioni per aggirare i controlli standardizzati o manipolare i dati contabili.

Accanto a tale criticità, si evidenzia inoltre la rigidità delle policy operative, che, se da un lato garantisce prudenza e coerenza con i principi contabili, dall'altro può ridurre la capacità del sistema di adattarsi alle specificità dei diversi contesti operativi. Un esempio emblematico è la regola che impone la svalutazione integrale dei crediti inferiori a 5.000 euro o con anzianità superiore a 720 giorni: una misura che contribuisce a rafforzare la prudenza nelle valutazioni, ma che rischia di non rappresentare fedelmente la natura di talune esposizioni. Nei rapporti con la Pubblica Amministrazione, ad esempio, crediti di importo contenuto o con tempi di incasso fisiologicamente lunghi non necessariamente riflettono una condizione di effettiva inesigibilità. In tali casi, l'applicazione rigida della policy può portare a svalutazioni eccessive, con effetti non sempre coerenti rispetto alla reale rischiosità del portafoglio crediti. In prospettiva antifrode, questo approccio riduce sì gli spazi di arbitrio gestionale, ma al prezzo di una minore tempestività e aderenza alla rappresentazione fedele, con il rischio di sacrificare la qualità informativa del bilancio a favore di un formalismo difensivo.

Alla luce di queste debolezze, la letteratura più recente propone l'introduzione di approcci tecnologici avanzati, basati su strumenti di *continuous auditing* e *machine learning*. L'adozione di tali soluzioni rappresenta un'evoluzione naturale dei sistemi di controllo interno, in quanto consente di superare il limite dei controlli periodici e retrospettivi, trasformandoli in un processo di monitoraggio pressoché real-time, capace di intercettare tempestivamente anomalie nei dati finanziari e operativi. (Ghafar I. ; Perwitasari W. ; Kurnia R., 2024) (Tharouma S.; Oudai M., 2022)

Nel ciclo attivo, ad esempio, l'impiego di algoritmi di *anomaly detection* applicati ai ricavi permetterebbe di analizzare grandi moli di dati storici e correnti, individuando pattern incoerenti rispetto alla consuetudine contrattuale o alla stagionalità delle

prestazioni. In tal modo sarebbe possibile segnalare rapidamente potenziali fenomeni di ricavi fittizi o anticipati, che rappresentano una delle aree più esposte a rischio di frode.

Nel ciclo crediti, modelli predittivi di *machine learning* potrebbero stimare con maggiore precisione il rischio di default dei clienti, superando la rigidità di regole fisse come la svalutazione automatica oltre una certa soglia o anzianità. Tali strumenti, elaborando dati storici di pagamento, indicatori settoriali e variabili macroeconomiche, consentirebbero di personalizzare la stima del rischio di insolvenza e di calibrare più accuratamente il fondo svalutazione, garantendo un equilibrio migliore tra prudenza, tempestività e rappresentazione fedele delle esposizioni.

Nel ciclo di magazzino, l'applicazione di algoritmi di analisi automatica dei movimenti consentirebbe di effettuare confronti continui tra entrate e uscite di merci, segnalando eventuali discrepanze non rilevabili con i soli controlli periodici. Questo approccio ridurrebbe il rischio di sopravvalutazione delle giacenze e permetterebbe di individuare omissioni nei carichi o scarichi in tempi molto più rapidi rispetto alle tradizionali conte fisiche di fine anno.

Infine, nel ciclo di tesoreria, l'integrazione di sistemi di intelligenza artificiale sui flussi bancari potrebbe generare alert in caso di movimenti sospetti o incongruenti rispetto ai pattern abituali, consentendo di rilevare immediatamente pagamenti irregolari o non autorizzati. Ciò garantirebbe un rafforzamento significativo della capacità preventiva, andando oltre la riconciliazione periodica e introducendo un monitoraggio dinamico e proattivo delle transazioni. L'introduzione di tali strumenti non avrebbe l'effetto di sostituire i presidi attuali, bensì di potenziarne l'efficacia: la logica è quella di integrare i controlli documentali, le riconciliazioni e le policy esistenti con tecniche avanzate che riducono i tempi di rilevazione e ampliano la portata delle verifiche.

Un ulteriore ambito di miglioramento riguarda la gestione del rischio residuo, ossia quella quota di esposizione che non può essere del tutto eliminata attraverso i controlli interni, anche quando questi risultino ben disegnati e correttamente implementati. In ottica antifrode, infatti, nessun sistema di presidi – per quanto evoluto – è in grado di azzerare completamente la possibilità di condotte illecite o manipolazioni contabili. È in questo contesto che strumenti di *risk transfer*, come le polizze crime, assumono un ruolo strategico quale presidio complementare.

Le polizze crime rappresentano coperture assicurative specificamente progettate per tutelare l'azienda contro perdite patrimoniali derivanti da frodi interne o esterne, comprendendo, tra l'altro, fenomeni di appropriazione indebita, falsificazione di documenti contabili, manipolazione dei flussi finanziari e frodi informatiche. La loro funzione non è preventiva in senso stretto, ma di resilienza finanziaria, consentendo all'impresa di contenere l'impatto economico qualora i controlli interni dovessero rivelarsi inefficaci o aggirati.

Nel corso di un secondo stage svolto nell'area ERM & Insurance di una primaria realtà italiana, ho avuto modo di approfondire il funzionamento di queste coperture, riscontrando la loro applicabilità in contesti caratterizzati da volumi elevati di transazioni e da una pluralità di rapporti con controparti pubbliche e private. In tali scenari, infatti, la probabilità che si verifichino eventi fraudolenti non è trascurabile, e la polizza crime si configura come uno strumento in grado di completare l'architettura difensiva aziendale, integrando i controlli con un livello ulteriore di protezione patrimoniale. La rilevanza di questo presidio complementare emerge con particolare evidenza in una prospettiva di sistema multilivello di difesa: da un lato, i controlli interni svolgono la funzione primaria di prevenzione e di rilevazione tempestiva delle anomalie; dall'altro, la polizza crime garantisce una risposta residuale, trasferendo parte del rischio a un soggetto esterno (l'assicuratore) e assicurando la sostenibilità economica dell'impresa anche in presenza di eventi fraudolenti non intercettati. Per queste ragioni ho ritenuto tale strumento applicabile al presente lavoro di tesi, nella logica di un rafforzamento del sistema di controllo interno in ottica antifrode. È tuttavia evidente che l'adozione di una polizza crime debba essere considerata e calibrata in base alla realtà aziendale di riferimento, alle sue dimensioni, al settore di appartenenza e al profilo di rischio specifico.

In sintesi, la gap analysis condotta ha evidenziato come il sistema di controllo interno della società, pur robusto, presenti margini di miglioramento in tre direzioni principali:

1. **Riduzione del gap temporale** il manifestarsi di un rischio e la sua rilevazione, attraverso l'adozione di tecnologie di audit continuo e sistemi di monitoraggio in tempo reale;
2. **Affinamento delle policy operative**, così da coniugare prudenza, tempestività e rappresentazione fedele delle operazioni aziendali;

3. **Gestione del rischio residuo mediante strumenti assicurativi**, quali le polizze crime, che integrano i controlli interni con una forma di protezione finanziaria capace di ridurre l'impatto economico di eventuali frodi non prevenute.

Questi interventi, se implementati, consentirebbero di rafforzare ulteriormente l'efficacia del sistema antifrode, trasformandolo in un modello capace non solo di prevenire e rilevare, ma anche di garantire una gestione più strutturata e proattiva dei rischi residui, in linea con le più recenti evoluzioni della corporate governance e del risk management.

CONCLUSIONI

Il presente lavoro di tesi ha preso avvio dall'interrogativo circa la capacità del sistema di controllo interno di costituire un presidio realmente efficace nella prevenzione delle frodi aziendali, verificandone l'effettiva operatività attraverso l'applicazione delle metodologie proprie del *fraud audit*.

L'analisi teorica ha permesso di delineare le basi concettuali e normative che sostengono il ruolo del revisore e dell'internal auditor nella gestione dei rischi di frode, evidenziando come le best practices più recenti abbiano progressivamente rafforzato la centralità di un approccio multilivello, integrato e proattivo ai controlli. In questo quadro, il *fraud audit* si configura come un'estensione critica dell'attività di revisione, non limitata alla mera rilevazione ex post, ma orientata alla prevenzione e alla mitigazione preventiva del rischio.

Il caso aziendale analizzato ha consentito di osservare concretamente come un sistema di controllo interno possa essere strutturato per rispondere alle esigenze di prevenzione del rischio di frode. La ricostruzione della cornice organizzativa e procedurale ha messo in luce la presenza di un modello articolato, fondato su policy specifiche, procedure formalizzate e strumenti di monitoraggio che riflettono le prescrizioni normative e le prassi di settore. L'analisi empirica ha offerto l'opportunità di verificare la coerenza di tali presidi rispetto alle aree di rischio individuate dall'impresa, ponendo le basi per l'applicazione delle metodologie di *fraud audit* in ottica esterna.

L'attività di revisione condotta ha confermato la sostanziale solidità del sistema di controllo interno osservato, ma ha anche evidenziato alcuni profili di vulnerabilità che ne riducono la capacità preventiva. In particolare, la periodicità delle verifiche, la persistenza di controlli manuali e la rigidità di alcune policy operative rappresentano aree di possibile miglioramento. Tali aspetti non compromettono la validità complessiva del modello, ma ne limitano la tempestività e l'adattabilità, in un contesto in cui le frodi si caratterizzano per dinamicità e complessità crescente.

La gap analysis condotta ha suggerito come lo sviluppo dei sistemi di controllo interno possa trarre beneficio dall'introduzione di tecnologie avanzate di *continuous auditing* e *data analytics*, capaci di ridurre il divario temporale tra evento e rilevazione. È emersa inoltre l'esigenza di affinare le regole operative al fine di garantire un equilibrio più

efficace tra prudenza, rappresentazione fedele e capacità preventiva, nonché l'opportunità di integrare il sistema di controllo con strumenti di *risk transfer*, come le polizze *crime*, che forniscono una protezione complementare contro i rischi residui.

Nel loro insieme, queste evidenze confermano come il *fraud audit*, applicato in maniera metodologicamente rigorosa e integrato nell'assetto dei controlli aziendali, rappresenti un presidio di particolare rilevanza per la prevenzione delle frodi. Il suo valore non risiede soltanto nella capacità di rilevare anomalie, ma soprattutto nella possibilità di orientare il sistema di controllo verso una gestione più dinamica e resiliente del rischio, in linea con i principi della corporate governance e del *risk management* contemporaneo.

La ricerca presenta inevitabilmente alcuni limiti, riconducibili principalmente al carattere monografico dello studio, basato sull'analisi di un singolo caso aziendale. Tale circostanza non consente di generalizzare i risultati, ma offre comunque spunti significativi per ulteriori approfondimenti, sia in termini comparativi su più realtà, sia in relazione all'applicazione di strumenti tecnologici innovativi al *fraud audit*.

In prospettiva, l'evoluzione dei sistemi di controllo interno dovrà confrontarsi sempre più con la necessità di coniugare i presidi tradizionali con le potenzialità offerte dalle tecnologie digitali, garantendo allo stesso tempo la sostenibilità economica delle soluzioni adottate. In questo scenario, il *fraud audit* continuerà a costituire uno strumento essenziale per l'evoluzione di modelli di governance che siano capaci non solo di prevenire e rilevare le frodi, ma anche di rafforzare la fiducia degli stakeholder nella trasparenza e nell'affidabilità delle informazioni aziendali.

BIBLIOGRAFIA E SITOGRAFIA

- Abdelatif, A., Nettour, D., Chaib, R., Verzea, I. & Bensehamdi, S. (2023). Improvement of enterprise risk visualization: risk mapping. *Technology Audit and Production Reserves*, vol. 6, pp. 20–27.
- Abdullahi, R. & Mansor, N. (2015). Fraud triangle theory and fraud diamond theory: understanding the convergent and divergent for future research. *International Journal of Academic Research in Accounting, Finance and Management Sciences*, vol. 5, no. 4, pp. 54–64.
- Acebes, F., González-Varona, J.M., López-Paredes, A. & Pajares, J. (2024). Beyond probability-impact matrices in project risk management: a quantitative methodology for risk prioritisation. *Humanities & Social Sciences Communications,* vol. 11.
- ACFE. (2024). Occupational fraud 2024: a report to the nations. *Association of Certified Fraud Examiners*.
- Airmic, Alarm, IRM. (2010). A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000. *Airmic, Alarm, IRM*.
- Al Karabsheh, F.I. (2021). The role of the external auditor to detect financial (fraud-corruption) in the financial statements of service corporations listed on the ASE. *Journal of Management Information and Decision Sciences*, vol. 24, Special Issue 4, pp. 1-15.
- Bonrath, A. & Euleric, M. (2023). Internal auditing's role in preventing and detecting fraud: an empirical analysis. *International Journal of Auditing*, vol. 28, pp. 615-631.
- Brazel, J.F., Carpenter, T.D. & Jenkins, J.G. (2010). Auditors' use of brainstorming in the consideration of fraud: reports from the field. *The Accounting Review*, vol. 85, no. 4, pp. 1273–1301.
- Carpenter, T.D. (2007). Audit team brainstorming, fraud risk identification, and fraud risk assessment: implications of SAS No. 99. *The Accounting Review*, vol. 82, no. 5, pp. 1119-1143.
- Cassa Depositi e Prestiti. (2025). Modello di Organizzazione, Gestione e Controllo ex D.Lgs. n. 231/2001. *Cassa Depositi e Prestiti S.p.A.*

https://www.cdp.it/internet/public/cms/documents/CDP-Modello-231-Parte-Generale-09-05-2025-ITA.pdf

- Center for Audit Quality (CAQ). (2024). The Role of the Auditor: Assessing and Responding to Fraud Risk. *Center for Audit Quality, Anti-Fraud Collaboration Report*.
- Confindustria. (2021). Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ai sensi del D. Lgs. 231/2001. *Confindustria*.
- Confindustria Dispositivi Medici. (2024). Linee guida per l'adozione dei modelli organizzativi ex D. Lgs. 231/2001 nel settore dei dispositivi medici. *Confindustria Dispositivi Medici*.
- Davis, N.A. & Harris, S.A. (2024). Leveraging machine learning models for real-time fraud detection in financial transactions. *International Journal of Computer Technology and Science*, vol. 1, no. 1, pp. 1–6.
- European Parliament. (2024). EU anti-fraud architecture – the role of EU-level players, how they cooperate and the challenges they face. *Policy Department for Budgetary Affairs, DG Internal Policies*. https://www.europarl.europa.eu/RegData/etudes/STUD/2024/763761/IPOL_STU%282024%29763761_EN.pdf
- Ghafar, I., Perwitasari, W. & Kurnia, R. (2024). The role of artificial intelligence in enhancing global internal audit efficiency: An analysis. *Asian Journal of Logistics Management*, vol. 3, no. 2, pp. 64-89.
- IAASB. (2009). International Standard on Auditing (ISA) 500 – Audit Evidence. *International Auditing and Assurance Standards Board*.
- IAASB. (2009). International Standard on Auditing (ISA) 240 (Revised) – The auditor's responsibilities relating to fraud in an audit of financial statements. *International Auditing and Assurance Standards Board*.
- IAASB. (2015). International Standard on Auditing (ISA) 330 – The auditor's responses to assessed risks. *International Auditing and Assurance Standards Board*.
- IAASB. (2016). International Standard on Auditing (ISA) 701 – Communicating key audit matters in the independent auditor's report. *International Auditing and Assurance Standards Board*.

- IAASB. (2019). International Standard on Auditing (ISA) 315 (Revised) – Identifying and assessing the risks of material misstatement. *International Auditing and Assurance Standards Board*.
- IAASB. (2020). International Standard on Auditing (ISA) 200 – Overall objectives of the independent auditor and the conduct of an audit in accordance with International Standards on Auditing. *International Auditing and Assurance Standards Board*.
- IAASB. (2024). Handbook of International Quality Management, Auditing, Review, Other Assurance, and Related Services Pronouncements. *International Auditing and Assurance Standards Board*. https://ifacweb.blob.core.windows.net/publicfiles/2024-08/IAASB-2023-2024-Handbook-Volume-1.pdf
- IIA, AICPA & ACFE. (2008). Managing the business risk of fraud. *The Institute of Internal Auditors, American Institute of Certified Public Accountants & Association of Certified Fraud Examiners*, pp 5-44.
- International Organization for Standardization (ISO). (2018). ISO 31000:2018 Risk management — Guidelines. *International Organization for Standardization*. https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en
- Kassem, R. (2023). External auditors' use and perceptions of fraud factors in assessing fraudulent financial reporting risk (FFRR): implications for audit policy and practice. *Security Journal*, vol. 37, pp. 875-902.
- Nichols, T. & Patterson, J. (2014). Social loafing: a review of the literature. *Journal of Management Policy and Practice*, vol. 15, no. 1, pp. 58–67.
- Lenel, A., Temple-Bird, C., Kawohl, W. & Kaur, M. (2005). How to organize a system of healthcare technology management. *How to Manage Series for Healthcare Technology*. *Ziken International, in collaboration with the World Health* Organization.
- Lestari, P.A. & Edeh, F.O. (2024). The impact of regulatory frameworks on fraud detection in auditing. *Sinergi International Journal of Accounting & Taxation*, vol. 2, no. 1, pp. 15-26.

- Mahmoud, T., Balachandran, W. & Altayyar, S. (2024). Advancing sustainable healthcare technology management: Developing a comprehensive risk assessment framework with a fuzzy analytical hierarchy process. *Sustainability*, vol. 16.
- Mohd-Nassir, M.D., Mohd-Sanusi, Z. & Ghani, E.K. (2016). Effect of brainstorming and expertise on fraud risk assessment. *International Journal of Economics and Financial Issues*, vol. 6, Special Issue 4, pp. 62-67.
- National Institute of Standards and Technology (NIST). (2024). Enterprise Risk Management Quick-Start Guide. *NIST Special Publication SP-1303, National Institute of Standards and Technology*.
- PartsSource. (2024). State of Healthcare Technology Management Insights Report. *PartsSource*. *[Industry Report]*.
- PartsSource. (2025). Data driven contract management: Four best practices to reduce cost of equipment service without compromising on quality. *PartsSource [Industry Report]*.
- PCAOB. (2004). AS 2401: Considerazione della frode in un audit di bilancio. *Public Company Accounting Oversight Board*. Disponibile su: https://pcaobus.org/oversight/standards/auditing-standards/details/AS2401
- PCAOB. (2024). AS 2201: Un audit del controllo interno sulla rendicontazione finanziaria integrato con un audit dei bilanci. *Public Company Accounting Oversight Board*. https://pcaobus.org/oversight/standards/auditing-standards/details/AS2201
- PCAOB. (2024). Auditing standards of the Public Company Accounting Oversight Board. *Public Company Accounting Oversight Board*. https://pcaobus.org/oversight/standards/auditing-standards
- Quick, R. & Tümmler, M. (2024). How to detect fraud in an audit: a systematic review. *Springer*.
- Schafer, J. & Schafer, B. (2018). Interpersonal affect, accountability and experience in auditor fraud risk judgments and the processing of fraud cues. *Faculty Publications Kennesaw State University*, pp. 1-38.
- Tharouma, S. & Oudai, M. (2022). A review of the literature on internal audit in the era of digital transformation. *Journal of International Audit, Management & Computer Sciences, vol. 6, no. 4, pp. 215-225*.

- The Business Research Company. (2025). *Healthcare Technology Management Global Market Report 2025*. T*he Business Research Company*. https://www.thebusinessresearchcompany.com/report/healthcare-technology-management-global-market-report
- The Institute of Internal Auditors (IIA). (2019). Fraud and Internal Audit – IIA Position Paper: Assurance over fraud controls fundamental to success. *The Institute of Internal Auditors.*
- The Institute of Internal Auditors (IIA). (2024). Internal Auditing and Fraud: Assessing Fraud Risk Governance and Management at the Organizational Level, 3rd ed. *The Institute of Internal Auditors / Internal Audit Foundation*.
- Unione Europea. (1995). Regolamento (CE, Euratom) n. 2988/95 del Consiglio, del 18 dicembre 1995, relativo alla tutela degli interessi finanziari delle Comunità europee. *Gazzetta ufficiale delle Comunità europee*. https://eur-lex.europa.eu/eli/reg/1995/2988/oj/eng
- World Health Organization (WHO). (2017). Country data on health technology management. *WHO Medical Device Technical Series*, pp. 1–18
- Zattoni, A. (2015). *Corporate governance*. Egea (Milano).

Documentazione interna consultata:

- Documentazione interna di revisione (2024): *Bilancio società.*
- Documentazione interna di revisione (2024): *Conclude on audit evidence for significant risks and estimates.*
- Documentazione interna di revisione (2024): *Form laws and regulations.*
- Documentazione interna di revisione (2024): *Group Accounting Manual.*
- Documentazione interna di revisione (2024): *Identify significant classes of transactions (SCOTs).*
- Documentazione interna di revisione (2024): *Mappatura applicazioni gestionali e infrastrutture tecnologiche (Excel).*
- Documentazione interna di revisione (2024): *Narrative ciclo attivo*.
- Documentazione interna di revisione (2024): *Narrative ciclo magazzino*.
- Documentazione interna di revisione (2024): *Narrative ciclo passivo.*

- Documentazione interna di revisione (2024): *Narrative ciclo tesoreria.*
- Documentazione interna di revisione (2024): *Planned responses to significant risks and higher risk estimates.*
- Documentazione interna di revisione (2024): *PM TE and SAD nominal amount*.
- Documentazione interna di revisione (2024*): Risks of material misstatement*.
- Documentazione interna di revisione (2024): *SRM_Summary Review Memorandum.*
- Documentazione interna di revisione (2024): *Test IPE – Information Provided by Entity (Excel).*
- Documentazione interna fornita dalla società (2024): *Linee Guida di Gruppo per il Modello 231 - Sezione Governance aziendale, ruoli e responsabilità.*
- Documentazione interna fornita dalla società (2024): *Linee Guida di Gruppo per il Modello 231 - Sezione Principi di comportamento nelle principali aree di rischio.*
- Documentazione interna fornita dalla società (2024): *Linee Guida di Gruppo per il Modello 231 - Sezione Sistema integrato di controllo interno.*
- Documentazione interna fornita dalla società (2024): *Modello di Organizzazione, di Gestione e Controllo All. 2 Mappatura dei processi critici.*
- Documentazione interna fornita dalla società (2024): *Modello di Organizzazione, di Gestione e Controllo All. 3 Codice Etico.*
- Documentazione interna fornita dalla società (2024): *Modello di Organizzazione, di Gestione e Controllo All. 7 Flussi informativi verso l'ODV.*
- Documentazione interna fornita dalla società (2024): *Modello di Organizzazione, di Gestione e Controllo All. 8 Whistleblowing.*
- Documentazione interna fornita dalla società (2024): *Modello di Organizzazione, di Gestione e Controllo Parte generale - Sezione Il processo di gestione del rischio*.
- Documentazione interna fornita dalla società (2024): *Modello di Organizzazione, di Gestione e Controllo Parte Speciale "Reati Societari".*
- Documentazione interna fornita dalla società (2024): *Strutturazione del modello organizzativo per la prevenzione dei reati.*