UNIVERSITÀ DEGLI STUDI DI SALERNO

Dipartimento di Scienze Aziendali

Management & Innovation Systems

Corso di Dottorato di Ricerca in Big Data Management

XXXIII Ciclo

Tesi di dottorato in

BEYOND THE ARM

L'uso dei sistemi esperti per la revisione contabile e l'individuazione delle frodi aziendali.

Coordinatore del dottorato:

Prof. Valerio Antonelli

Tutor del dottorato:

Prof. Raffaele D'Alessio

Dottoranda:

Dott.ssa Teresa Puca

Anno Accademico 2019/2020

INDICE

PREMESSA

Il presente lavoro ha ad oggetto l'uso dei sistemi esperti e delle nuove tecnologie per la revisione contabile, con particolare riferimento all'individuazione delle frodi aziendali correlate alla falsa informativa finanziaria. I capitoli di cui si compone il testo ripercorrono le fasi di sviluppo del lavoro di ricerca eseguito nel corso degli anni di dottorato, sintetizzando le materie e le tematiche approfondite grazie agli studi svolti nell'ambito delle frodi, delle discipline forensi e delle nuove tecnologie applicate alle attività di *audit*.

Punto di partenza dell'elaborato è costituito dalla disamina delle principali tipologie di frode mediante l'analisi dei più celebri casi di frode che la storia ci tramanda e dei più importanti schemi fraudolenti codificati in ambito internazionale. Il primo capitolo risulta, quindi, interamente dedicato al mondo delle frodi, alle loro caratteristiche e ai principali modelli che spiegano quali siano le condizioni personali e aziendali che spingono un individuo a frodare.

Il secondo capitolo è, invece, dedicato all'esame delle discipline forensi e al ruolo svolto nell'ambito delle frodi dai professionisti che operano in tale campo con particolare attenzione alla materia del *fraud auditing.*

Il *fraud auditing* è finalizzato a individuare la presenza di fenomeni fraudolenti nell'ambito delle organizzazioni economiche mediante un'attività di indagine mirata in grado di rilevare i principali segnali di frode (i c.d. *red flags*) e eseguire le successive attività di verifica delle anomalie riscontrate. Sulla base di quanto descritto, l'attività di ricerca condotta ha avuto tra gli obiettivi quello di analizzare le possibilità di integrare le tecniche di investigazione tipiche del *fraud auditing* nelle procedure impiegate nelle attività di revisione contabile. A tal fine, è stato fondamentale evidenziare i tratti caratteristici e le differenze esistenti tra il *fraud* e il *financial audit* per identificare i possibili punti di contatto tra le due discipline e le principali aree di intervento.

Di fondamentale importanza per lo sviluppo, il potenziamento e il miglioramento dell'efficienza e dell'efficacia delle attività di revisione contabile è l'impiego di sistemi esperti, dell'intelligenza artificiale e di forme di intelligenza aumentata in grado di creare sinergie e interazioni con l'intelligenza umana e il giudizio professionale del revisore.

La "digitalizzazione" delle procedure e delle attività di revisione costituisce un punto di svolta fondamentale per lo svolgimento di questa attività professionale che necessita sempre di più di innalzare il livello qualitativo del servizio offerto e la fiducia risposta dagli utilizzatori di bilancio.

Le attività di ricerca teorica condotte sono state integrate da attività di ricerca applicativa e empirica svolte nel corso della collaborazione avuta con la società RSM Società di Revisione e Organizzazione Contabile S.p.A. che ha dato vita ad un progetto innovativo finalizzato alla realizzazione di un *software* interno e un *software* di revisione rivolto ai professionisti e alle società di revisione di più piccole dimensioni.

Obiettivo del progetto è stato quello di creare un sistema in grado di guidare il professionista nel corso dell'intero processo di revisione, proponendo procedure e attività riprogettate in chiave informatica. La digitalizzazione delle procedure è stata implementata prevedendo la gestione automatizzata dei processi routinari e ripetitivi, l'automatizzazione dei processi più complessi e che richiedono la gestione di una grande quantità di informazioni, l'utilizzo dell'intelligenza artificiale e aumentata per l'esecuzione delle verifiche finalizzate all'individuazione delle frodi.

I risultati dell'attività empirica svolta sono illustrati all'interno del terzo capitolo della tesi che presenta le principali caratteristiche del *software Revisya* realizzato e alcune delle funzioni più innovative in esso contenute, come la funzione dedicata all'esecuzione dei test sul libro giornale e le analisi finalizzate a identificare elementi predittivi e possibili manipolazioni contenute nei dati di bilancio.

I risultati raggiunti mostrano come le attività di revisione traggano importanti benefici dall'utilizzo di strumenti avanzati sia in termini di miglioramento delle attività svolte, di riduzione dei tempi di esecuzione e di efficientamento delle procedure sia in riferimento alle maggiori opportunità di individuazione delle frodi.

CAPITOLO 1 – Le frodi aziendali

1.1 La frode negli studi aziendali: profili storici

1.1.1 Profili storici della frode

La frode rappresenta un fenomeno avente radici millenarie, che si è evoluto con l'uomo e con la nascita e l'espansione delle organizzazioni economiche, tanto che è possibile pensare che le frodi siano direttamente proporzionali allo sviluppo del sistema economico[1].

Le organizzazioni economiche hanno, infatti, dato vita a nuove opportunità di frode. In particolare, la diffusione delle frodi e dei principali scandali finanziari si lega alla nascita delle *corporation* che si formarono nell'Europa del diciassettesimo secolo allo scopo di finanziare l'espansione coloniale europea[2].

«In the world of commerce, organizations incur costs to produce and sell their products or services. These costs run the gamut: labor, taxes, advertising, occupancy, raw materials, research and development, and, yes, fraud and abuse. The latter cost, however, is fundamentally different from the former: the true expense of fraud and abuse is hidden, even if it is reflected in the profit-and-loss figures[3]». Così *Weels*, fondatore dell'*Association of Certified Fraud Examiners* (ACFE), annovera frodi e abusi tra i costi che possono essere sostenuti da tutte le organizzazioni economiche, a prescindere dal settore di riferimento e dalla dimensione aziendale. Si tratta di costi nascosti ma che hanno specifico riflesso economico per le aziende e che possono causare danni di varia natura: l'entità dei danni sarà maggiore in tutte le organizzazioni non dotate degli opportuni strumenti di prevenzione e controllo.

La frode è, quindi, un fenomeno diffusissimo di cui tutte le organizzazioni private e pubbliche devono tener conto nell'ambito della propria gestione e nell'implementazione di procedure adeguate e di un efficace sistema di controllo interno.

A dimostrazione della grande diffusione di questa tipologia di illeciti vi è anche la notevole attenzione dell'opinione pubblica nei confronti delle attività fraudolente, attenzione che è

---

[1] D'ALESSIO R., ANTONELLI V., *Principi di Auditing. Concetti, modelli, metodologie, applicazioni*, Volume I, Edises, 2021, p. 611; *«Nonostante il recente interesse per gli scandali, sollevato dalla crisi finanziaria e dai tragici eventi che stanno colpendo l'economia mondiale, non bisogna pensare alle frodi come un'invenzione dell'uomo contemporaneo».*

[2] D'ALESSIO R., ANTONELLI V., *Principi di Auditing. Concetti, modelli, metodologie, applicazioni*, Volume I, Edises, 2021, p. 611; Cfr. TOMS S., *Financial scandals: a historical overview*, Accounting and Business Research, 49(5), 2019, pp.477-499.

[3] WELLS T. G., *International Fraud Handbook*, Wiley, 2018, p. 3.

sempre di più cresciuta a partire dagli anni Ottanta in poi. In precedenza, l'interesse nei confronti delle frodi era molto ridotto e poca importanza veniva attribuita a questa tipologia di crimini in ragione della mancanza dell'elemento della violenza che li contraddistingue[4]. Gli scandali finanziari che si sono verificati nel corso degli ultimi decenni del Novecento hanno, però, modificato fortemente la percezione della frode poiché hanno reso palese la sua gravità e i danni ad essa correlati che si riversano sul tessuto economico e sociale[5].

Nonostante l'interesse nei confronti del fenomeno oggetto di analisi sia piuttosto recente e vi sia una strettissima correlazione con le organizzazioni economiche, la frode non può essere considerata come una forma di illecito di recente origine, in quanto *«(…) frodi, abusi e comportamenti scorretti hanno da sempre interessato il mondo del commercio fin dagli albori della civiltà o, per meglio esprimersi, fin da quando ha fatto la sua comparsa, nell'agire umano, il fenomeno dello scambio di risorse fra diversi soggetti[6]»*.

A testimonianza di quanto appena detto è emblematica la presenza nel codice di Hammurabi risalente al 1780 a.C. di un paragrafo dedicato proprio a disciplinare specifiche ipotesi di furto di bestiame[7].

Presso la civiltà egizia è, inoltre, possibile collocare la prime attività di *Forensic accounting* della storia svolte dai contabili reali. *«According to some, forensic accounting is one of the oldest professions and dates back to the Egyptians. The ''eyes and ears'' of the king was a person who basically served as a forensic accountant for Pharaoh, watchful over inventories of grain, gold, and other assets. The person had to be trustworthy, responsible, and able to handle a position of influence[8]».* Per evitare che i soggetti addetti alla contabilità e preposti all'inventariazione di beni quali grano e oro, potessero effettuare furti della merce che controllavano, furono istituiti due scrivani indipendenti per ogni operazione da svolgere. Se i totali e i dati riportati dai due contabili coincidevano, erano esclusi furti o irregolarità, in caso di risultati differenti, invece, i due contabili

[4] POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 3.

[5] Cfr. POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 3; *«(…) si sono generati, a livello mondiale, una crescente consapevolezza dell'elevata perniciosità e gravità del fenomeno e, al contempo, un forte giudizio critico nei riguardi delle misure preventive, dissuasive e investigative messe in atto dalle autorità nonché dai governi per contrastare tali azioni illegali, misure giudicate troppo blande, inadeguate quando non tardive e inutili».*

[6] POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 2.

[7] POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 2

[8] SINGLETON T., SINGLETON A., *Fraud Auditing and Forensic Accounting*, Four Edition, John Wiley & Sons, Inc, 2010, p. 3.

sarebbero stati entrambi giustiziati. Tale regola, quindi, generava un doppio controllo esercitato reciprocamente tra i contabili del re che avevano cura di svolgere in maniera attenta e precisa il proprio lavoro e contestualmente controllare e verificare accuratamente il lavoro svolto dall'altro contabile.

La frode, le attività di controllo e di individuazione correlate e le norme previste per prevenire, contrastare e sanzionare le frodi e i loro autori hanno, quindi, origini remote nonostante la loro diffusione e l'importanza attribuita dalla società abbiano assunto una portata rilevante solo nel corso degli ultimi decenni. La maggiore attenzione attribuita al fenomeno e ai suoi effetti è stata favorita dagli importanti scandali finanziari che si sono susseguiti nel corso del tempo e che sono divenuti sempre più frequenti in seguito alla nascita delle aziende e all'evoluzione ed espansione delle attività economiche e del commercio internazionale.

Nei prossimi paragrafi saranno analizzate le frodi più famose della storia degli ultimi secoli che hanno consentito di codificare veri e propri schemi fraudolenti, oggi utilizzati per identificare i possibili scenari di frode e le strategie di occultamento implementate dai frodatori.

1.1.2 La *South Sea Bubble* e le bolle speculative del XVII e XVIII secolo

Con la nascita e la diffusione delle organizzazioni economiche avutasi nel XVII secolo, si sono presentate nuove e numerose opportunità di frode. Nel periodo considerato, i governi nazionali affidavano alle nuove organizzazioni missioni che avevano finalità pubbliche e in cambio tali compagnie venivano riconosciute legalmente e autorizzate a operare, ottenendo, inoltre, la separazione tra la proprietà e la gestione dell'organizzazione, così da garantire anche la posizione degli azionisti, protetti da eventuali perdite grazie alla responsabilità limitata[9].

Tra le prime e più importanti frodi che hanno coinvolto le organizzazioni economiche tra il 1600 e il 1700 rientrano le c.d. "*Tulipmania*", "*Mississippi Bubble*" e "*South Sea Bubble*".

[9] SINGLETON T., SINGLETON A., Fraud Auditing and Forensic Accounting, Four Edition, John Wiley & Sons, Inc, 2010, p. 3; *«The advent of business organizations created new opportunities for fraud. The earliest corporations were formed in seventeenth-century Europe. Nations chartered new corporations and gave them public missions in exchange for a legal right to exist, separation of ownership from management, and limited liability that protected shareholders from losses of the business entity. One such corporation, the Massachusetts Bay Company, was chartered by Charles I in 1628 and had a mission of colonizing the New World».*

La *Tulipmania*

La *Tulipmania* (Bolla dei tulipani) è, in assoluto, la prima bolla economica della storia verificatasi nel 1637 in Olanda e relativa all'uso di strumenti finanziari correlati alla produzione e commercializzazione dei tulipani.

Il tulipano iniziò ad essere coltivato in Olanda alla fine del 1500 ed ebbe velocemente grande successo e diffusione, in particolare tra gli appartenenti alla borghesia dell'epoca, fortemente interessati alle varietà più rare di questo fiore. La coltivazione dei tulipani ebbe, quindi, un forte impulso e la produzione crebbe nel corso dei primi anni del Seicento, così come la sperimentazione di nuove specie. Il tulipano divenne presto un prodotto di lusso con una domanda più alta dell'offerta, ciò anche in considerazione del lungo ciclo di produzione di questo fiore. Tali fattori spinsero al rialzo i prezzi e favorirono la nascita di negoziazioni e veri e propri investimenti caratterizzati da contratti aventi ad oggetto diritti sui bulbi: si trattava di una prima forma di *future*. La negoziazione era caratterizzata dall'acquisto di fiori non ancora prodotti mediante pagamento anticipato di una parte del prezzo e della corresponsione del saldo alla consegna della merce. Gli stessi contratti di compravendita erano a loro volta oggetto di altre negoziazioni e venivano acquistati da altri commercianti creando così delle lunghe catene tra venditori e compratori. Nel corso del 1637 le aste dei tulipani portarono a un aumento incontrollato dei prezzi, ma il mercato crollò in seguito all'asta di Haarlem andata deserta: l'evento provocò un panico tale da far crollare i prezzi dei bulbi in tutta l'Olanda. I sottoscrittori dei contratti in corso furono costretti a pagare l'intera cifra pattuita nonostante il valore di mercato dei tulipani fosse smisuratamente inferiore, ciò fino all'intervento della giustizia olandese che regolamentò il settore rendendo flessibile l'adempimento contrattuale. Dopo tale evento, che ebbe importanti ricadute sui produttori e commercianti dei tulipani, il loro mercato e le relative negoziazioni terminarono.

La bolla del Mississippi

La bolla del Mississippi è legata, invece, al nome dello scozzese John Law e alla sua operazione di ristrutturazione delle finanze francesi grazie al c.d. *Law's systeme*, implementato tra il 1715 e il 1720 e che coinvolgeva le colonie del Nord America tra le quali era presente anche il territorio che costituisce l'attuale Mississippi. Nel 1716 fu fondata la *General Bank* che aveva l'obiettivo di emettere moneta cartacea o banconote garantite dalle riserve di oro e argento della banca. In questo modo Law intendeva aumentare la circolazione del denaro e stimolare la crescita delle attività commerciali, così da risollevare la situazione economica francese che stava attraversando

in quel periodo una importante fase di depressione. L'anno successivo Law fondò la *Compagnie d'Occident* che fu incaricata di controllare e gestire i commerci tra la Francia e il Canada e le colonie americane. A ciò si affiancava un modello di sviluppo dei territori coloniali che prevedeva l'affidamento dello stesso a una compagnia che traeva profitto dalla riscossione delle tasse e la contestuale conversione del debito pubblico in azioni di un monopolio istituito dal governo[10]. In tale contesto, la compagnia del Mississippi si finanziava in base ad uno schema che prevedeva la raccolta di fondi in contanti tramite la vendita di azioni e titoli di stato con un contestuale basso tasso di interesse da corrispondere per le obbligazioni: in questo modo il supporto alle finanze francesi consentiva alla società di ottenere un flusso di cassa più sicuro[11].

La compagnia del Mississippi ebbe una rapida espansione che la portò ad ottenere il commercio del tabacco e ad espandersi notevolmente nell'ambito delle attività commerciali. Law ottenne, inoltre, il controllo delle società che commercializzavano con la Cina e con le Indie Orientali (*Compegnie des Indes*), acquisì il diritto di coniare nuova moneta e di riscuotere la maggior parte delle tasse francesi[12]. Il valore delle azioni della *Mississippi Company* aumentava notevolmente con l'espansione dell'impero economico creato da Law e gli investimenti crescevano fortemente. Il punto di rottura fu determinato dalla vendita di azioni effettuata da alcuni investitori che decisero di convertire le plusvalenze ottenute in oro, ciò determinò l'inizio della riduzione dei prezzi di vendita, il raddoppio dell'offerta di moneta e un forte aumento dell'inflazione. Law fu costretto a svalutare in più fasi il prezzo delle azioni della *Mississippi Company*, ma questo lo portò a perdere il controllo della compagnia che passò ai suoi rivali i quali confiscarono le azioni degli investitori che non erano in grado di dimostrare di aver effettuato il pagamento con beni reali[13]. La bolla della compagnia del Mississippi causò un disastro finanziario che determinò la riduzione di almeno i due terzi delle azioni in circolazione e ingenti perdite per gli investitori e per l'economia francese che tornò a stampare banconote solo dopo ottanta anni da questo evento.

La *South Sea Bubble*

A conclusione di questa breve sintesi delle principali caratteristiche delle prime bolle speculative della nostra storia, non poteva mancare la maggiore e più importante frode del periodo considerato: si tratta della bolla speculativa nota con il nome di *South Sea Bubble* che deriva da

[10] ATACK J., NEAL L., *The Origins and Development of Financial Markets and Institutions*, *The Mississippi Bubble revisited*, Cambridge University Press, 2009, pp. 103-104.
[11] MOEN J., *John Law and the Mississippi Bubble: 1718-1720*, Mississippi Historical Society, 2001.
[12] MOEN J., *John Law and the Mississippi Bubble: 1718-1720*, Mississippi Historical Society, 2001
[13] MOEN J., *John Law and the Mississippi Bubble: 1718-1720*, Mississippi Historical Society, 2001

quello della compagnia mediante la quale la frode è stata perpetrata. La *South Sea Company* venne costituita in Inghilterra nel 1711 al fine di assumersi l'onere del debito pubblico inglese, pari a 10 milioni di sterline, ricevendo in cambio un interesse annuo corrisposto dallo stato e ottenendo privilegi per l'esplorazione e lo sfruttamento del commercio dei mari del sud America e con le colonie spagnole. In particolare, dal 1713, in base a quanto stabilito dal Trattato di Utrecht, la compagnia ottenne la possibilità di effettuare spedizioni annuali per rifornire di schiavi le colonie spagnole. Il primo viaggio finalizzato alla compensazione del debito statale acquisito fu effettuato nel 1717 e comportò l'emissione di azioni in più *tranche*, ognuna delle quali era caratterizzata dall'innalzamento del prezzo*. «The company made its first trading voyage in 1717 and made little actual profit to offset the £10 million of government bonds it had assumed. South Sea then had to borrow £2 million more[14]».*

Nel 1719, la Società rilevò un'altra parte del debito nazionale, il c.d. *"lottery loan"*. Il prestito era fortemente illiquido nonostante fosse corrisposto un alto tasso di interesse e i titoli di stato non erano trasferibili prontamente, inoltre erano presenti elevati sconti sui prezzi. Per tutte queste ragioni i titoli di stato furono scambiati con azioni della compagnia che consentivano agli investitori di ottenere *asset* caratterizzati da un maggior grado di liquidità, allo stato di abbassare il livello degli interessi sul proprio debito e alla compagnia di realizzare profitti da tale operazione[15].

L'anno successivo la compagnia decise di realizzare un'operazione ancora più ambiziosa acquisendo tutto il debito inglese residuo e scambiando il debito con azioni a un prezzo non prestabilito: *This implied that as the stock price appreciated, more debt could be bought for each share[16]*. Dalla conclusione di tale accordo, per il quale la compagnia ottenne voto favorevole da parte del Parlamento solo in seguito ad una forte attività di corruzione, furono emesse periodicamente nuove azioni a prezzi sempre crescenti[17].

---

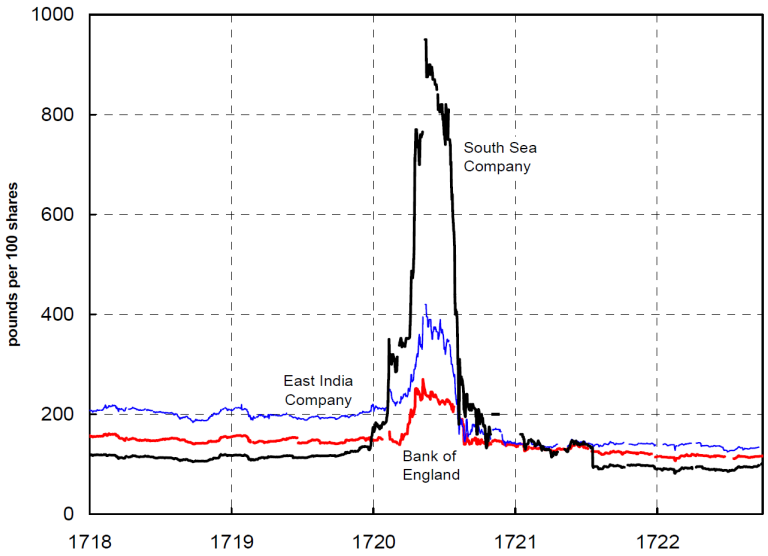
[14] SINGLETON T., SINGLETON A., *Fraud Auditing and Forensic Accounting*, Four Edition, John Wiley & Sons, Inc, 2010, p. 3

[15] GIUSTI G., NOUSSAIR C., VOTH H-J, *Recreating the South Sea Bubble: Lessons from an Experiment in Financial History*, University of Zurich, 2014, p. 6; *«In 1719, the Company took over another part of the national debt, referred to as the "lottery loan". While paying a high rate of interest, the loan was highly illiquid. Bonds could not readily be transferred; price discounts were substantial. The operation that swapped these government bonds for equity in the South Sea Company was widely considered a success the investors gained a more liquid asset, the government lowered the interest charges on its debt, and the company made a profit»*

[16] GIUSTI G., NOUSSAIR C., VOTH H-J, *Recreating the South Sea Bubble: Lessons from an Experiment in Financial History*, University of Zurich, 2014, p. 7.

[17] SINGLETON T., SINGLETON A., *Fraud Auditing and Forensic Accounting*, Four Edition, John Wiley & Sons, Inc, 2010, p. 3; *«In 1719, the company proposed a scheme by which it would take on the entire remaining national debt in Britain, over £30 million, using its own stock at 5 percent in exchange for government bonds*

Figura 1 - Andamento del prezzo delle azioni tra il 1719 e il 1723



Fonte: GIUSTI G., NOUSSAIR C., VOTH H-J, Recreating the South Sea Bubble: Lessons from an Experiment in Financial History, University of Zurich, 2014, p. 5

Il grafico mostra l'andamento del prezzo delle azioni emesse dalla *South Sea Company* tra il 1719 al 1723 effettuando un confronto con l'oscillazione del valore azionario delle altre principali società inglesi del periodo. Tra il 1720 e il 1721 il prezzo ebbe la massima crescita passando dal valore di 120 sterline nel gennaio del 1720, fino a raggiungere le 1000 sterline in agosto. A fronte del forte aumento del prezzo delle azioni era però corrisposto dallo stato un interesse sempre costante e la compagnia non realizzava operazioni commerciali di numero e valore tale da poter sostenere tale crescita dei prezzi. La conseguenza di tale situazione fu la graduale riduzione del rapporto tra utili e prezzo delle azioni: ogni emissione era sempre meno conveniente delle precedenti. La situazione e l'andamento degli utili connessi agli investimenti azionari erano ormai noti tanto che un membro del Parlamento, Archibald Hutcheson, pubblicò molteplici opuscoli nel corso del 1920 che illustravano dettagliatamente quali sarebbero stati i guadagni e le perdite per

lasting until 1727. Although the Bank of England offered also to assume the debt, Parliament approved the assumption of the debt by the South Sea Company. Its stock ros from £128 in January 1720 to £550 by the end of May that year, in a speculation frenzy».

gli investitori in base al periodo di acquisto delle azioni[18]. Il meccanismo di fondo dello schema messo in atto dalla Compagnia dei Mari del Sud si reggeva sulla possibilità di rimborsare gli investitori con i nuovi acquisti di azioni contando sulla continua crescita del prezzo delle azioni. Anche gli investitori speravano di guadagnare sfruttando le prospettive di crescita del prezzo che potevano garantire profitti superiori rispetto ad investimenti alternativi[19].

Nello stesso anno, il prezzo raggiunto dalle azioni e la crescente consapevolezza dello schema attuato dalla compagnia e della graduale riduzione della prospettiva di guadagno, spinsero gli investitori a vendere in modo massiccio i titoli acquistati. In conseguenza alla vendita dei titoli si determinò il crollo del prezzo delle azioni che alla fine dell'anno raggiunse le 100 sterline. La bolla speculativa determinò una grave crisi finanziaria che ridusse in miseria numerosi investitori ed ebbe un effetto così dirompente sull'economia e la politica inglese tale da portare all'emanazione del "*The Bubble Act"*. La risposta dello stato prevedeva, tra l'altro, il divieto di costituire liberamente società per azioni, le quali potevano nascere solo per concessione della Corona o del Parlamento.

Nel dicembre dello stesso anno il Parlamento diede inizio ad un'indagine sulla compagnia spinto dall'indignazione e dalle pressioni degli investitori frodati la maggior parte dei quali faceva parte dell'aristocrazia dell'epoca. Per eseguire tale indagine venne ingaggiato un revisore esterno, Charles Snell, che fu incaricato di controllare e verificare il contenuto dei libri contabili della *South Sea Company*. Si tratta di un evento storicamente molto importante per la professione forense in quanto *«This hiring was the first time in the history of accounting that an outside auditor was brought in to audit books, and marks the beginning of Chartered Accountants in England and thus the beginning of Certified Public Accountants (CPAs) and financial audits as we know them today. Thus CPAs owe their profession, at least to a large extent, to a fraud[20]».* Dalla relazione finale emessa da Snell nel 1921 emerse la fitta rete di corruzione che aveva caratterizzato la gestione

[18] GIUSTI G., NOUSSAIR C., VOTH H-J, *Recreating the South Sea Bubble: Lessons from an Experiment in Financial History*, University of Zurich, 2014, p. 9;

[19] GIUSTI G., NOUSSAIR C., VOTH H-J, *Recreating the South Sea Bubble: Lessons from an Experiment in Financial History*, University of Zurich, 2014, p. 10; *«Our answer is that new subscribers could possibly benefit from rising inherent values of their shares as a result of additional stock issuance in the future – again, if bondholders could be bought out more cheaply, the intrinsic value of shares would increase. Note that for this mechanism to work no actual purchase of bonds is necessary – it is enough that it is planned. New investors are willing to buy because they hope that they will gain if prices continue on an upward trend (which then translates into a self-fulfilling prophecy). The prospect of future issuance can turn the loss in the present into a purchase that, at least in expectation, can turn out to be profitable at some point in the future».*

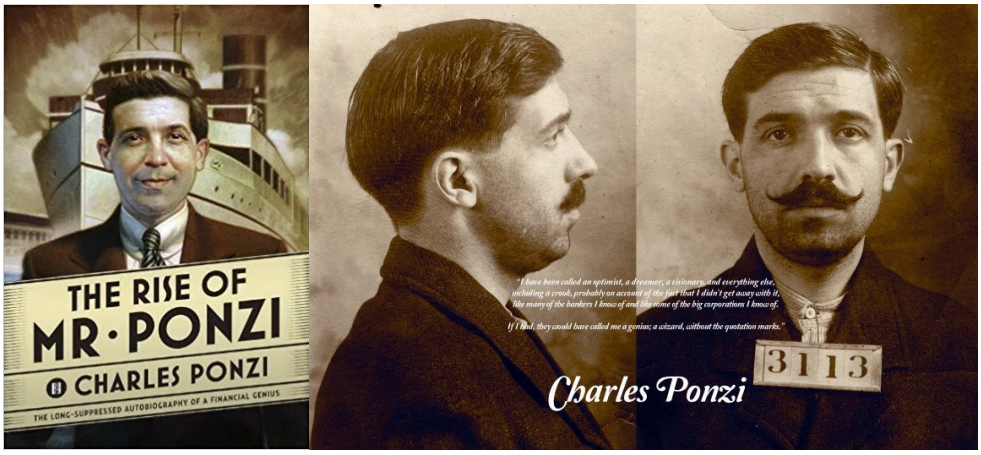
[20] SINGLETON T., SINGLETON A., *Fraud Auditing and Forensic Accounting*, Four Edition, John Wiley & Sons, Inc, 2010, p. 4.

della compagnia e favorito lo schema fraudolento attuato, ma non fu possibile perseguire tutti gli artefici della frode in quanto molti di loro avevano già abbandonato il paese[21].

1.1.3 Charles Ponzi e il suo celebre schema di frode piramidale

La disamina delle principali e più famose frodi della storia non può esimersi dalla trattazione dello schema di frode piramidale attuato all'inizio del '900 dall'italiano Ponzi.

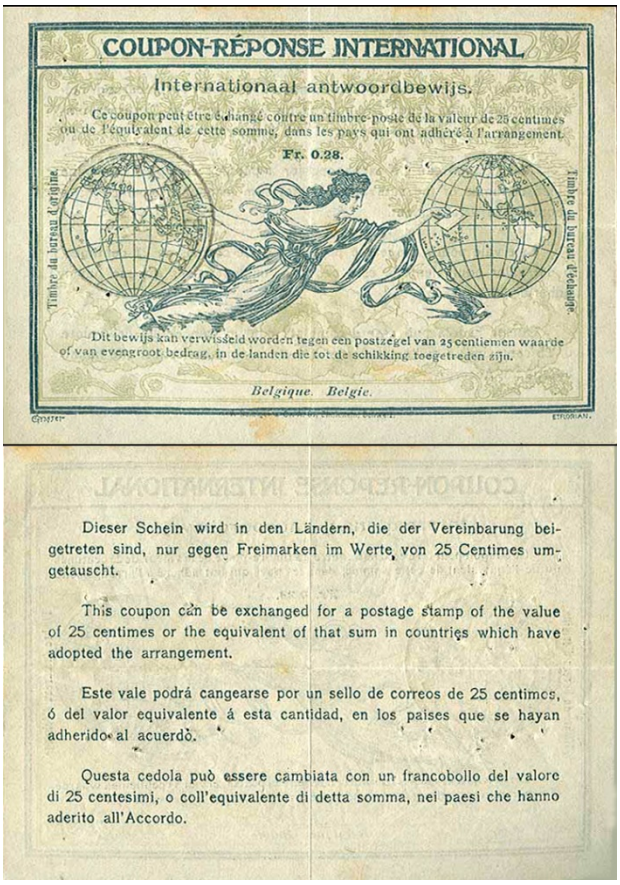
Charles Ponzi è considerato uno dei più grandi truffatori della storia tanto che lo schema piramidale di frode da lui impiegato è noto proprio con il nome di "Schema Ponzi" o "*Ponzi's Scheme*"[22]. Nato a Lugo (RA) il 3 marzo del 1882 e cresciuto a Parma, emigra negli Stati Uniti dopo aver abbandonato gli studi universitari con l'obiettivo di guadagnare e arricchirsi in poco tempo. In seguito a numerosi licenziamenti per truffa e furto e due periodi di reclusione causati da una condanna per la falsificazione di un assegno e da una per immigrazione clandestina si trasferisce nuovamente a Boston nel 1918.



[21] SINGLETON T., SINGLETON A., Fraud Auditing and Forensic Accounting, Four Edition, John Wiley & Sons, Inc, 2010, p. 4; *«In 1721, Snell submitted his report. He uncovered widespread corruption and fraud among the directors in particular and among company officials and their friends at Westminster. Unfortunately, some of the key players had already fled the country with the incriminating records in their possession. Those who remained were examined and some estates were confiscated».*

[22] Cfr. SINGLETON T., SINGLETON A., Fraud Auditing and Forensic Accounting, Four Edition, John Wiley & Sons, Inc, 2010, p. 292; lo schema piramidale attuato da Ponzi non fu il primo nel suo genere, ma la sua operazione fraudolenta fu di una portata tale da renderla tra le più conosciute e famose tanto che da allora si fa sempre riferimento allo schema Ponzi.

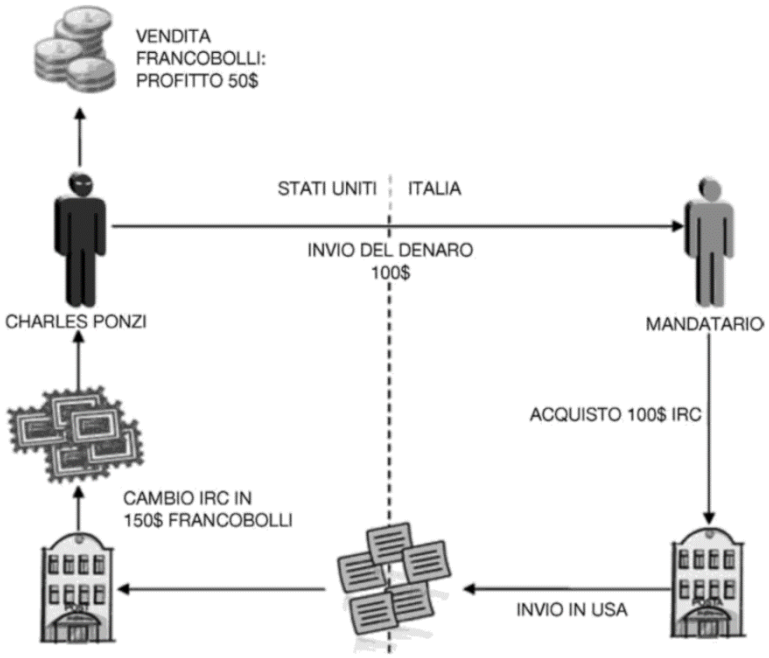
È a Boston che nel 1919 inizia ad attuare la grande truffa dei Buoni di Risposta Internazionali, dopo aver ricevuto uno di questi buoni da una società spagnola[23]. I Buoni di Risposta Internazionali o *International Response Coupon* (IRC) venivano inviati nell'ambito della corrispondenza internazionale per consentire al destinatario di acquistare i francobolli da impiegare nella risposta. L'esigenza nasceva dalle differenze presenti nel livello dei prezzi e nel costo della vita, in particolare tra paesi europei e Stati Uniti e, di conseguenza, nel diverso valore dei francobolli da utilizzare per l'invio della corrispondenza. Il buono inviato da un paese europeo aveva un valore inferiore rispetto ad un buono acquistato negli Stati Uniti, ma il controvalore in francobolli era lo stesso in ogni paese.



[23] POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 257; *«L'anno della svolta è il 1919. Ponzi riceve una lettera da una società spagnola che chiede informazioni circa la guida che Charles aveva pubblicato, la Guida del Commerciante, una sorta di vademecum per promuovere rapporti commerciali, contenente la pubblicità e gli indirizzi di una serie di inserzionisti che veniva spedito su richiesta degli interessati. Dentro la busta inviatagli dalla società spagnola trova un Buono di Risposta Internazionale che Ponzi non aveva mai visto prima. Quello che scopre gli permetterà di arricchirsi velocemente».*

Ponzi decise, quindi, di sfruttare questo meccanismo di utilizzo e conversione degli IRC per trarre profitto dalla vendita dei francobolli acquistati negli Stati Uniti mediante Buoni di Risposta Internazionali italiani secondo lo schema illustrato nella seguente immagine.

Figura 2 - Lo schema attuato da Ponzi



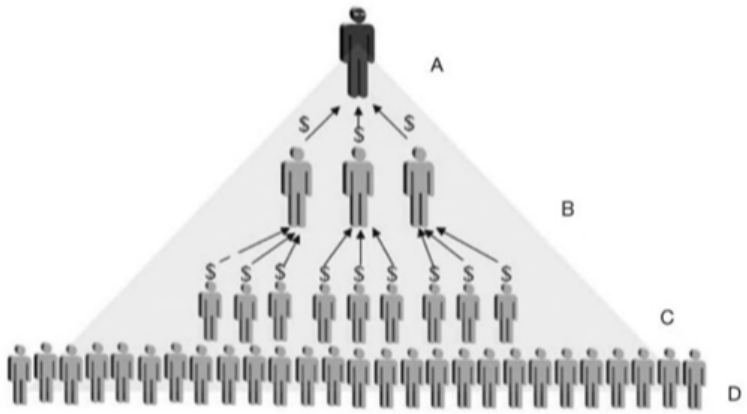
Fonte: POGLIANI G., PECCHIARI N., MARIANI M., Frodi aziendali. Forensic accounting, fraud auditing e litigation, Egea, 2012, p. 258

Lo schema consente di ottenere una sintesi dell'intero business implementato da Ponzi e delle principali fasi e attività di cui esso si componeva. Il modello prevedeva, come prima fase del processo, l'invio di denaro in Italia ad un mandatario che era incaricato di acquistare IRC nel nostro Paese e poi inviare tali buoni negli Stati Uniti. Ciascun buono era acquistato in Italia ad un certo valore e poi scambiato con una quantità di francobolli statunitensi di valore maggiore: a questo punto era sufficiente vendere i francobolli statunitensi per ottenere un profitto dalla differenza di valore rispetto all'IRC acquistato in Italia. In particolare, con un dollaro inviato in Italia era possibile acquistare 66 buoni ognuno dei quali veniva convertito in un francobollo da 5

centesimi, in questo modo con un dollaro era possibile ottenere francobolli per un valore totale di 3,30 dollari[24].

Ponzi implementò lo schema di investimento mediante la *Securities Exchange Company* appositamente fondata e promettendo agli investitori, e inizialmente garantendo, un rendimento del 50% anche in soli 45 giorni[25]. I profitti conferiti ai primi investitori derivavano, però, dai fondi raccolti dai successivi investitori: il meccanismo si basa, infatti, sulla possibilità di allargare gradualmente il numero degli investitori per poter garantire i rendimenti futuri. Lo schema Ponzi rientra tra i c.d. schemi piramidali in cui *«il danaro versato dai nuovi investitori è utilizzato per remunerare chi è al vertice della piramide. L'unica possibilità perché lo schema produca i suoi guadagni si fonda, dunque, sulla speranza che sempre nuovi investitori aderiscano[26]»*.

Figura 3 - Lo schema piramidale



Fonte: POGLIANI G., PECCHIARI N., MARIANI M., Frodi aziendali. Forensic accounting, fraud auditing e litigation, Egea, 2012, p. 252

Come mostrato in figura, lo schema si basa sul coinvolgimento di gruppi di investitori che è possibile collocare su molteplici livelli. Gli investitori di ciascun livello versano il proprio capitale

[24] Cfr. ASSOCIATION OF CERTIFIED FRAUD EXAMINERS, *Fraud Examiners Manual*, 2011, p. 2.403; *«The scheme involved the alleged buying of international postal reply coupons in Europe using foreign currencies, which had depreciated substantially against the dollar in the years after World War I. Ponzi claimed that these coupons, bought at a discount, could then be redeemed at full face value, yielding a substantial profit»*.

[25] GOLDEN T.W., SKALAK S. L., CLAYTON M.M., *A guide to forensic accounting investigation*, John Wiley & Sons, Inc., Hoboken, New Jersey, 2006, p. 69.

[26] POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 251.

ai soggetti posti al livello superiore e ottengono un profitto dal versamento effettuato dagli investitori di livello inferiore: *«il guadagno di ogni "investitore" è rappresentato dal capitale versato dai soggetti da lui reclutati, al netto del versamento che a sua volta, ha dovuto versare per aderire al sistema*[27]*»*. Ovviamente, la probabilità di attrarre un crescente numero di investitori diminuisce nel corso del tempo e di conseguenza la possibilità che gli investitori più recenti riescano ad ottenere il profitto sperato. A ciò si aggiunga che non è possibile parlare di un vero e proprio investimento e, quindi, di un'attività in grado di generare valore aggiunto e profitto, ma di un meccanismo di remunerazione che si basa sulla raccolta di fondi in più *tranche*.

Lo schema Ponzi presenta, però, delle differenze rispetto a un tipico schema piramidale in quanto non si basa sul reclutamento di ulteriori investitori da parte dei nuovi partecipanti, ma tutto il sistema risulta essere gestito da un unico soggetto posto al vertice della piramide (gli schemi possono avere al vertice una persona o anche una società)[28]. Il coinvolgimento di nuovi investitori è inizialmente garantito dalla promessa di alti rendimenti ottenibili mediante innovative strategie di investimento, ma l'afflusso di nuovi investitori rallenta nel corso del tempo o addirittura può fermarsi bruscamente determinando il crollo dell'intero sistema creato.

Anche lo schema implementato da Ponzi nel 1920 giunse al medesimo epilogo con un improvviso crollo della fiducia riposta dagli investitori e il conseguente dissesto del sistema di investimento implementato. Il 26 luglio del 1920, infatti, il *Post*, in seguito ai crescenti dubbi sulla capacità di Ponzi di riuscire ad attrarre e a raccogliere un così elevato ammontare di investimenti, iniziò a pubblicare articoli che mettevano in luce le anomalie e le incertezze correlate all'intero meccanismo. Il giornale si servì, inoltre, della consulenza di Clarence Barron, importante analista finanziario, dalla quale emerse chiaramente che gli alti rendimenti ottenuti da Ponzi non erano in alcun modo correlati a investimenti significativi effettuati e che, in base al business e ai relativi rendimenti, dovevano circolare almeno 160 milioni di IRC mentre ne risultavano in circolazione soltanto un quinto[29].

---

[27] POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 253; *«Due sono i principali argomenti per i quali questo meccanismo di frode è destinato a fallire: 1. il numero di potenziali partecipanti è limitato e, conseguentemente, la piramide non può autoalimentarsi all'infinito; 2. il profitto non si genera mediante un investimento ma con il conferimento di denaro effettuati da un altro partecipante; pertanto il profitto di un soggetto si trasforma nella perdita per un altro soggetto».*

[28] Cfr. GOLDEN T.W., SKALAK S. L., CLAYTON M.M., A guide to forensic accounting investigation, John Wiley & Sons, Inc., Hoboken, New Jersey, 2006, pp. 69 e ss; SINGLETON T., SINGLETON A., BOLOGNA J., LINDQUIST R., *Fraud Auditing and Forensic Accounting*, Third Edition, John Wiley & Sons, Inc, 2006, p. 38.

[29] POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 259; la quantità di buoni in circolazione era molto inferiore a quella avrebbe dovuto essere presente in base al business implementato, inoltre non si registravano importanti acquisti di buoni.

«There were two main problems. First, although Ponzi claimed to be trading over $10 million worth of postal reply coupons, only a few hundred thousand dollars worth actually existed. A more fatal flaw was the fact that the scheme relied on new investor funds to pay returns to earlier investors[30]».

Gli articoli pubblicati sul *Post* crearono una vera e propria ondata di panico tra tutti gli investitori che iniziarono a richiedere rimborsi per un ammontare superiore alle entrate ottenute, ciò determinò l'insolvenza di Ponzi, la bancarotta e il successivo arresto il 13 agosto con 86 frodi tra i capi di accusa.

In base all'analisi di uno schema di frode piramidale come quello attuato da Ponzi con il business degli IRC è possibile individuare quali sono i *red flags* che caratterizzano questa tipologia di schema. I *red flags* sono tipicamente riassumibili nei seguenti punti[31]:

- *too good to be true*;
- un improvviso successo;
- scarsa trasparenza informativa;
- strategie di investimento troppo complesse;
- insistenza a reinvestire.

Con l'espressione "*too good to be true*" si intende fare riferimento a tutti quegli investimenti che promettono l'ottenimento di rendimenti di molto superiori ai normali rendimenti ottenibili con investimenti alternativi similari. Normalmente, il promotore di tali investimenti presenta l'operazione come una vera e propria opportunità da cogliere tempestivamente, in questo modo si tenta di impedire al cliente di effettuare ulteriori analisi o acquisire approfondite informazioni sul business in oggetto. Queste peculiarità sono tra le più rappresentative della possibile esistenza di uno schema Ponzi e devono essere accuratamente valutate e considerate prima di intraprendere una simile operazione di investimento.

Altri elementi di anomalia che possono essere sintomatici della presenza di uno schema piramidale sono rappresentati dal forte e improvviso successo del business, quindi dalla veloce crescita del numero dei partecipanti all'investimento, e la scarsa trasparenza informativa relativa ai dati di *performance*, ai bilanci e a tutta la documentazione che dovrebbe essere obbligatoriamente messa a disposizione degli investitori. A ciò si aggiunga l'eventuale alta

[30] ASSOCIATION OF CERTIFIED FRAUD EXAMINERS, *Fraud Examiners Manual*, 2011, p. 2.403.

[31] L'elencazione e la descrizione dei *red flags* è tratta da POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 265.

complessità delle strategie di investimento implementate, complessità tale da non rendere chiaro il business ai comuni investitori. Seppur articolare, le strategie di business devono essere sempre comprensibili e chiare per gli investitori e non lasciare dubbi o incertezze in merito ai numerosi aspetti che contraddistinguono una determinata operazione: *«Strategie di investimento altamente complesse e difficili da spiegare ai comuni investitori possono in realtà nascondere la realtà degli investimenti effettuati*[32]*».*

Infine, la forte insistenza a reinvestire in seguito all'ottenimento di elevati profitti rappresenta un ulteriore *red flag* tipico di uno schema piramidale in quanto solo mediante il reinvestimento e, quindi, il nuovo apporto di fondi è possibile che il sistema continui ad alimentarsi nel corso del tempo.

1.1.4 Il caso Madoff

Tra i casi più importanti di frode implementata sulla base dello schema Ponzi rientra la truffa da 65 miliardi organizzata da uno dei finanzieri più importanti degli Stati Uniti, Bernard Madoff.

Madoff è nato il 29 aprile 1938 a New York e cresciuto nella stessa città in una modesta famiglia di origini ebraiche. I suoi genitori erano figli di immigrati, polacchi da parte del padre e rumeni e austriaci da parte della madre. Madoff e la sua famiglia hanno vissuto nell'epoca della *Grande Depressione* e della crisi economica dei primi decenni del '900, attraversando momenti molto difficili dovuti alle ristrettezze economiche in cui versavano[33].

L'ingresso nell'alta finanza della famiglia Madoff avvenne negli anni '50 mediante l'attività di intermediario finanziario che la madre di Madoff svolgeva tramite la società da lei fondata, la *Gibraltar Securities*. In particolare, la madre svolgeva attività di *dealer*, quindi investiva in titoli acquistati da istituti di credito, poi rivenduti a prezzi maggiorati ad investitori privati. Questo tipo di attività portò la famiglia ad esporsi finanziariamente in modo importante, a tal punto che l'ente governativo preposto impose la chiusura della società a causa della precaria situazione finanziaria. Nonostante tali difficoltà, la famiglia riuscì a garantire a Madoff un elevato livello di istruzione, egli, infatti si diplomò alla *Far Rockaway High School* nel 1956 e nel 1960 superò l'esame per conseguire la licenza di operatore finanziario nella compravendita dei titoli e conseguì

[32] POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 265.

[33] Cfr. PASQUINI M., *Bernie Madoff. Il grande illusionista di Wall Street*, Area51 Publishing s.r.l., San Lazzaro di Savena (Bologna), 2018, p. 5 e ss.

la laurea in scienze politiche presso la *Hofstra University*[34]. Da questo momento, Madoff iniziò ad avviare la propria attività di investitore e a interessarsi attivamente al mondo della finanza di cui anche la moglie Ruth faceva parte lavorando nel mercato azionario. Nello stesso anno fondò la *Bernard L. Madoff Investment Securities* (BMIS), grazie alla quale riuscì a intraprendere la propria ascesa professionale operando nel business del brokeraggio su mercati regolamentati e OTC e iniziando ad acquisire come clienti società di dimensioni sempre maggiori grazie alla garanzia di rendimenti costanti pari al 10% degli investimenti effettuati.

La società iniziò a crescere e la reputazione di Madoff a raggiungere elevati livelli correlati alle performance realizzate, all'assenza di perdite subite e alla notevole fiducia accordata dagli appartenenti alla comunità ebraica. In questo modo Madoff riuscì ad acquisire clienti sempre più importanti e i milionari più famosi dell'epoca, non solo americani, ma anche europei, acquisendo, tra l'altro, importanti fondi speculativi come l'*RMF Division* di *Man Group* e *Tremont*[35].

Il volume d'affari di Madoff divenne talmente rilevante che la sua azienda fu scelta per entrare a far parte del gruppo designato a sviluppare il NASDAQ, di cui Madoff fu presidente dal 1990 al 1993.

La frode fu attuata da Madoff nell'ambito della parallela attività di *advisory* implementata e in cui operavano esclusivamente persone di fiducia e, in particolare, i membri della propria famiglia.

Il grande successo di Madoff svolse un ruolo importante per accrescere la fiducia e la credibilità riposta dagli investitori, i quali erano rassicurati dal tipo di rendimento garantito, contenuto ma stabile nel tempo. Il senso si sicurezza era rafforzato, inoltre, dalla possibilità di prelevare il denaro in ogni momento al pari di qualsiasi deposito bancario ma con il vantaggio di ottenere un tasso di interesse maggiore.

Considerando i *red flags* tipici di uno schema piramidale descritti al paragrafo 1.1.3, Madoff era in grado, in base al proprio sistema di aggirare il c.d. *too good to be true* proprio in ragione del minor tasso di rendimento assicurato agli investitori, allineato ad altri investimenti comparabili. Inoltre, come descritto in precedenza, era assente l'elemento dell'*insistenza a reinvestire* in

[34] PASQUINI M., *Bernie Madoff. Il grande illusionista di Wall Street*, Area51 Publishing s.r.l., San Lazzaro di Savena (Bologna), 2018, p. 5 e ss

[35] Madoff era riuscito a presentare il suo business come esclusivo e appannaggio dei soli "fortunati" appartenenti a una ristretta cerchia di privilegiati e amici. Cfr. PETRAS J., *Bernard Madoff: Wall Street Swindler Strikes Powerful Blows for Social Justice*, 20 dicembre 2008; *«Many of the swindled super-rich clients forced their money on Madoff, who sternly imposed rigorous conditions on potential clients: He insisted they have recommendations from existing investors, deposit a substantial amount and guarantee their own solvency. Most considered themselves lucky to have their funds taken by the highly respected Wall Street…swindler. Madoff's standard message was that the fund was closed…but because they came from the same world (board members of Jewish charities, pro-Israel fund raising organizations or the 'right' country clubs) or were related to a friend, colleague or existing clients, he would take their money»*.

quanto il business era presentato come esclusivo e appannaggio di una ristretta cerchia di privilegiati. Infine, era assente l'elemento della *scarsa trasparenza informativa* in quanto la società inviava periodicamente agli investitori una documentazione dettagliata e particolareggiata che apparentemente non destava alcun sospetto sulla presenza di operazioni e transazioni false.

L'apparente solida costruzione dello schema implementato da Madoff aveva, però, un punto di debolezza rappresentato dal fatto che negli anni i rendimenti non avevano mai avuto alcuna flessione, permanendo sempre al di sopra del 10%. Fu su tale aspetto che iniziarono a concentrarsi i dubbi dell'analista finanziario Harry Markopolos, che in seguito a uno studio della strategia *split strike conversion* di Madoff, giunse a conclusione che doveva necessariamente trattarsi di una frode. Nel 1999 presentò, quindi, alla SEC un primo rapporto che evidenziava tutti gli elementi di anomalia riscontrati. I sospetti di Markopolos non furono approfonditi dalla SEC se non nel 2006, in seguito alla presentazione di un secondo dettagliato rapporto[36] , ma dall'indagine che ne seguì la SEC non riuscì a trovare alcuna prova che indicasse la presenza di una frode.

Solo nel 2008 il sistema creato da Madoff iniziò a sgretolarsi a causa delle difficoltà connesse alla crisi economica e alle richieste di disinvestimento da parte degli investitori che continuavano a crescere, fino al punto di rottura che si ebbe quando i fondi non furono più sufficienti a gestire i rimborsi e venne alla luce l'intera truffa[37].

Madoff venne arrestato l'11 dicembre del 2008 e condannato a 150 anni di carcere per undici differenti reati finanziari. La truffa Madoff è costata una perdita di circa 18 miliardi di fondi raccolti per una frode del valore totale di 65 miliardi che ha provocato danni enormi all'economica degli Stati Uniti colpendo anche importanti investitori istituzionali di altri Paesi oltre che numerosissimi investitori privati di ogni estrazione e ceto sociale.

[36] Il rapporto denominato *The World's Largest Hedge Fund is a Fraud* poneva l'attenzione sull'anomala stabilità dei rendimenti che non poteva essere sostenuta finanziariamente a meno che non celasse una frode piramidale basata su uno schema Ponzi.

[37] ASSOCIATION OF CERTIFIED FRAUD EXAMINERS, *Fraud Examiners Manual*, 2011, p. 2.404; *«Unfortunately for Madoff, his scheme began to unravel in December 2008, when the financial crisis caused an increasing demand of cash withdrawals from his clients. The increase in redemptions caused his scheme to collapse when there were not enough funds from new investments to pay them off, and so, like all Ponzi schemes, it collapsed».*

1.2 La lezione della storia

1.2.1 La frode e i *white collar crime*

Il termine frode sottende una vasta categoria di condotte illecite correlate alle attività economiche e al mondo imprenditoriale. Al pari di ogni altro fenomeno criminoso, la frode ha origini remote ma si è diffusa notevolmente a partire dalla nascita delle organizzazioni economiche e continua ad evolversi e a mutare tanto che non è possibile avere una definizione universale in grado di ricomprendere tutte le possibili fattispecie che ne fanno parte. In particolare, importanti cambiamenti si sono avuti con l'avvento delle nuove tecnologie e della diffusione dell'*Information Technology*, dell'Intelligenza Artificiale in ambito aziendale e, in generale, della crescente informatizzazione e automatizzazione dei processi produttivi. In ragione di tali cambiamenti, gli schemi e le tecniche fraudolente si rinnovano ed evolvono tanto da poter essere considerati un fenomeno in continua evoluzione.

Tra le numerose definizioni di frode, una delle più diffuse è quella di frode quale crimine. In base a tale definizione è possibile affermare che *«Fraud is a generic term, and embraces all the multifarious means which human ingenuity can devise, which are resorted to by one individual, to get an advantage over another by false representations. No definite and invariable rule can be laid down as a general proposition in defining fraud, as it includes surprise, trick, cunning and unfair ways by which another is cheated. The only boundaries defining it are those which limit human knavery»*[38]. La definizione appena citata mette in luce la grande varietà che presentano le fattispecie fraudolente, da considerare come un vasto sottoinsieme di condotte criminose.

Aspetto comune a tutte le condotte fraudolente è, sicuramente, l'utilizzo di molteplici mezzi finalizzati a conseguire mediante l'inganno un vantaggio ingiusto.

Il processo che porta alla realizzazione di una frode può essere concepito in modo lineare e sviluppato su tre elementi fondamentali:

- il soggetto che pone in essere la frode;
- l'inganno;
- la vittima che subisce il danno.

Sulla base di tali elementi, il processo di realizzazione della frode presuppone che *«l'attore (soggetto attivo), attraverso artifici e raggiri induce in errore la vittima (soggetto passivo) e*

[38] SINGLETON T., SINGLETON A., BOLOGNA J., LINDQUIST R., *Fraud Auditing and Forensic Accounting*, Third Edition, John Wiley & Sons, Inc, 2006, p. 2; Michigan Criminal Law, Chapter 86, Sec. 1529.

procura a sé stesso o ad altri un vantaggio ingiusto unito ad un ingiusto danno per la vittima o per altri"[39].

L'ISA Italia 240 definisce la frode come un *«atto intenzionalmente perpetrato con l'inganno da parte di uno o più componenti dell'organo di governo aziendale, del personale dipendente o di terzi, allo scopo di conseguire vantaggi ingiusti o illeciti».* In base al principio di revisione citato, quindi, la frode presuppone la presenza dell'inganno, perpetrato intenzionalmente da chi la commette e il raggiungimento di vantaggi ingiusti o illeciti ottenuti, tipicamente, mediante appropriazione di ricchezza di proprietà di terzi[40].

La definizione tradizionale così individuata deve essere, però, ampliata per tener conto di tutte le fattispecie che, pur non presentando l'elemento dell'inganno e dell'appropriazione di ricchezza rientrano ugualmente nella categoria delle frodi: si pensi a tutte le ipotesi in cui lo scopo della frode è quello di conseguire un vantaggio competitivo anziché un aumento della ricchezza posseduta[41].

Per comprendere più nel dettaglio il fenomeno fraudolento è opportuno collocare la frode nel contesto più ampio della criminalità economica in cui rientrano tutte le condotte illecite che abbiano contenuto economico e, quindi, siano correlate ad attività economico-imprenditoriali.

Il termine maggiormente utilizzato per identificare il fenomeno della criminalità economica è sicuramente quello di *"White collar crime".* L'espressione è stata introdotta nel 1938 dal criminologo Edwin H. Sutherland in occasione della presentazione da lui tenuta al convegno dell'*American Sociological Society*. L'espressione consente di distinguere nettamente la criminalità economica dalla criminalità violenta, ponendo l'accento su una delle caratteristiche tipiche del soggetto che commette una frode: essere apparentemente insospettabile. A differenza di ciò che avviene per i reati violenti, infatti, la frode è celata dallo svolgimento di attività e operazioni lecite e messa in atto da soggetti rispettabili nell'ambito dello svolgimento della propria attività lavorativa: *«unlike other offences, part of the method of fraud is to conceal*

---

[39] ALLEGRINI M., D'ONZA G., MANCINI D., GARZELLA S., *Le frodi aziendali. Frodi amministrative, alterazioni di bilancio e computer crime*, Franco Angeli, Milano, 2003, p. 15.

[40] POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 4. Gli autori sottolineano che l'inganno è perpetrato allo scopo di *«conseguire un vantaggio nei riguardi di un terzo»* e che il termine frode si riferisce a *«qualunque tipo di inganno – comprensivo di fattispecie che vanno dalla manipolazione della verità alla soppressione e occultamento di qualsiasi fatto e informazione – in conseguenza del quale una parte è indotta a separarsi da elementi di sua proprietà per meno del loro valore effettivo o a riconoscere un corrispettivo maggiore del giusto per averi di proprietà altrui».*

[41] POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 4 e ss.

its existence. A bank robber uses threats or force, while a bank embezzler not only steals money, but also covers up the theft»[42].

Per le ragioni descritte e a causa della mancanza dell'elemento della violenza e dell'uso della forza, fino a pochi decenni fa non veniva data la giusta attenzione a questo tipo di reati che, di conseguenza, non venivano percepiti come dannosi al pari dei reati violenti[43].

1.2.2 Il triangolo delle frodi e le sue varianti

Riprendendo quanto stabilito dall'ISA Italia 240 e dal contenuto delle principali definizioni della fattispecie, la frode rappresenta un atto intenzionale che ha la finalità di conseguire un vantaggio ingiusto o illecito. Si tratta di atti perpetrati da soggetti che potremmo definire "di fiducia" che, in particolari circostanze e in presenza di specifiche condizioni, diventano "trasgressori di fiducia"[44]. Le motivazioni che spingono una persona apparentemente insospettabile e, molto spesso, di elevato status sociale a commettere una frode sono state oggetto di importanti studi. A Donald Cressey, allievo del professore e criminologo Edwin Sutherland che ha elaborato e introdotto la definizione dei *white collar crime*, si deve uno dei modelli teorici più importanti nell'identificazione di tali motivazioni: il Triangolo delle Frodi. Tale modello è stato concepito da Cressey a seguito di numerosi studi empirici condotti nel corso dell'elaborazione della propria tesi di laurea, studi che hanno avuto ad oggetto i risultati di più di 200 interviste effettuate direttamente dallo studioso a detenuti incriminati per reati di appropriazione indebita. Sulla base di queste ricerche, Cressey riuscì ad individuare le tre motivazioni che spingono un individuo a perpetrare una frode:

- Pressione.
- Opportunità.
- Giustificazione.

[42]ASSOCIATION OF CERTIFIED FRAUD EXAMINERS, *Fraud Examiners Manual (International)*, 2011, p. I-3.

[43] SINGLETON T., SINGLETON A., BOLOGNA J., LINDQUIST R., Fraud Auditing and Forensic Accounting, Third Edition, John Wiley & Sons, Inc, 2006, p. 1: *«One person can injure another either by force or through fraud. The use of force to cause bodily injury is frowned on by most organized societies; using fraud to cause financial injury to another does not carry the same degree of stigma».*

[44] D'ALESSIO R., ANTONELLI V., BOZZA E., *Principi di Auditing. Concetti, modelli, metodologie, applicazioni*, Volume I, Edises, 2017, p. 268.

Figura 4 - Il Triangolo delle Frodi

Fonte: D'ALESSIO R., ANTONELLI V., BOZZA E., Principi di Auditing.
Concetti, modelli, metodologie, applicazioni, Volume I, Edises, 2017, p. 268

Affinché un soggetto sia spinto a commettere un atto fraudolento è, quindi, fondamentale che egli senta la necessità di soddisfare dei bisogni che costituiscono per lui una "pressione". Generalmente la pressione è correlata ad esigenze finanziarie ed economiche, ma è possibile che sia generata anche da altre motivazioni non finanziarie come la necessità di migliorare il livello delle performance conseguite, uno stato di frustrazione lavorativa o ancora per la voglia di "sfidare" il sistema[45]. Le motivazioni che possono spingere un individuo a commettere una frode possono essere, quindi, anche molteplici e diversificarsi in base alla personalità e alle caratteristiche soggettive di chi le commette.

Oltre a tali bisogni pressanti, è necessario che il frodatore individui reali opportunità di poter commettere una frode e di farlo in modo occulto mediante strumenti e azioni apparentemente lecite. Le opportunità variano in base al tipo di frode da commettere: se diventa più difficile attuare una frode, il numero di potenziali frodatori si ridurrà[46].

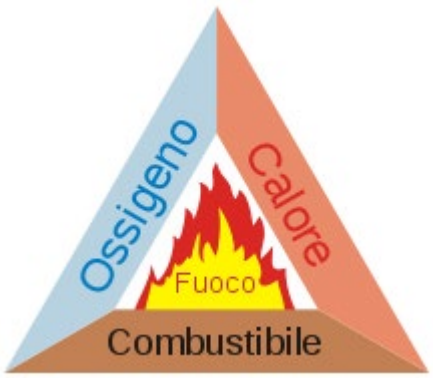
[45] ALBRECHT W.S., ALBRECHT C.O., ALBRECHT C.C., ZIMBELMAN M.F., *Fraud Examination*, Fourth edition, South-Western Cengage Learning, 2011, p. 34; «*Most pressures involve a financial need, although nonfinancial pressures, such as the need to report financial results better than actual performance, frustration with work, or even a challenge to beat the system, can also motivate fraud».*

[46] SCHUCHTER A., LEVI M., *The Fraud Triangle revisited*, Macmillan Publishers Ltd, 0955–1662 Security Journal, 2013; *«(…) a potential fraudster reacts to an opportunity structure; if a particular type of fraud is made harder to commit, the number of offences (and in the long run, attempts) will reduce*»

Infine, chi froda ha necessità di percepire e considerare il proprio comportamento come un atto non criminoso[47]. L'elemento della "giustificazione" deriva da un processo di razionalizzazione che consente di individuare le giuste motivazioni che permettono al frodatore di considerare l'azione fraudolenta come accettabile[48].

I tre elementi sono sempre presenti e costituiscono un tratto comune a tutte le frodi che possono essere paragonate a un incendio che può avere origine solo in presenza di ossigeno, combustibile e calore. È da tale similitudine che è possibile paragonare il triangolo delle frodi al c.d. Triangolo del Fuoco: solo in presenza di tutti gli elementi sopra elencati è possibile avere un incendio[49].

Figura 5 - Triangolo del Fuoco



Fonte: D'ALESSIO R., ANTONELLI V., BOZZA E., Principi di Auditing. Concetti, modelli, metodologie, applicazioni, Volume I, Edises, 2017, p. 269

Come per un incendio, anche gli elementi che caratterizzano una frode sono interattivi e si compensano tra loro. Ad esempio, in presenza di una più forte pressione sarà minore il livello di

[47] D'ALESSIO R., ANTONELLI V., BOZZA E., *Principi di Auditing. Concetti, modelli, metodologie, applicazioni*, Volume I, Edises, 2017, p. 268.

[48] ALBRECHT W.S., ALBRECHT C.O., ALBRECHT C.C., ZIMBELMAN M.F. *Fraud Examination*, Fourth edition, South-Western Cengage Learning, 2011, p. 34; « Fraud perpetrators need a way to rationalize their actions as acceptable».

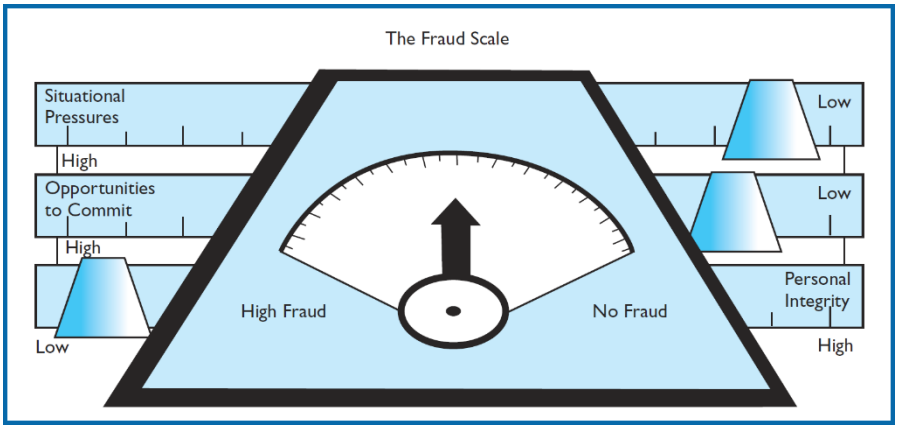
[49] D'ALESSIO R., ANTONELLI V., BOZZA E., *Principi di Auditing. Concetti, modelli, metodologie, applicazioni*, Volume I, Edises, 2017, p. 269: «*I vigili del fuoco sanno che un fuoco può essere estinto eliminando uno dei tre elementi. L'estinzione dell'incendio, infatti, si ottiene per raffreddamento, sottrazione del combustibile e soffocamento. L'ossigeno è spesso eliminato utilizzando sostanze chimiche. Il calore è eliminato versando l'acqua sugli incendi. Il combustibile viene rimosso costruendo linee tagliafuoco o eli-minando la fonte del combustibile.Come per gli elementi del triangolo del fuoco, i tre elementi nel triangolo di frode sono interattivi. Più il combustibile è infiammabile, meno ossigeno e calore ci vuole per accendere un fuoco. Allo stesso modo, più puro è l'ossigeno, meno infiammabile deve essere il combustibile per accenderlo»*

giustificazione necessario a spingere e motivare il frodatore all'azione e, allo stesso tempo, se il frodatore è più disonesto saranno necessarie minori opportunità e pressioni[50].

I tre elementi introdotti con il Triangolo delle Frodi rappresentano il punto di riferimento anche di altri modelli utilizzati per spiegare le motivazioni che spingono a commettere una frode. Di particolare rilevanza, in tal senso, è il modello *The Fraud Scale* di Albrecht. Tale modello può essere considerato come alternativo al Triangolo delle Frodi e rappresentativo delle relazioni e interazioni esistenti tra i tre elementi che costituiscono una frode. Prima di approfondire le caratteristiche del modello, è fondamentale evidenziare come gli autori abbiamo effettuato un'importante modifica data dalla sostituzione dell'elemento della "Giustificazione" con quello dell'"Integrità personale" del soggetto che commette tali illeciti. Osservando il modello è evidente come un minor livello di integrità personale renda più semplice razionalizzare il comportamento fraudolento e richieda un minor livello di opportunità o pressioni percepite, al contrario, in presenza di una maggiore integrità personale il frodatore avrà necessità di percepire maggiormente le pressioni o individuare una opportunità maggiore di commettere l'illecito. L'elemento dell'integrità personale è quindi posto in una relazione di proporzionalità inversa rispetto agli altri due elementi: considerando le stesse opportunità di commettere una frode e livelli di pressione similari, due individui saranno più o meno spinti a commettere l'illecito proprio in base ai principi etici personalmente adottati.

[50] ALBRECHT W.S., ALBRECHT C.O., ALBRECHT C.C., ZIMBELMAN M.F., *Fraud Examination*, Fourth edition, South-Western Cengage Learning, 2011, p. 35; «With fraud, the greater the perceived opportunity or the more intense the pressure, the less rationalization ittakes to motivate someone to commit fraud. Likewise, the more dishonest a perpetrator is, the less opportunity and/or pressure it takes to motivate fraud».

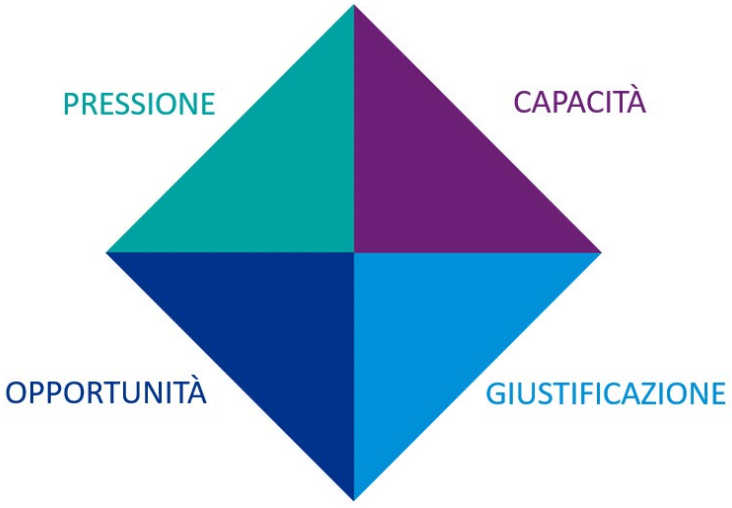
Figura 6 - The Fraud Scale



Fonte: ALBRECHT W.S., ALBRECHT C.O., ALBRECHT C.C., ZIMBELMAN M.F. Fraud Examination, Fourth edition, South-Western Cengage Learning, 2011, p. 35

I modelli appena analizzati trovano la propria naturale evoluzione nel c.d. *Diamante della frode* elaborato da Wolfe e Hermanson e risalente al 2004. Gli autori hanno aggiunto un ulteriore elemento indispensabile per poter commettere una frode: la capacità del soggetto che la compie. Anche tale modello nasce da importanti studi empirici e dalla constatazione che, in tutte le frodi analizzate, un fattore fondamentale era costituito dalle capacità del frodatore di commettere l'azione.

Figura 7 - Il Diamante della frode



Fonte: D'ALESSIO R., ANTONELLI V., BOZZA E., Principi di Auditing. Concetti, modelli, metodologie, applicazioni, Volume I, Edises, 2017, p. 271

In base agli studi effettuati dai due autori, la persona in grado di commettere una frode è tipicamente posta in posizione autorevole all'interno dell'organizzazione economica o preposta allo svolgimento di funzioni caratterizzate da un certo livello di prestigio. La capacità di commettere una frode è, inoltre, correlata alla conoscenza dei sistemi informativi aziendali e del sistema di controllo interno così da conoscere tutti i possibili punti di debolezza e, di conseguenza, le migliori opportunità per intraprendere l'azione. Oltre a tali aspetti correlati alle *skills* professionali e alla posizione lavorativa ricoperta, gli autori puntano l'attenzione su aspetti soggettivi e connessi alla personalità dell'individuo. Si tratta, innanzitutto, del forte *ego* che il frodatore deve possedere e della fiducia nell'azione che dovrà intraprendere e, in secondo luogo, della capacità di affrontare lo stress correlato al compimento della frode e delle attività finalizzate al suo occultamento[51].

A conclusione dell'analisi dei modelli rappresentativi delle modalità e motivazioni che spingono un soggetto a commettere una frode, non può mancare il più recente modello MICE proposto da Kranahcer nel 2010. MICE è acronimo di *Money, Ideology, Coercion, Ego* e si focalizza sulle motivazioni che spingono un soggetto a frodare, costituite, appunto, da[52]:

- Denaro: prima leva che spinge a frodare è la necessità di ottenere denaro per appagare i più svariati bisogni.
- Ideologia: predisposizione personale o familiare che porta l'individuo a ritenere che frodare sia giusto.
- Coercizione: in alcuni casi l'individuo non agisce su proprio impulso personale ma è costretto a frodare da altri.
- Ego: motivo che spinge a frodare per ottenere maggiore successo o potere o per non perdere quanto già in possesso del frodatore.

[51] Cfr. D'ALESSIO R., ANTONELLI V., BOZZA E., *Principi di Auditing. Concetti, modelli, metodologie, applicazioni*, Volume I, Edises, 2017, p. 271.

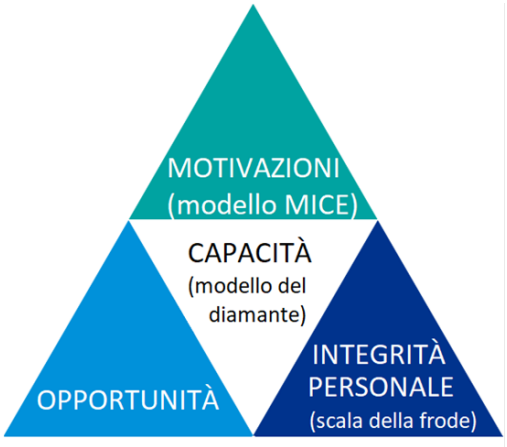
[52] Cfr. D'ALESSIO R., ANTONELLI V., BOZZA E., *Principi di Auditing. Concetti, modelli, metodologie, applicazioni*, Volume I, Edises, 2017, p. 271; «*Le credenza familiare o ideologia spinge un soggetto a ritenere che sia giusto frodare, mentre la coercizione si verifica quando gli individui vengono costretti a frodare. L'ego può essere un al-tro motivo per la frode poiché le persone non ammettono di aver fallito e di perdere la loro re-putazione o la posizione di potere di fronte alla famiglia o alla collettività. La sete di denaro, poi, per i più svariati scopi è la molla, più pericolosa, per spingere un individuo alla frode*»

Figura 8 - Il modello MICE

Fonte: D'ALESSIO R., ANTONELLI V., BOZZA E., Principi di Auditing.
Concetti, modelli, metodologie, applicazioni, Volume I, Edises, 2017, p. 272

Tutti i modelli appena analizzati e descritti sono stati condensanti nel 2012 in nuovo modello proposto da Kassem e Higson. «(…) *Kassem e Higson hanno pensato di condensare le ricerche precedenti in un unico modello "il nuovo triangolo delle frodi" ritenendo che solo una valutazione sistemica di motivazioni, opportunità, integrità e capacità del truffatore possono aiutare nella prevenzione delle frodi*[53]».

Figura 9 - Il nuovo triangolo delle frodi



Fonte: D'ALESSIO R., ANTONELLI V., BOZZA E., Principi di Auditing.
Concetti, modelli, metodologie, applicazioni, Volume I, Edises, 2017, p. 272

[53] D'ALESSIO R., ANTONELLI V., BOZZA E., *Principi di Auditing. Concetti, modelli, metodologie, applicazioni*, Volume I, Edises, 2017, p. 272.

L'ISA Italia 240, nella sezione "Linee guida ed altro materiale esplicativo" stabilisce che «*La frode, sia nel caso di falsa informativa finanziaria sia di appropriazione illecita di beni ed attività dell'impresa, implica l'esistenza di incentivi o pressioni a commetterla, la percezione di un'occasione per perpetrarla e la possibilità di giustificare l'atto*». In base a tale definizione anche il principio di revisione riprende gli elementi che caratterizzano il Triangolo della frode individuando le tre caratteristiche che sono sempre presenti:

- incentivi e/o pressioni;
- occasioni;
- inclinazioni/giustificazioni.

Il principio di revisione approfondisce, inoltre, i fattori di rischio strettamente connessi all'attività del revisore e che possono essere individuati in tutti i casi di frode rientranti nella categoria della falsa informativa finanziaria e dell'appropriazione illecita di beni e attività. L'appendice del documento riporta, infatti, tutti i fattori di rischio suddivisi in base alle due categorie sopraripportate e distinti a seconda che si riferiscano a incentivi e pressioni, opportunità e giustificazioni.

1.2.3 Le caratteristiche del perfetto frodatore

Come evidenziato nei precedenti paragrafi, la frode è un illecito in cui è assente l'elemento della violenza e in cui il soggetto che la pone in essere usa tutti gli strumenti a sua disposizione per dissimulare l'azione. Il frodatore è un "insospettabile" in grado di mascherare la propria condotta grazie al proprio status sociale e alla posizione professionale e lavorativa ricoperta. È, inoltre, un soggetto che opera su impulso di pressioni che derivano dall'esigenza di soddisfare dei bisogni considerati necessari ed indispensabili e spinto dalle reali opportunità di poter porre in essere il proprio disegno criminoso. Al contempo, il frodatore presenta delle particolari caratteristiche personali e psicologiche che gli consentono di giustificare il proprio operato, ciò è influenzato, in particolare, dal livello di integrità personale che può incentivare o disincentivare l'azione[54].
Gli elementi elencati e la capacità dei frodatori di porre in essere strategie in grado di occultare il proprio operato, rendono particolarmente difficile prevenire e individuare le frodi, ma anche

[54] Cfr. POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 31; *«(…) la scelta di "deviare" dal corretto modo di agire e l'abilità di giustificare tale comportamento trovano origine più in fattori attinenti alla psiche di un soggetto che alla sua razionalità».*

svolgere le necessarie indagini[55]. *«Ciò che invece parrebbe essere più difficile da gestire da parte di tali soggetti e, pertanto potrebbe rappresentare un valido strumento idoneo a mettere in risalto la presenza di elementi sintomatici del compimento di un'azione illegale riguarda la sfera più strettamente personale di un individuo, il suo modo di agire, il suo comportamento e atteggiamento esteriore[56]».* Pogliani (et al.) intendono così mettere in evidenza le difficoltà dell'individuo di mantenere il controllo ed avere un comportamento e atteggiamenti sempre lineari nel corso del tempo. La dimensione psicologica deve essere, quindi, sempre considerata in modo opportuno in quanto da questi aspetti è possibile acquisire importanti elementi che consentono di migliorare le opportunità di individuazione di una frode e delle motivazioni che hanno spinto i suoi autori a implementarla. Da tali considerazioni emerge l'importanza di comprendere il profilo tipico di un frodatore, da valutare come un aspetto chiave nell'attività di prevenzione e individuazione delle frodi, ciò anche in relazione al fatto che le caratteristiche tipiche di un "colletto bianco" sono molto differenti da quelle di altre categorie di criminali[57].

L'importanza degli aspetti psicologici e personali dei frodatori è stata confermata dagli studiosi Tommie e Aaron Singleton che evidenziano come, considerando i dati provenienti dagli studi criminologici e sociologici, le frodi non sono causate esclusivamente da fattori esterni all'individuo, legati quindi alle condizioni economiche, politiche e sociali e a pressioni di carattere competitivo, ma anche da fattori psicologici e interiori che rendono alcuni soggetti maggiormente predisposti a commettere questo tipo di reati[58].

---

[55] POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 30; *«Tutte le informazioni, le osservazioni e le analisi effettuate da settant'anni a questa parte hanno evidenziato la indiscussa capacità dei frodatori non solo di elaborare sottili e sofisticate strategie di azione, ma anche di utilizzare tutta una serie articolata e complessa di strumenti utili a mascherare il loro operato, rendendo così difficoltoso ogni tentativo di prevenzione ma anche di indagine tu tali crimini».*

[56] POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 30.

[57] SINGLETON T., SINGLETON A., *Fraud Auditing and Forensic Accounting*, Four Edition, John Wiley & Sons, Inc, 2010, p. 49; *«A key aspect of preventing and detecting fraud is to understand the profile of typical fraudsters, by type of fraud. Regarding asset misappropriation, the person is usually someone who was not suspected, oftentimes least suspected.*
The profile of white-collar criminals is very different from blue-collar criminals, or street criminals. This fact makes fraud even more difficult to prevent or detect».

[58] SINGLETON T., SINGLETON A., *Fraud Auditing and Forensic Accounting*, Four Edition, John Wiley & Sons, Inc, 2010, p. 49; *«In view of the principles mentioned, one might conclude that fraud is caused mainly by factors external to the individual: economic, competitive, social, and political factors, and poor controls. But how about the individual? Are some people more prone to commit fraud than others? And if so, is that a more serious cause of fraud than the external and internal environmental factors previously discussed? Data from criminology and sociology seem to suggest so»*.

L'analisi condotta dagli autori parte da alcuni concetti generali che è possibile affermare sul modo in cui le persone agiscono, ciò considerando i concetti di "onestà" e "disonestà":

«Begin by making a few generalizations about people:

- *Some people are honest all of the time.*
- *Some people are dishonest all of the time.*
- *Most people are honest some of the time.*
- *Some people are honest most of the time.»* [59]

L'analisi prosegue considerando che, al di fuori delle generalizzazioni appena descritte, le persone agiscono sulla base di molteplici ragioni collegate sia alla sfera personale sia a situazioni organizzative. In particolare, viene proposta una suddivisione tra tre tipologie di variabili:

- variabili personali;
- variabili organizzative;
- variabili esterne.

Nella prima categoria di variabili rientrano le attitudini e abilità personali, gli atteggiamenti e le preferenze, i bisogni e i desideri personali e, infine, i valori e le convinzioni che contraddistinguono l'individuo. Le variabili organizzative sono strettamente legate, invece, alla tipologia di lavoro svolto e alle caratteristiche organizzative e gestionali dell'azienda. Gli autori fanno riferimento, infatti, alla natura e allo scopo del lavoro, agli strumenti e al livello di formazione fornito, alla presenza di un sistema di ricompensa e riconoscimento, al livello qualitativo della gestione e della supervisione, alla chiarezza delle responsabilità del ruolo e degli obiettivi da perseguire, alla fiducia interpersonale e al clima motivazionale ed etico che caratterizza l'organizzazione, in particolare in riferimento al *Tone at the top* e al comportamento e ai valori che ispirano il comportamento di superiori e colleghi.

Le variabili esterne completano il quadro appena descritto considerando ulteriori elementi che possono favorire comportamenti fraudolenti quali il grado di concorrenza presente nel settore di appartenenza, le condizioni economiche generali e i valori sociali, in questo caso facendo riferimento anche ai valori etici dei concorrenti e dei principali modelli politici e sociali.

Seppur esemplificativa e non esaustiva, l'elencazione delle variabili consente di avere un'idea più approfondita degli innumerevoli fattori che possono agire sulla psiche di un individuo e favorire comportamenti criminosi. La componente psicologica e personale gioca, quindi, un ruolo molto

[59] SINGLETON T., SINGLETON A., *Fraud Auditing and Forensic Accounting*, Four Edition, John Wiley & Sons, Inc, 2010, p. 49.

importante anche nelle attività di individuazione delle frodi potendo, al contempo, favorire o limitare le possibilità di individuare i relativi segnali.

La componente psicologica può costituire un limite nell'individuazione delle frodi, o meglio dei frodatori, in quanto i dipendenti che hanno maggiori opportunità di commettere una frode sono i soggetti in cui la proprietà o il management ripone il più alto livello di fiducia: *«(…) management will often be surprised by the identity of the dishonest employee. It is most often someone who was trusted and widely regarded as a good employee. It is only logical that the trusted employees would have access and opportunity to commit fraud.*

Managers typically do not provide access to information and assets for employees they don't trust. Only the trusted employees can access the bank accounts and look at confidential information—exactly the type of access that is needed to commit fraud»[60].

Di conseguenza, maggiore è il grado di fiducia risposto nei dipendenti e l'alto ruolo ricoperto in azienda, minori saranno i sospetti del management che tali soggetti possano essere disonesti e porre in essere attività fraudolente.

Allo stesso tempo, il comportamento di chi commette una frode può costituire un importante elemento per la sua individuazione. Come accennato nella parte iniziale del presente paragrafo, è difficile per un individuo agire sempre in modo lineare e coerente nel tempo. Di conseguenza il comportamento e l'atteggiamento esteriore possono costituire importanti segnali per l'individuazione di un'azione illecita. I cambiamenti nei comportamenti e nello stile di vita dei dipendenti costituiscono un fattore da monitorare attentamente e analizzare con l'obiettivo di individuare potenziali indizi di frode. I fattori da considerare sono molteplici e molto differenti tra loro. Innanzitutto, devono essere attentamente valutate eventuali dipendenze da alcol e droghe che possono costituire la causa che spinge un individuo a frodare per poter ottenere le risorse necessarie a sostenere i costi di tali dipendenze o subentrare successivamente come conseguenza dell'illecito commesso[61]. Analoghe considerazioni possono essere sviluppate per tutte le tipologie di dipendenza come quella del gioco d'azzardo.

«Behavioral changes, such as becoming uncooperative, argumentative, or defensive, can be signs of problems as well. These behaviors may be signs of dissatisfaction at work, which could be a

[60] COENEN T.L., *Expert Fraud Investigation. A step by step guide*, John Wiley & Sons, Inc, 2009, p. 10; l'autore spiega chiaramente come frequentemente il management sia sorpreso dell'identità del o dei dipendenti disonesti presenti in azienda, ciò in quanto, nella maggior parte dei casi, si tratta delle persone nelle quali si riponeva un maggior grado di fiducia.

[61] GOLDEN T.W., SKALAK S. L., CLAYTON M.M., *A guide to forensic accounting investigation*, John Wiley & Sons, Inc., Hoboken, New Jersey, 2006, p. 300.

reason for an employee to commit fraud. Or they could be an outward sign of an employee's stress as she or he engages in on-the-job fraud»[62].

Senza considerare situazioni e problemi più gravi ed evidenti, quindi, anche cambiamenti comportamentali apparentemente meno significativi possono rappresentare chiari segnali di possibili frodi, in particolare quando è presente un alto livello di insoddisfazione che rende un dipendente poco collaborativo e sempre "sulla difensiva". A tutto ciò è necessario aggiungere eventuali cambiamenti riscontrati nel tenore di vita che difficilmente un frodatore riuscirà a tenere nascosti soprattutto nel lungo periodo. Di frequente, infatti, le maggiori possibilità economiche spingono chi ha commesso una frode a cedere all'acquisto di beni di lusso o troppo costosi rispetto al tenore di vita che si intende mostrare all'esterno.

«None of these lifestyle changes alone is a definite indicator that fraud is occurring. Even several of these characteristics identified in one employee may not mean that a fraud is in progress. However, these signs are small pieces of a puzzle, and they should be watched carefully, because they are sometimes related to an occupational fraud.[63]*»*

Gli aspetti personali dei potenziali frodatori sono, ovviamente, da valutare non in modo isolato ma in correlazione con altri *red flag* individuati tramite le attività di controllo che, se significativi e sufficienti, possono condurre all'individuazione di chiari segnali di frode.

Considerando l'importanza del profilo psicologico e delle caratteristiche personali dei frodatori, sono stati condotti numerosi studi e analisi empiriche, in particolare dall'ACFE a partire dal 1993. Facendo riferimento al primo report pubblicato nel 2010 sul "*Report to the Nation on occupational fraud and abuse"*, Pogliani (et al.) hanno evidenziato l'importanza di tali studi nel determinare i c.d. "tratti demografici" dei frodatori, facendo riferimento, in particolare, alla categoria degli *occupational fraud*[64]. Gli autori hanno sintetizzato quanto emerso dalla ricerca mettendo in evidenza che *«in media, le frodi di maggiori dimensioni – o, meglio, che hanno provocato il danno economico più ampio – sono state realizzate da soggetti collocati ai più alti livelli della scala gerarchica aziendale, in grande maggioranza di sesso maschile, con un'età*

---

[62] COENEN T.L., *Expert Fraud Investigation. A step by step guide*, John Wiley & Sons, Inc, 2009, p. 9.

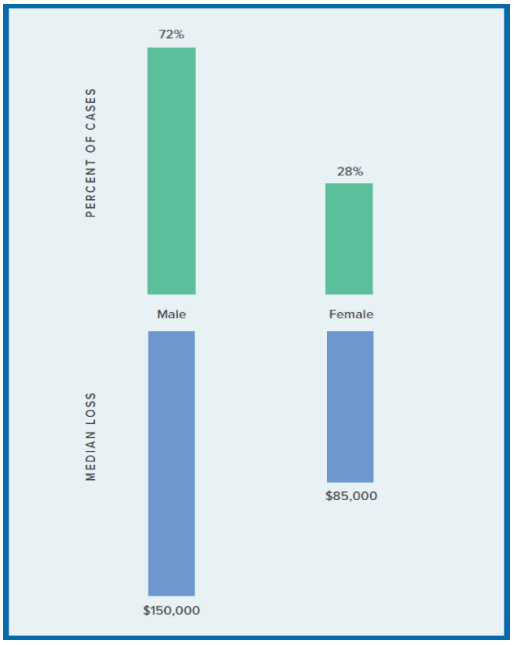
[63] COENEN T.L., *Expert Fraud Investigation. A step by step guide*, John Wiley & Sons, Inc, 2009, p. 9.

[64] POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 32; gli autori sottolineano che lo scopo degli studi condotti dall'ACFE sia quello di ottenere maggiori informazioni sulle caratteristiche tipiche dei soggetti che commettono azioni illecite ai danni delle aziende in cui sono assunti precisando che il termine "occupational fraud" è utilizzato *«per indicare lo sfruttamento della posizione professionale per il proprio esclusivo arricchimento mediante il deliberato abuso o illegittimo sfruttamento delle risorse o, più in generale, del patrimonio di un'organizzazione economica».*

oscillante fra i 40 e i 60 anni, un'anzianità media superiore ai 10 anni presso l'azienda e un grado di scolarità alquanto elevata[65]*.»*

Il *Report to the Nations* del 2020, conferma gran parte di questi dati, presentando, allo stesso tempo, le evoluzioni che vi sono state nel corso dell'ultimo decennio nelle caratteristiche dei frodatori. La maggioranza dei frodatori è ancora di sesso maschile con una percentuale del 72% e una perdita media causata all'azienda di 150.000,00 $ rispetto agli 85.000,00 $ stimati per il genere femminile[66].

Figura 10 - Distribuzione di genere



Fonte: ACFE, Report to the Nations. 2020 Global Study on occupational fraud and abuse, p.43

È interessante evidenziare come le percentuali appena descritte presentino delle importanti variazioni se si fa riferimento a singole regioni. Il gap tra uomini e donne, infatti, tende quasi ad azzerarsi se si considera il Nord America in cui la percentuale maschile dei frodatori si abbassa al 59%, mentre guardando ai dati relativi al Nord Africa e al Sud-est Asiatico i frodatori risultano per più del 90% uomini[67]. In Europa il rapporto si mantiene, invece, in linea con la media mondiale.

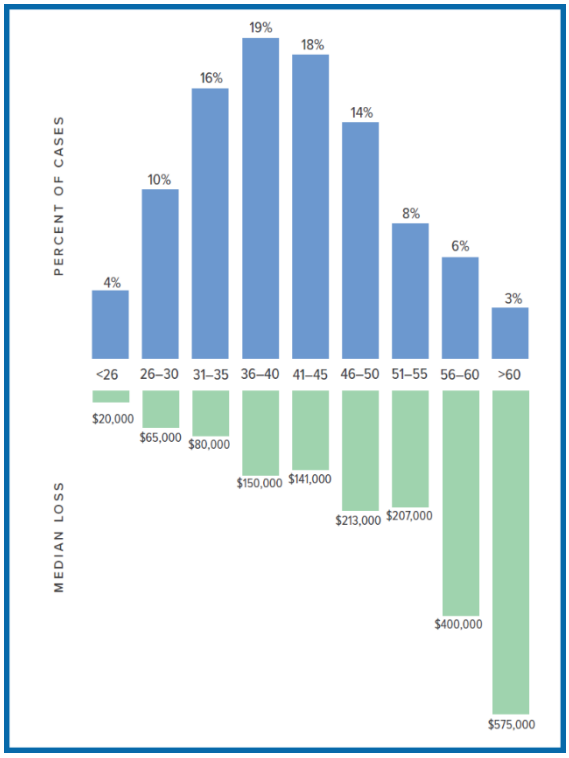
[65] POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 32.
[66] Cfr. ACFE, *Report to the Nations. 2020 Global Study on occupational fraud and abuse.*
[67] ACFE, *Report to the Nations. 2020 Global Study on occupational fraud and abuse*, p. 43; *«There was a large variance in the gender distribution of occupational fraudsters based on geographic region (…) in the United States and Canada, males accounted for only 59% of occupational fraud perpetrators, whereas in*

Approfondendo i dati sulla distribuzione di genere in relazione al ruolo ricoperto in azienda, la percentuale di frodi commesse dagli uomini aumenta fortemente all'aumentare del livello occupazionale. Se si considera, infatti, la categoria degli impiegati, le percentuali risultano del 64% e 36%, rispettivamente relative agli uomini e alle donne, con una perdita media causata di 60.000,00 $ (identica per i due generi). La situazione cambia fortemente per le categorie dei manager e dei proprietari/amministratori che presentano una percentuale di frodatori uomini dell'86% con una perdita media di 795.000,00 $ rispetto ai 172.000,00 $ stimati per le donne.
L'analisi effettuata dall'ACFE ha consentito di costruire una vera e propria "mappa" della distribuzione di genere che, in parte, conferma i dati statistici relativi al livello occupazionale e alle percentuali di uomini e donne che rivestono posizioni chiave in ambito lavorativo. Le differenze sono, quindi, anche correlate al divario esistente nelle prospettive di crescita lavorativa e di avanzamento di carriera tuttora presenti tra uomini e donne e alle maggiori opportunità per chi riveste ruoli più elevati all'interno della gerarchia aziendale di commettere azioni fraudolente. Per quanto riguarda l'età media rilevata dall'ultimo report, è possibile notare come il 53% dei frodatori abbia un'età compresa tra i 31 e i 45 anni, mentre la media delle perdite cagionate aumenta all'aumentare dell'età del frodatore fino ad arrivare a un valore di 575.000,00 $ per le frodi commesse da soggetti con età superiore ai sessanta anni[68]. In figura sono riportati tutti i dati suddivisi per fascia d'età.

Southern Asia and the Middle East and North Africa, men committed more than 90% of occupational frauds.»

[68] ACFE, *Report to the Nations. 2020 Global Study on occupational fraud and abuse*, p. 45.

Figura 11 - Distribuzione per fasce d'età



Fonte: ACFE, Report to the Nations. 2020 Global Study on occupational fraud and abuse, p.45

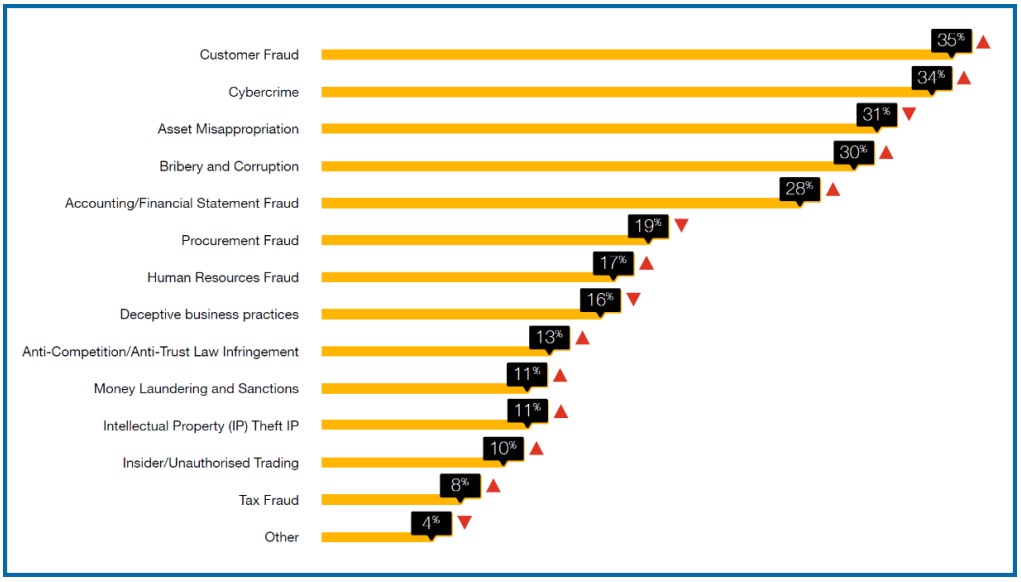
1.2.4 Gli impatti delle frodi sul sistema economico e aziendale

La frode è un fenomeno in costante evoluzione e crescita in quanto sono sempre più numerose le possibilità e le modalità con cui è possibile dar vita a questo tipo di reato. Il tasso delle frodi resta, quindi, molto alto nonostante siano sempre più numerosi ed efficaci gli strumenti e le tecniche utilizzate per prevenirle e contrastarle e la numerosità dei casi è accompagnata da ingenti perdite per il sistema economico e aziendale.

In base al PwC's *Global Economic Crime e Fraud Survey* del 2020, le perdite registrate negli ultimi 24 mesi a causa delle frodi ammontano a circa 42 bilioni di dollari statunitensi. Il dato tiene conto soprattutto dei costi effettivamente quantificabili come perdite, dei costi finanziari diretti, delle sanzioni, in quanto altra parte dei costi è di difficile determinazione poiché legata ai danni di

immagine dell'azienda, alla posizione di mercato nonché alle future opportunità di crescita[69]. La *survey* del 2020 della *Big Four* è stata condotta analizzando le risposte e la situazione di più di 5.000 intervistati, il 47% dei quali ha dichiarato di aver avuto esperienza di frode negli ultimi 24 mesi[70]. In venti anni questo dato si colloca al secondo posto per quantità di frodi riscontrate, con una media di incidenti per azienda pari a 6 nel periodo considerato e un forte aumento rilevato delle seguenti tipologie di frode: *Costumer fraud*, *Cybercrime*, Appropriazione indebita di beni aziendali, abuso d'ufficio e corruzione[71]. Nel grafico seguente, tratto dal documento redatto da PwC viene mostrata nel dettaglio l'incidenza di ciascuna tipologia di frode e l'incremento o decremento rispetto al passato.

Figura 12 - Frequenza per tipologia di frode



Fonte: PwC's Global Economic Crime e Fraud Survey, Fighting fraud: A never-ending battle, PWC, 2020, p.4.

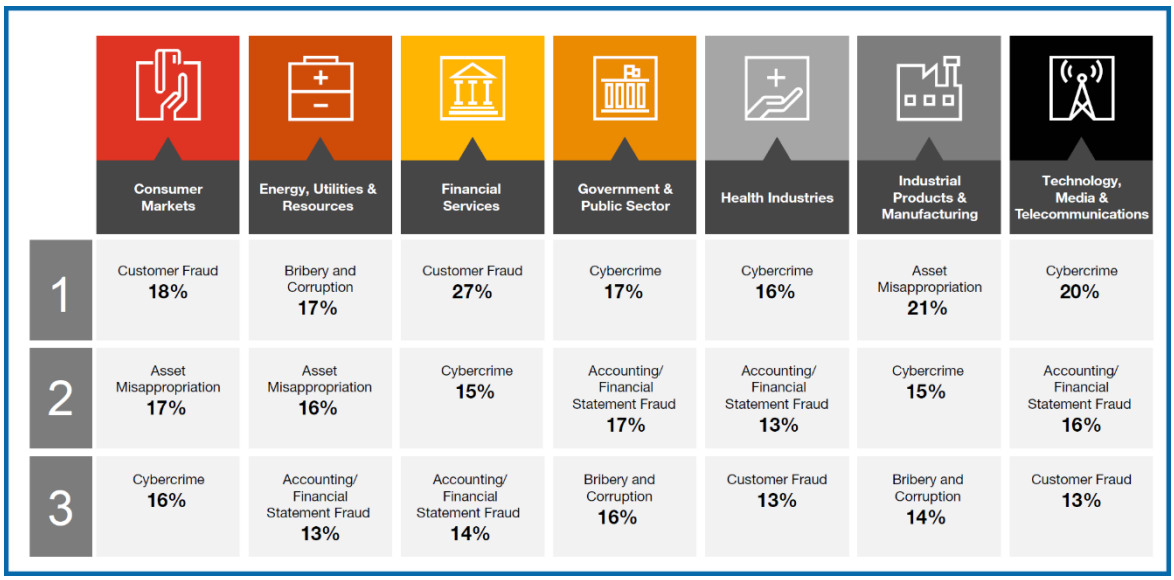
[69] PwC's Global Economic Crime e Fraud Survey, *Fighting fraud: A never-ending battle*, PWC, 2020, p.7; *«Fraud losses are complex. Some costs can be tallied: direct financial loss or costs due to fines, penalties, responses and remediation. But some costs are not easily quantified — including brand damage, loss of market position, employee morale, and lost future opportunities.»*

[70] PwC's Global Economic Crime e Fraud Survey, Fighting fraud: A never-ending battle, PWC, 2020, p. 3.

[71] Cfr. PwC's Global Economic Crime e Fraud Survey, Fighting fraud: A never-ending battle, PWC, 2020, p. 3

L'analisi ha inoltre approfondito la distribuzione delle tipologie di frode tra i principali settori di riferimento: è interessante notare come, tra le prime tre tipologie di frode presenti in ciascun settore, rientra quasi per tutte quella del *cybercrime*.

Figura 13 - Distribuzione delle frodi per settore



	Consumer Markets	Energy, Utilities & Resources	Financial Services	Government & Public Sector	Health Industries	Industrial Products & Manufacturing	Technology, Media & Telecommunications
1	Customer Fraud **18%**	Bribery and Corruption **17%**	Customer Fraud **27%**	Cybercrime **17%**	Cybercrime **16%**	Asset Misappropriation **21%**	Cybercrime **20%**
2	Asset Misappropriation **17%**	Asset Misappropriation **16%**	Cybercrime **15%**	Accounting/ Financial Statement Fraud **17%**	Accounting/ Financial Statement Fraud **13%**	Cybercrime **15%**	Accounting/ Financial Statement Fraud **16%**
3	Cybercrime **16%**	Accounting/ Financial Statement Fraud **13%**	Accounting/ Financial Statement Fraud **14%**	Bribery and Corruption **16%**	Customer Fraud **13%**	Bribery and Corruption **14%**	Customer Fraud **13%**

Fonte: PwC's Global Economic Crime e Fraud Survey, Fighting fraud: A never-ending battle, PWC, 2020, p.4.

Circa il 13% degli intervistati ha, inoltre, dichiarato di aver subito perdite maggiori a 50 milioni di dollari per singolo episodio. I danni causati da frodi messe in atto da soggetti interni all'azienda (37%) provocano perdite più ingenti rispetto a quelle implementate da soggetti interni: il 43% delle frodi caratterizzate da perdite superiori a 100 milioni si riferisce, infatti, proprio a soggetti interni, i c.d. *insiders*.

1.3 I principali schemi di frode

1.3.1 La classificazione delle frodi

Da quanto analizzato nei precedenti paragrafi è emerso chiaramente come le possibilità e le modalità di commettere una frode siano in continua evoluzione e trasformazione e di come i frodatori implementino piani e programmi molto dettagliati e accurati al fine di occultare il proprio disegno criminoso. Allo stesso tempo, in base alla casistica e allo studio delle frodi individuate nel corso degli anni, è possibile constatare come gli schemi di frode attuati siano sostanzialmente invariati. *«Se dunque è vero che il perpetratore delle medesime è generalmente reputato essere un soggetto in possesso di elevate doti di intelligenza, competenza e creatività, è altrettanto vero che queste non sono, se non eccezionalmente, applicate alla progettazione di schemi fraudolenti innovativi o particolarmente complessi nella loro essenza, quanto piuttosto nelle complementari azioni di "occultamento" messe in atto allo scopo, appunto, di mascherare l'intento ultimo delle attività compiute*[72]*».*

Per queste motivazioni, è stato possibile raccogliere e categorizzare gli schemi di frode in base a specifiche metodologie e criteri di classificazione, a volte anche molto differenti tra loro, che confrontano gli schemi creando dei *cluster* omogenei in base alle caratteristiche tipiche di ognuno.

Ai fini dell'analisi svolta è opportuno non considerare l'intera categoria dei *white collar crime,* ma restringere il campo di indagine a quella degli *occupational fraud*, frodi commesse da un individuo nell'ambito dell'organizzazione economica in cui è impiegato. Un'importante definizione di *occupational fraud* è fornita dall'ACFE che afferma quanto segue *«Occupational fraud is formally defined as the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets*[73]*».*

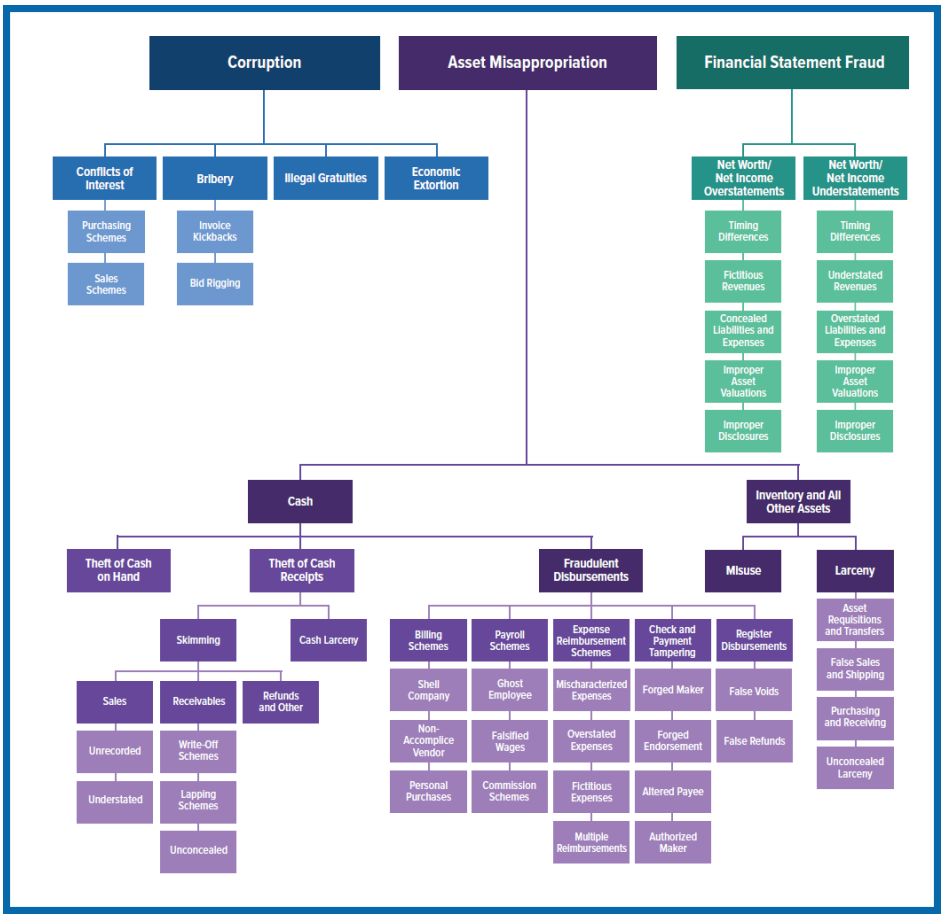
Considerando tale definizione, l'ACFE classifica le frodi secondo lo schema noto come *Fraud Tree*, così chiamato per la sua tipica struttura ad albero che prevede la suddivisione delle frodi in tre categorie principali:

1. *Corruption* - corruzione;
2. *Asset Misappropriation* – appropriazione indebita di beni aziendali;

[72] POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 64; gli autori mettono in evidenza come nel tempo vengano implementati prevalentemente schemi di frode consolidati, spesso caratterizzati da logiche e meccanismi molto semplici.
[73] ACFE, *Report to the Nations. 2020 Global Study on occupational fraud and abuse*, p. 6.

3. *Financial Statement Fraud* – falsa informativa finanziaria.

Figura 14 - Albero delle frodi



Fonte: ACFE, Report to the Nations. 2020 Global Study on occupational fraud and abuse, p.11

Quando si parla di corruzione si fa riferimento a soggetti che utilizzano il proprio ruolo per influenzare un'operazione e ottenere benefici per sé stessi o per altri violando le regole di comportamento e le procedure imposte dalla propria organizzazione economica e i diritti di terzi[74]. L'appropriazione indebita di beni aziendali si riferisce, invece, al furto o all'utilizzo improprio di beni aziendali, mentre la falsa informativa finanziaria comprende tutte le ipotesi di falsificazione del bilancio di un'organizzazione economica[75].

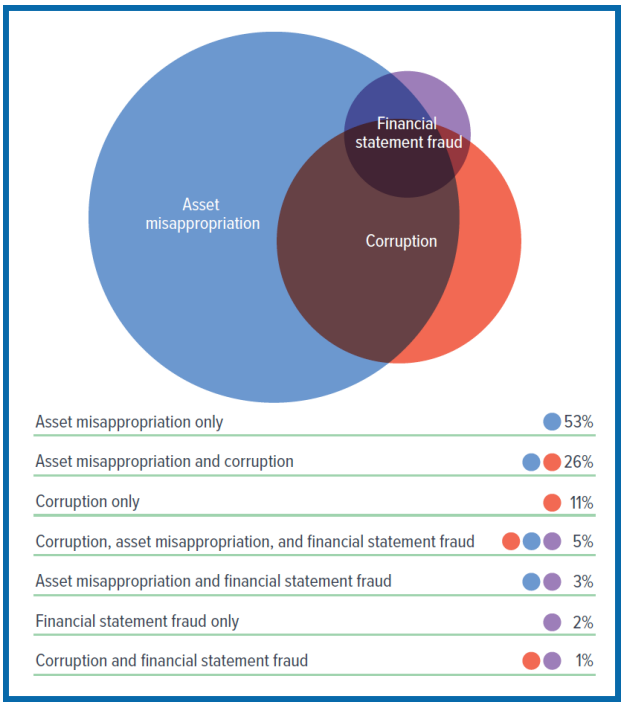
[74] POGLIANI G., PECCHIARI N., MARIANI M., Frodi aziendali. Forensic accounting, fraud auditing e litigation, Egea, 2012, p. 71; *«In particolare rientrano nella fattispecie richiamata le promesse, le offerte di tangenti o altri vantaggi come pure le pressioni e i condizionamenti di decisioni o scelte di soggetti pubblici o aziendali in presenza di conflitti di interessi».*

[75] ALBRECHT W.S., ALBRECHT C.O., ALBRECHT C.C., ZIMBELMAN M.F., *Fraud Examination*, Fourth edition, South-Western Cengage Learning, 2011, p. 10.

L'appropriazione indebita rappresenta la tipologia di frode più diffusa con una percentuale di incidenza dell'86% rispetto al totale delle *occupational fraud* commesse, ma con un impatto in termini di perdite provocate all'organizzazione che ne è vittima di gran lunga inferiore rispetto alle altre tipologie e, in particolare, alla falsa informativa finanziaria[76]. Il report dell'ACFE evidenzia come, a fronte di un'incidenza del 10% sul totale, i casi di falsa informativa finanziaria determinano una perdita media di 954.000,00 $ rispetto ai 100.000,00 $ stimati per l'appropriazione indebita di beni aziendali e i 200.000,00 $ per la corruzione[77].

L'ACFE, nel report del 2020, ha anche sottolineato come, in almeno un terzo dei casi il frodatore commette più schemi di frode appartenenti a differenti categorie. La massima frequenza è raggiunta dall'appropriazione indebita correlata a fenomeni di corruzione: le due tipologie di frode si presentano contestualmente nel 26% dei casi. Il grafico seguente riporta nel dettaglio l'incidenza di ciascuna categoria di frode, considerata singolarmente e associata a una o più delle altre tipologie.

Figura 15 - Casi in cui un frodatore commette più di una tipologia di frode



Fonte: ACFE, Report to the Nations. 2020 Global Study on occupational fraud and abuse, p.12

[76] Cfr. ACFE, *Report to the Nations. 2020 Global Study on occupational fraud and abuse*, p. 10; POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 70 e ss.

[77] ACFE, *Report to the Nations. 2020 Global Study on occupational fraud and abuse*, p. 10.

Oltre alla classificazione delle frodi appena analizzata e che sarà approfondita nei successivi paragrafi, sono presenti altre due tipologie di classificazione molto utilizzate. La prima suddivide le frodi tra quelle perpetrate "contro" un'organizzazione economica e quelle perpetrate "per conto" della stessa: nel primo caso, vittima della frode sarà proprio l'organizzazione economica, mentre nel secondo i danni derivanti dalla frode andranno ad incidere su soggetti terzi. Esempio della seconda tipologia di frode è il caso della falsa informativa finanziaria effettuata per presentare una migliore situazione economico finanziaria dell'azienda e risultati superiori in termini di performance «*In this case, the executives of the company benefit because a company's stock price increases or remains artificially high and the victims are investors in the company's stock*[78]».

Le frodi possono essere, infine, classificate in base al soggetto che ne è vittima. La classificazione comprende quattro categorie di riferimento[79]:

- Frodi in cui la vittima è l'organizzazione economica;
- *Management fraud*;
- Frodi ai danni di investitori e consumatori;
- Altre frodi.

La prima categoria prevista raggruppa tutte le frodi in cui la vittima è la stessa organizzazione economica e il soggetto che la pone in essere può essere un dipendente, un fornitore o un cliente. Di seguito una breve descrizione delle differenti tipologie appena elencate:

- *Employee embezzlement* (appropriazione indebita da dipendenti): si tratta di un tipo di frode in cui il soggetto che la pone in essere è un dipendente che a sua volta sottrae beni ad altri dipendenti sfruttando la propria posizione lavorativa.
- *Vendor fraud* (frode attuata da parte dei fornitori): questa tipologia di frode è messa in atto da un fornitore ai danni dell'organizzazione economica a cui sono venduti beni o servizi, ciò mediante forniture non conformi agli accordi contrattuali intercorsi.
- *Customer fraud* (frode attuata da parte dei consumatori): in questo caso sono i consumatori ad agire frodando l'organizzazione economica dalla quale acquisiscono beni

[78] ALBRECHT W.S., ALBRECHT C.O., ALBRECHT C.C., ZIMBELMAN M.F., *Fraud Examination*, Fourth edition, South-Western Cengage Learning, 2011, p. 9; gli autori evidenziano che molto spesso l'alterazione sia finalizzata a gonfiare i risultati aziendali per poter aumentare i bonus di fine anno dei dirigenti e che spesso tale tipologia di frode coinvolge organizzazioni economiche che hanno conseguito perdite nei precedenti esercizi o risultati inferiori alle aspettative.

[79] Cfr. ALBRECHT W.S., ALBRECHT C.O., ALBRECHT C.C., ZIMBELMAN M.F., *Fraud Examination*, Fourth edition, South-Western Cengage Learning, 2011, p. 10.

o servizi. *«Customers don't pay, pay too little, or get too much from the organization through deception»*[80].

Il *management fraud* si identifica, invece, con la falsa informativa finanziaria e, quindi, con la manipolazione dei bilanci e dei risultati ottenuti dall'organizzazione economica al fine di presentare una situazione migliore a danno degli azionisti e dei finanziatori[81].

A differenza della tipologia di frode appena analizzata, le frodi perpetrate contro investitori e consumatori possono essere attuate da qualsiasi tipo di persona per attirare con l'inganno altri individui e convincerli ad investire in schemi fraudolenti.

Nella categoria delle altre frodi, infine, rientrano tutte le azioni illecite che non è possibile ricondurre a una delle altre categorie precedentemente descritte.

Nei paragrafi successivi saranno analizzate più nel dettaglio le tre macrocategorie relative alle *Occupational Fraud*, le loro caratteristiche e gli schemi più importanti che fanno riferimento a ciascuna di esse.

1.3.2 Corruzione

La corruzione rappresenta la prima categoria di *Occupational Fraud* presente nell'Albero delle Frodi elaborato dall'ACFE. Per le sue caratteristiche, rientra pienamente nell'ambito dei *white collar crime* e si colloca probabilmente tra le più antiche forme di frode. Tipicamente la corruzione si considera legata ai rapporti con la pubblica amministrazione e finalizzata ad ottenere agevolazioni e "favori" aggirando il normale e regolare iter burocratico, ma risulta ampiamente diffusa anche nell'ambito dei rapporti privati[82].

«These types of schemes involve a payoff in return for some sort of advantage or preferential treatment, an undisclosed relationship that nets a party a financial or operational advantage or favor, or an attempt to force certain preferential action to be taken[83]*».*

In base alla precedente definizione, è chiaro che la corruzione possa essere finalizzata ad ottenere qualsiasi tipologia di vantaggio o di trattamento preferenziale e che non necessariamente

[80] ALBRECHT W.S., ALBRECHT C.O., ALBRECHT C.C., ZIMBELMAN M.F., *Fraud Examination*, Fourth edition, South-Western Cengage Learning, 2011, p. 10; è tramite l'inganno che i consumatori riescono ad ottenere forniture maggiori o a pagare un prezzo inferiore rispetto a quanto concordato contrattualmente.

[81] SINGLETON T., SINGLETON A., BOLOGNA J., LINDQUIST R., *Fraud Auditing and Forensic Accounting*, Third Edition, John Wiley & Sons, Inc, 2006, p. 45.

[82] POGLIANI G., PECCHIARI N., MARIANI M., Frodi aziendali. Forensic accounting, fraud auditing e litigation, Egea, 2012, p. 112.

[83] COENEN T.L., *Expert Fraud Investigation. A step by step guide*, John Wiley & Sons, Inc, 2009, p. 153.

l'obiettivo sia correlato all'acquisizione di benefici di tipo finanziario[84]. Affinché si verifichi questa tipologia di frode è sempre necessaria la presenza di almeno due soggetti, un delegante e un delegato che agisce per consentire al primo l'ottenimento di un beneficio illecito[85]. Come in qualsiasi schema di frode anche la corruzione è sempre intenzionale e implica la pianificazione e la premeditazione delle azioni da svolgere e il contestuale occultamento dell'illecito. *«Scopo del corruttore è quello di indurre, dietro riconoscimento di denaro o altro beneficio, un individuo (corrotto) ad agire impropriamente nell'esercizio delle proprie funzioni per il conseguimento di un vantaggio. Questo indebito vantaggio rappresenta la manifestazione del danno provocato da tale crimine e consente di identificare chi, direttamente o indirettamente, lo abbia subito[86]».*

I danni provocati da fenomeni di corruzione sono ingenti e molteplici, ciò per differenti ragioni. Innanzitutto, per poter corrompere un individuo è necessario corrispondergli denaro o altri benefici che, necessariamente, non potranno essere tracciati e provenire da operazioni lecite. Nella maggior parte dei casi, infatti, come evidenziato anche nel precedente paragrafo, la corruzione è un fenomeno che si accompagna ad altre attività fraudolente e, in particolare, all'appropriazione indebita di beni aziendali. Generalmente l'appropriazione indebita rappresenta lo strumento che consente di concretizzare un episodio di corruzione e ottenere i mezzi necessari a poterlo attuare.

Il danno cagionato alle organizzazioni economiche deriva, quindi, sia dalle risorse sottratte illecitamente all'organizzazione economica e da utilizzare per l'azione corruttiva da implementare, sia dalle perdite che derivano dall'impossibilità per l'azienda di operare alle normali condizioni di mercato (con riferimento ai processi della domanda e dell'offerta di beni e servizi) e conseguire profitti e risultati più elevati[87].

La corruzione è un fenomeno che può essere a sua volta suddiviso in quattro sottocategorie che sottendono differenti schemi di frode:

---

[84] Cfr. POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 112; *«la corruzione implica la violazione di un dovere inerente alla propria posizione, è finalizzata al conseguimento di un beneficio (non necessariamente economico) ed è realizzata in forma non manifesta e riservata»*.

[85] Cfr. SINGLETON T., SINGLETON A., BOLOGNA J., LINDQUIST R., Fraud Auditing and Forensic Accounting, Third Edition, John Wiley & Sons, Inc, 2006, p. 101.

[86] POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 113.

[87] COENEN T.L., *Expert Fraud Investigation. A step by step guide*, John Wiley & Sons, Inc, 2009, p. 153; *«Corruption schemes deprive companies, their owners, and employees of honest services and make it impossible for companies to compete fairly in the bid process or earn all of the profits to which they are entitled. When an employee or associate is taking money off the top of a transaction or compromising a company's process, the harm is more far-reaching than she or he probably realizes»*.

1. *Bribery* (corruzione);
2. Conflitto di interessi;
3. Estorsione;
4. *Illegal gratuities*

Bribery

I termini *Bribery* e *Corruption* possono essere entrambi tradotti come "corruzione" in italiano, ma nel gergo legale presentano un significato e una definizione differente.

Per *Bribery* si intende *«A price, reward, gift, or favor bestowed or promised with a view to pervert the judgment of or influence the action of a person in a position of trust»*, mentre con il termine *Corruption* si fa riferimento a *«The act of doing something with an intent to give some advantage inconsistent with official duty and the rights of others; a fiduciary ' s or official ' s use of a station or office to procure some benefit either personally or for someone else, contrary to the rights of others»*[88].

Il termine *Corruption* ha, quindi, una portata più ampia e, considerando la classificazione dell'ACFE, rappresenta l'intera categoria di frodi in cui rientrano *Bribery*, *Conflict of Interest schemes*, *Economic Extortion schemes* e *Illegal Gratuity schemes*.

Quando si parla di corruzione in senso stretto si fa riferimento, invece, a tutte le attività che comportano l'offerta o la ricezione di denaro o altri valori al fine di influenzare un atto ufficiale[89].

Se la corruzione è finalizzata a influenzare una decisione relativa al business o alle scelte di un'organizzazione economica si parla, nello specifico, di *commercial bribery* e l'azione illecita coinvolge non agenti governativi o impiegati pubblici, ma dipendenti dell'azienda coinvolta[90].

---

[88] VONA L.W., *Fraud Risk Assessment. Building a Fraud Audit Program*, John Wiley & Sons, Inc., 2008, p. 135; le definizioni sono tratte dal *Black ' s Law Dictionary* e consentono di distinguere e definire correttamente i due termini.

[89] ASSOCIATION OF CERTIFIED FRAUD EXAMINERS, *Fraud Examiners Manual*, 2011, p. 1.701; ALBRECHT W.S., ALBRECHT C.O., ALBRECHT C.C., ZIMBELMAN M.F., *Fraud Examination*, Fourth edition, South-Western Cengage Learning, 2011, p. 516; *«Bribery involves the offering, giving, receiving, or soliciting of anything of value to influence an official act. The term "official act" means that traditional bribery statutes only proscribe payments made to influence the decisions of government agents or employees».*

[90] È interessante notare come questo tipo di corruzione non sia considerata reato in tutti gli stati. Gli Stati Uniti costituiscono un importante punto di riferimento in tal senso poiché manca una legge federale che vieri la corruzione commerciale in tutti i casi previsti. Cfr. ASSOCIATION OF CERTIFIED FRAUD EXAMINERS, *Fraud Examiners Manual*, 2011, p. 1.701; *«Commercial bribery may or may not be a criminal offense. For example, in the United States there is no general federal law prohibiting commercial bribery in all instances. However, there are statutes prohibiting bribery of employees of financial institutions to influence a loan. Therefore, the law of your particular jurisdiction and the facts of the case will determine whether bribery in the private sector may be prosecuted criminally. Commercial bribery can often be pursued in the civil courts as breach of fiduciary duty or conflict of interest».*

Esempi tipici di questo tipo di frode sono le tangenti pagate dai fornitori ai manager per potersi assicurare la conclusione di uno specifico contratto o i pagamenti ricevuti dai dipendenti dell'azienda per scopi similari[91].

È possibile affermare che si tratti di una vera e propria transazione commerciale illegale e che la tangente sia impiegata per "comprare l'influenza del destinatario" e quindi ottenere che operi illegalmente per consentirgli di ottenere un vantaggio[92].

L'ACFE individua due ragioni fondamentali che determinano il verificarsi di un fenomeno di corruzione con corresponsione di una tangente: la presenza di un'operazione a cui l'organizzazione economica non è interessata o il rifiuto di concludere un'operazione nell'interesse dell'organizzazione in assenza della ricezione di una tangente. Nel primo caso la tangente rappresenta il mezzo che consente all'interessato di concludere una transazione o un accordo che in assenza di corruzione non sarebbe stato concluso da parte dell'organizzazione economica. Nel secondo caso, invece, sono i soggetti che operano in ambito aziendale a rifiutarsi di concludere l'operazione in assenza dell'ottenimento di una tangente, ciò anche in presenza di operazioni che sarebbero svolte nell'interesse dell'organizzazione e, quindi, a suo vantaggio[93].

Gli schemi che rientrano nella categoria della corruzione possono essere a loro volta suddivisi in altre due categorie:

1. *Kickbacks*: tangenti pagate ai dipendenti di un'organizzazione economica dai fornitori al fine di ottenere un maggior fatturato o ampliare il business con l'azienda vittima della frode.
2. *Bid-rigging schemes*: l'azione illecita è commessa dal dipendente dell'azienda per favorire un particolare fornitore nel processo di valutazione delle offerte.

L'ACFE spiega che gli schemi di *Kickbacks* sono molto simili agli schemi di fatturazione previsti nell'ipotesi di appropriazione indebita di beni aziendali, ma che rientrano nella categoria della corruzione in quanto possono essere attuati solo in presenza di accordi tra fornitore e dipendenti, quindi in presenza di collusione tra due soggetti collegati all'organizzazione economica che ne è vittima.

---

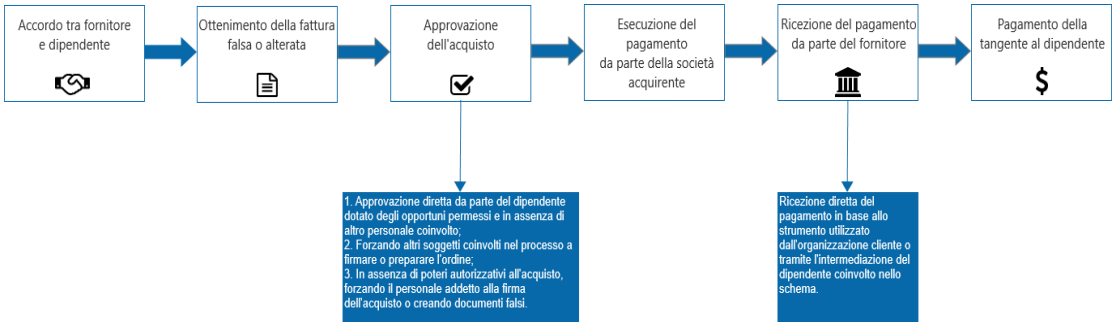
[91] ALBRECHT W.S., ALBRECHT C.O., ALBRECHT C.C., ZIMBELMAN M.F., *Fraud Examination*, Fourth edition, South-Western Cengage Learning, 2011, p. 516.

[92] ASSOCIATION OF CERTIFIED FRAUD EXAMINERS*, Fraud Examiners Manual*, 2011, p. 1.701; *«At its heart, a bribe is a business transaction, albeit an illegal or unethical one. A person "buys" something with the bribes he pays. What he buys is the influence of the recipient».*

[93] ASSOCIATION OF CERTIFIED FRAUD EXAMINERS, *Fraud Examiners Manual*, 2011, p. 1.701*; «This may be the convention of the industry/country in which he is operating and accepted by the person offering the bribe not as immoral but as a necessary expense and in the interests of his own organisation»*

Le operazioni di *Kickbacks* coinvolgono quasi sempre dipendenti che svolgono mansioni nei processi legati al ciclo acquisti della società, in quanto presuppongono l'emissione di fatture fittizie o con prezzi "gonfiati". Il grafico seguente sintetizza e semplifica i principali step di cui si compone un tipico schema di *Kickbacks* così come illustrato nel relativo grafico presente nel *Fraud Examiners Manual* dell'ACFE.

Figura 16 - Schema di sintesi Kickbacks



Fonte: Ns. elaborazione schema Kickbacks ASSOCIATION OF CERTIFIED FRAUD EXAMINERS, Fraud Examiners Manual, 2011, p. 1.703

Una delle fasi principali dello schema è rappresentato dall'approvazione dell'acquisto in quanto è possibile sia che il dipendente corrotto abbia i poteri per autorizzarlo, sia che non possieda tali poteri. Nel caso in cui il dipendente non svolga un ruolo che gli consenta di approvare gli acquisti dell'azienda, egli dovrà agire in modo da forzare tale fase del processo per ottenere l'autorizzazione da parte del personale addetto o procurando falsa documentazione che corrisponda alla fattura falsa o alterata. Nell'ipotesi in cui, invece, il dipendente sia in possesso di adeguati poteri autorizzativi potrà procedere all'approvazione dell'acquisto in modo del tutto autonomo oppure, in presenza di altro personale addetto alla preparazione degli ordini di acquisto, inducendo o forzando i subordinati all'esecuzione.

Considerando le caratteristiche specifiche di questo schema di frode, lo strumento più utile per poterle individuare è costituito dalla *data analysis* e dall'utilizzo di sistemi di analisi e software in grado di valutare la correttezza e la coerenza di prezzi e quantità mettendo in luce eventuali irregolarità o volumi di acquisti dal medesimo fornitore che si discostano dalla soglia considerata normale[94]. Possibili *red flags* sono costituiti, in tale ipotesi, da prezzi delle materie prime molto più alti del normale o da un elevato volume di acquisti nei confronti di uno o più fornitori[95].

[94] COENEN T.L., *Expert Fraud Investigation. A step by step guide*, John Wiley & Sons, Inc, 2009, p. 154.
[95] COENEN T.L., *Expert Fraud Investigation. A step by step guide*, John Wiley & Sons, Inc, 2009, p. 154; *«The quality of raw materials or merchandise should be monitored closely. It is not uncommon for a supplier to*

I *Bid-rigging schemes* sono, invece, schemi in cui il pagamento della tangente risulta finalizzato a influenzare il normale processo di selezione dei fornitori. *«In the competitive bidding process, all bidders are legally supposed to be placed on the same plane of equality, bidding on the same terms and conditions. Each bidder competes for a contract based on the specifications set forth by the purchasing company. Vendors submit confidential bids stating the price at which they will complete a project in accordance with the purchaser's specifications*[96]*».*

Attuando questo schema il fornitore ha la possibilità di ottenere da un dipendente informazioni riservate che gli consentano di vincere il processo di selezione o ottenere l'assegnazione del contratto mediante una selezione solo apparentemente reale[97].

Per poter individuare questa seconda tipologia di corruzione è importante analizzare l'eventuale presenza di contratti particolarmente onerosi o con un numero di offerenti basso e verificare, in presenza di un fornitore che abbia vinto più selezioni, se le sue offerte siano state presentate all'ultimo minuto o presentino delle differenze e margini molto ridotti, in quanto è probabile che abbia ottenuto informazioni dall'interno[98].

1.3.3 Appropriazione indebita di beni aziendali

L'*Asset misappropriation* o appropriazione indebita di beni aziendali è un tipo di frode attuata tramite la sottrazione o l'utilizzo improprio di beni di proprietà dell'organizzazione economica. *«Gli schemi di asset misappropriation si caratterizzano per la presenza di un soggetto che sottrae o utilizza impropriamente le risorse dell'azienda a proprio beneficio sfruttando le vulnerabilità*

---

substitute inferior goods in order to make a greater profit from the transactions. The supplier has a lower cost for the inferior goods, but is charging the price of the higher-quality goods to the customer. There is an instant profit, and this is one type of fraud involved in kickback schemes. If quality issues are discovered, look into the potential for a corruption scheme».

[96] ASSOCIATION OF CERTIFIED FRAUD EXAMINERS, *Fraud Examiners Manual*, 2011, p. 1.707.

[97] COENEN T.L., *Expert Fraud Investigation. A step by step guide*, John Wiley & Sons, Inc, 2009, p. 154; *«Bid-rigging is a type of bribery scheme in which a vendor is given some sort of advantage in what is supposed to be a competitive bidding process. One vendor may be given insider information to help win the bid, or a vendor may have already been secretly selected, with a phony bidding process set up to ensure that this vendor "wins" the bid. An employee may also rig the process of bidding for a contract by crafting the specifications for bids so narrowly that only one vendor will "qualify" to bid».*

[98] COENEN T.L., *Expert Fraud Investigation. A step by step guide*, John Wiley & Sons, Inc, 2009, p. 154; *«Bid-rigging can be detected by recognizing an unusually high contract price. If there are a low number of bidders in conjunction with this, suspicion should be even higher. Look for unusual bidding patterns or an apparent collusion, based on the similarity of information in the bids. A vendor with a track record of winning contracts with bids submitted at the last minute and by very slim margins might indicate that an employee is supplying that vendor with information about the other submitted bids».*

presenti nei processi aziendali e occultando il proprio intento fraudolento con il ricorso a pratiche mistificatorie[99]*».*

Questa categoria di frode è quella che presenta un tasso di frequenza nettamente superiore alle altre in quanto può essere perpetrata da qualsiasi soggetto coinvolto nei processi aziendali, inoltre presenta una casistica molto ampia in quanto può avere ad oggetto sia l'ottenimento di disponibilità monetarie sia di altri beni. Proprio sulla base di questa considerazione, la prima importante suddivisione tra gli schemi di *asset misappropriation* deve essere effettuata tra i due sottoinsiemi seguenti:

- *Cash misappropriation*;
- *No cash misappropriation*.

La prima categoria è sicuramente quella che si presenta con maggiore frequenza, soprattutto perché risulta molto più semplice appropriarsi di denaro invece che di altri beni e anche perché è più semplice il successivo utilizzo delle disponibilità monetarie[100].

Le appropriazioni aventi ad oggetto denaro possono essere, a loro volta, suddivise nelle seguenti categorie:

1. *Theft of Cash on Hand*;
2. *Theft of Cash Receipts*;
3. *Fraudulent Disbursements*.

Il primo sottoinsieme si riferisce a tutte le appropriazioni indebite che comportano la sottrazione di denaro "*on hand*", quindi mediante un vero e proprio furto delle disponibilità monetarie aziendali. La definizione dell'ACFE è la seguente: *«A scheme in which the perpetrator misappropriates cash kept on hand at the victim organization's premises (e.g., employee steals cash from a company vault)*[101]*».*

L'esempio riportato nella definizione, facendo riferimento al furto di denaro dal *caveau* aziendale, è particolarmente esplicativo per poter identificare correttamente tutti gli episodi di frode che rientrano in questa categoria.

---

[99] POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 72.

[100] POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 72; gli autori sottolineano che è molto più semplice appropriarsi di denaro invece che di altri beni in quanto vi sono minori problemi legati ad occultabilità e ingombro e minori interventi successivi per trasformare il bene in denaro, legati, ad esempio alla ricerca di un ricettatore o a un mercato di sbocco del bene.

[101] ACFE, *Report to the Nations. 2020 Global Study on occupational fraud and abuse*, p. 86.

Il secondo sottoinsieme del *Theft of Cash Receipts* si riferisce, invece, alla sottrazione di denaro che avviene nell'ambito della gestione degli incassi. Per analizzare questa tipologia di *asset misappropriation* è fondamentale considerare che nella stessa rientrano i seguenti schemi:

- *Skimming*;
- *Cash Larceny*.

Nel primo caso, le disponibilità monetarie sono sottratte all'azienda prima che sia effettuata la relativa rilevazione contabile, mentre nel secondo il denaro è sottratto in seguito alla registrazione in contabilità[102]. La seconda tipologia è, ovviamente, molto più semplice da rilevare per il sistema di controllo interno dell'organizzazione economica, questa è la ragione per cui risulta essere molto meno diffusa rispetto agli schemi di *Skimming*. Uno dei metodi maggiormente utilizzati per poter occultare il *cash larceny* è l'attuazione del *Kiting* che sfrutta il trasferimento del denaro tramite giroconto tra diversi conti correnti bancari. Per poter nascondere la sottrazione di denaro sarà necessario effettuare trasferimenti con importi non corrispondenti e con la contestuale alterazione della rilevazione in contabilità. Generalmente il *kiting* è effettuato in corrispondenza della chiusura dell'esercizio, sfruttando i tempi tecnici bancari di rilevazione delle operazioni[103].

Gli schemi di *skimming* sono, invece, molto più frequenti in quanto non correlati ad alcuna registrazione contabile: ciò rende più difficile poter individuare questa tipologia di frode e, allo stesso tempo, richiede minori attività per dissimulare l'azione. Questa tecnica è utilizzata da dipendenti che svolgono funzioni connesse al ciclo attivo aziendale e può riguardare le vendite, i crediti, i rimborsi o altre operazioni.

Lo *skimming* delle vendite presuppone che sia effettuata una vendita diretta ai clienti e la possibilità di incassare somme di denaro che non saranno successivamente rilevate in contabilità o saranno rilevate solo in modo parziale: si parla, rispettivamente, di *skimming* delle vendite non registrate e di *skimming* delle vendite sottovalutate[104].

---

[102] ASSOCIATION OF CERTIFIED FRAUD EXAMINERS, *Fraud Examiners Manual*, 2011, p. 4.524.

[103] POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 73; *«In particolare, l'ammanco è dissimulato nel modo seguente: immediatamente prima della chiusura dell'esercizio il frodatore emette un assegno a valere sul c/c presso un istituto di credito; l'accadimento è registrato in contabilità nell'esercizio successivo e – per effetto dei tempi tecnici bancari – l'estratto conto al 31.12 della banca non riporterà alcuna movimentazione di denaro; consapevole di ciò l'individuo potrà depositare l'assegno in parola su altro conto corrente aziendale intrattenuto con la medesima banca o altra banca; questa volta egli procede alla corretta registrazione del versamento entro la data di fine esercizio».*

[104] Crf. ACFE, *Report to the Nations. 2020 Global Study on occupational fraud and abuse*, p. 11; POGLIANI G., PECCHIARI N., MARIANI M., Frodi aziendali. Forensic accounting, fraud auditing e litigation, Egea, 2012, p. 76.

Nel primo caso il frodatore sottrae l'intero incasso della vendita diretta eseguita nei confronti del cliente. Ciò che rende più complesso gestire questa tipologia di frode è l'adozione di comportamenti che non insospettiscano il cliente stesso o siano rilevati da colleghi o dal sistema di controllo interno aziendale, ad esempio tramite telecamere poste nei luoghi aperti al pubblico[105].

«The most difficult part in skimming at the register is that the employee must commit the overt act of taking money. If the employee takes the customer's money and shoves it into his pocket without entering the transaction on the register, the customer will probably suspect that something is wrong and might report the conduct to another employee or a manager. It is also possible that a manager, a fellow employee, or a surveillance camera will spot the illegal conduct. Therefore, it is often desirable for a perpetrator to act as though he is properly recording a transaction while he skims sales[106]».

Per poter simulare l'esecuzione della corretta operazione di incasso il frodatore potrebbe manomettere il registratore di cassa, eseguire la transazione fuori dal normale orario di lavoro o emettere una ricevuta falsa[107]. La manipolazione del registratore di cassa può consentire al dipendente di simulare l'inserimento di una transazione o registrare una transazione diversa dalla vendita in modo che non risulti nella distinta di cassa e non vi siano differenze tra il dato registrato e la consistenza effettiva di cassa[108]. In molti casi queste attività di occultamento si traducono nella presenza di una distinta di cassa con degli spazi in bianco o con salti di numerazione: l'attenta valutazione di questi indizi può condurre il sistema di controllo interno aziendale a individuare chiari segnali di questa tipologia di frode[109].

Le transazioni eseguite al di fuori dell'orario di lavoro sono utilizzate, invece, soprattutto nei casi in cui il dipendente sia dotato di ampia autonomia organizzativa in relazione alla gestione delle vendite e degli orari di apertura al pubblico. In questo caso, infatti, il dipendente deve avere

---

[105] Cfr. POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 76.

[106] ASSOCIATION OF CERTIFIED FRAUD EXAMINERS, *Fraud Examiners Manual*, 2011, p. 1.404.

[107] POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 76; *«Pertanto l'azione può essere compiuta sfruttando situazioni particolari, anche artificiosamente generate dalla creatività dell'attore: fra le diverse tecniche si possono annoverare la manomissione dei registratori di cassa, l'effettuazione di vendite al di fuori dell'orario lavorativo oppure la mancata emissione di regolare ricevuta sostituita da un documento alternativo».*

[108] Cfr. ASSOCIATION OF CERTIFIED FRAUD EXAMINERS, *Fraud Examiners Manual*, 2011, p. 1.404.

[109] Cfr. ASSOCIATION OF CERTIFIED FRAUD EXAMINERS, *Fraud Examiners Manual*, 2011, p. 1.404; il manuale mette in evidenza come gli spazi bianchi presenti tra le transazioni possano essere eliminati tramite la successiva sostituzione del nastro all'interno del registratore di cassa, mentre risulta più complessa l'ipotesi dell'interruzione della sequenza numerica dovuta a salti e omissioni tra le transazioni registrate.

l'opportunità di effettuare vendite al pubblico in orari differenti da quelli previsti e senza l'autorizzazione del management o della proprietà[110].

L'esempio da manuale proposto dall'ACFE è il seguente[111]:

«A manager of a retail facility went to work two hours early every day, opening his store at 8:00 a.m. instead of 10:00 a.m., and pocketed all the sales made during these two hours. He rang up sales on the register as if it was business as usual, but then removed the register tape and all the cash he had accumulated. The manager then started from scratch at 10:00 as if the store was just opening. The tape was destroyed so there was no record of the beforehours revenue»

Per poter implementare questa tipologia di frode è necessario che sussistano gravi carenze nel sistema di controllo interno o che il dipendente lavori presso una *branch* o una sede distaccata che non sia sottoposta ad una supervisione diretta[112].

Il problema più importante che si presenta nell'implementazione di questa tipologia di frode risulta essere lo squilibrio tra la quantità di merce fisicamente presente in magazzino e la quantità risultante dalla contabilità aziendale. Per effetto delle vendite eseguite, infatti, la quantità di beni in magazzino sarà inferiore alla quantità contabilizzata: questa anomalia è facilmente individuabile mediante i più semplici controlli aziendali di confronto tra le quantità o di programmazione ed esecuzione dei nuovi ordini di acquisto dei beni oggetto della frode[113]. Pogliani (et al.) mette in evidenza che l'individuazione di una simile discrasia comporterà l'innalzamento del livello di attenzione e di controllo, riducendo le possibilità di reiterare questo tipo di frode a meno che non si implementi una strategia fondata sull'esecuzione di molteplici azioni ma di impatto minimo e con diversificazione delle fonti e dei beni che ne sono oggetto come nel caso della *Salami Technique*: *«Questa tecnica (…) non si pone l'obiettivo di eliminare discrasie o anomalie derivanti dall'azione fraudolenta, quanto piuttosto di contenere la loro*

---

[110] Cfr. ASSOCIATION OF CERTIFIED FRAUD EXAMINERS, *Fraud Examiners Manual*, 2011, p. 1.404; POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 77.

[111] ASSOCIATION OF CERTIFIED FRAUD EXAMINERS, *Fraud Examiners Manual*, 2011, p. 1.404.

[112] ASSOCIATION OF CERTIFIED FRAUD EXAMINERS, *Fraud Examiners Manual*, 2011, p. 1.404; *«Some of the most costly skimming schemes are perpetrated by employees who work at remote locations or without close supervision. This can include on-site sales persons who do not deal with registers, independent salesmen who operate off-site, and employees who work at branches or satellite offices. These employees have a high level of autonomy in their jobs, which often translates into poor supervision and, in turn, to fraud».*

[113] POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation,* Egea, 2012, p. 78; *«Il frodatore è conscio che il più evidente punto di debolezza di uno schema di skimming, ove le cessioni di beni non sono registrate, è la presenza di un ammanco di magazzino, cioè l'ovvio squilibrio che si verifica tra quantità fisiche in giacenza e quantità contabilizzate»*; gli autori mettono in evidenza che anche i sistemi di controllo aziendale meno sofisticati e affidabili effettuino un simile confronto di controllo tra le quantità, risulta quindi molto facile individuare tale tipo di anomalia.

ampiezza (in termini di frequenza e di valore) entro una soglia tale da non suscitare particolari allarmi in coloro che li dovessero rilevare»[114].

A differenza dello *skimming* delle vendite non registrate, lo *skimming* delle vendite sottovalutate presuppone l'esecuzione di una rilevazione ma per un importo inferiore rispetto a quello effettivo. Non vi è, quindi, una vera e propria omissione della rilevazione contabile, di conseguenza vengono meno le problematiche affrontate nel precedente schema relative agli ammanchi di magazzino, ma la registrazione di un importo più basso: proprio la differenza tra il valore che si riesce ad ottenere dal cliente e il valore rilevato costituisce l'ammontare dell'appropriazione indebita. Una delle modalità più frequenti con cui è possibile attuare lo schema presentato è l'applicazione di uno sconto fittizio, rilevato in contabilità ma non praticato realmente nei confronti del cliente.

Lo *skimming* dei crediti è un ulteriore schema fraudolento eseguito nella fase di incasso dei crediti maturati nei confronti della clientela, quindi dopo che la rilevazione contabile sia già avvenuta. In questo caso si può far riferimento a tre varianti di frode:

- *Write-off Schemes*;
- *Lapping Schemes*;
- *Unconcealed*.

Tra questi schemi quello utilizzato più di frequente è il *Lapping* che viene eseguito dal frodatore utilizzando gli incassi pervenuti da altri clienti. Più nel dettaglio, l'ammontare sottratto a un cliente viene occultato contabilmente tramite l'accreditamento di somme versate da un successivo cliente: ovviamente questo schema richiede che il meccanismo di occultamento sia reiterato sui successivi conti coinvolti[115].

Il terzo e ultimo sottoinsieme con cui si completa il *Cash misappropriation* è costituito dal *Fraudulent Disbursements* che, a differenza degli schemi di *Skimming* coinvolge le attività correlate al ciclo acquisti. In particolare, gli schemi in oggetto, nascono con l'obiettivo di indurre l'azienda al pagamento di somme di denaro che saranno illecitamente acquisite dal frodatore[116].

---

[114] POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 79.

[115] ASSOCIATION OF CERTIFIED FRAUD EXAMINERS, Fraud Examiners Manual, 2011, p. 1.414.

[116] POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 81; *«Se, dunque, nei casi precedenti lo schema fraudolento agiva cercando di "intercettare" il flusso di denaro in entrata nelle disponibilità aziendali, in questi casi agisce allo scopo di promuovere o "stimolare" il flusso in uscita di risorse».*

Di seguito una panoramica delle molteplici tipologie di *Fraudulent Disbursements*[117]*:*

- *Billing Schemes*: gli schemi di questa tipologia nascono con l'obiettivo di indurre l'azienda al pagamento di fatture false o con prezzi gonfiati o fatture personali del frodatore.
- *Payroll Schemes*: si riferiscono a frodi che coinvolgono il ciclo lavoro e la corresponsione delle retribuzioni allo scopo di indurre l'azienda al pagamento di retribuzioni o risarcimenti falsi.
- *Expense Reimbursement Schemes*: schemi basati su richieste di rimborso dei dipendenti del tutto fittizie o con spese superiori rispetto a quelle effettivamente sostenute.
- *Check and Payment Tampering*: questa tipologia di frode viene perpetrata mediante l'emissione, l'alterazione o il furto di assegni bancari emessi dall'organizzazione economica.
- *Register Disbursements*: falsificazione delle operazioni mediante inserimento di transazioni a copertura di furti di denaro.

La seconda categoria di *Asset Misappropriation* è costituita dalle appropriazioni indebite che hanno ad oggetto non denaro ma altri beni aziendali: si tratta delle appropriazioni relative a "*Inventory and All Other Assets*". L'appropriazione indebita può essere correlata all'effettivo furto del bene oppure al suo utilizzo improprio. Tali due aspetti sono alla base della differenza presente tra *Misuse* e *Larceny*.

Si parla di *Misuse* quando il dipendente aziendale non si appropria completamente del bene ma lo utilizza per scopi e attività personali incrementando il livello dei costi sostenuti dall'azienda. *«Assets that are misused but not stolen typically include company vehicles, company supplies, computers, securities, information, and office equipment. These assets are also used by some employees to conduct personal work on company time»*[118]*.*

Di portata e gravità di gran lunga superiore sono, invece, i danni che potenzialmente possono essere provocati dal vero e proprio furto di beni aziendali, in particolare se si tratta di beni di elevato valore sottratti dai magazzini aziendali. A questa categoria di frode si riferisce, inoltre, il

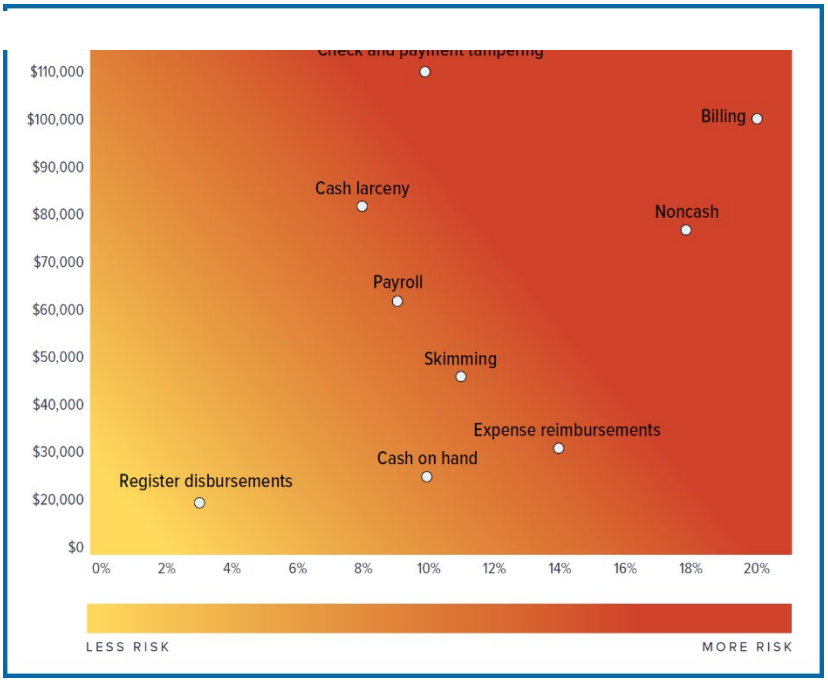
[117] La schematizzazione delle tipologie di Fraudulent Disbursements deriva dalla tabella esemplificativa proposta in ALBRECHT W.S., ALBRECHT C.O., ALBRECHT C.C., ZIMBELMAN M.F., *Fraud Examination*, Fourth edition, South-Western Cengage Learning, 2011, p. 509.

[118] ALBRECHT W.S., ALBRECHT C.O., ALBRECHT C.C., ZIMBELMAN M.F., Fraud Examination, Fourth edition, South-Western Cengage Learning, 2011, p. 514.

furto di informazioni relative ai beni intangibili quali brevetti, strategie di marketing, marchi, brevetti e informazioni commerciali e industriali[119].

Il *Report to the Nations* dell'ACFE riporta l'analisi della frequenza e delle perdite medie provocate da ciascuna tipologia di *Asset Misappropriation Fraud* evidenziando il livello di rischio per ognuna e rappresentando i risultati mediante la seguente *heat map*.

Figura 17 - Heat Map



Fonte: ACFE, Report to the Nations. 2020 Global Study on occupational fraud and abuse, p.13

Lo schema che presenta maggiori rischi e contestualmente una maggiore frequenza e perdite più elevate è il *Billing*, seguito dal *Check and payment tampering*, che a fronte di una minore frequenza presenta perdite medie molto elevate, e dagli schemi *Non-cash*, al secondo posto in termini di frequenza.

L'ISA Italia 240, trattando delle responsabilità del revisore relativamente alle frodi nella revisione contabile del bilancio, individua due differenti categorie di frode:

- Politiche di falsificazione dei bilanci;
- Appropriazione illecita di beni e attività dell'impresa.

Con riferimento all'appropriazione illecita di beni e attività dell'impresa, il principio di revisione, sottolinea che spesso queste azioni sono implementate dai dipendenti aziendali, normalmente

[119] POGLIANI G., PECCHIARI N., MARIANI M., Frodi aziendali. Forensic accounting, fraud auditing e litigation, Egea, 2012, p. 94.

per beni di esiguo valore, ma che, soprattutto nel caso in cui sia coinvolta la direzione aziendale, questa tipologia di frode può dar vita a perdite significative. Tale effetto deriva dalle maggiori possibilità che la direzione ha di commettere tale illecito in riferimento a beni e attività di valore superiore in virtù delle più ampie possibilità di occultare o dissimulare le appropriazioni illecite.
Le modalità di realizzazione di questa tipologia di frode elencate dall'ISA Italia 240 sono le seguenti:

- la distrazione di incassi (per esempio, appropriandosi di incassi di crediti verso clienti o dirottando su conti personali incassi a fronte di crediti già stralciati);
- il furto di beni materiali o di proprietà intellettuali (per esempio sottraendo merci di magazzino per uso personale o per rivenderle, appropriandosi di scarti di produzione per rivenderli, accordandosi con un concorrente per rivelare informazioni tecnologiche dietro pagamento);
- pagamenti da parte dell'impresa per beni e servizi non ricevuti (per esempio pagamenti a fornitori inesistenti, tangenti pagate dai fornitori ai responsabili degli acquisti in cambio di prezzi gonfiati, pagamenti a dipendenti inesistenti);
- l'utilizzo dei beni e delle attività dell'impresa per finalità personali (per esempio come garanzia di un prestito personale o di un prestito ad una parte correlata).

L'appropriazione indebita è normalmente effettuata da soggetti interni all'azienda, ma non è escluso che anche persone esterne possano dar vita a questo tipo di frode. Quando l'illecito è occultato all'organo di governo aziendale e alla funzione amministrativa, non si avranno riflessi anche sulle scritture contabili, di conseguenza la consistenza reale dei beni e delle attività risulterà essere diversa da quanto riportato nell'informativa economico-finanziaria: ad esempio possono aversi rimanenze inventariate e valutate in misura superiore a quella reale o può verificarsi l'ipotesi di un mancato storno degli altri beni aziendali e delle relative sopravvenienze passive[120].

1.3.4 Politiche di falsificazione dei bilanci

Per *Financial Statement Fraud* si intende «*A scheme in which an employee intentionally causes a misstatement or omission of material information in the organization's financial reports (e.g.,*

[120] D'ALESSIO R., ANTONELLI V., BOZZA E., *Principi di Auditing. Concetti, modelli, metodologie, applicazioni*, Volume I, Edises, 2017, p. 266.

recording fictitious revenues, understating reported expenses, or artificially inflating reported assets)[121]*».*

Lo schema di frode presuppone l'alterazione dell'informativa finanziaria mediante la presentazione di una situazione patrimoniale o reddituale diversa da quella effettiva e contenente informazioni non corrette da destinare agli utilizzatori del bilancio d'esercizio[122]. Questa tipologia di frode è implementata prevalentemente dai soggetti che sono posti al vertice dell'organizzazione economica in quanto presuppone che vi sia una diretta partecipazione nelle attività relative alla contabilità e alla preparazione dell'informativa finanziaria.

L'alterazione dei bilanci può essere finalizzata sia a sopravvalutare uno o più elementi patrimoniali o reddituali sia a sottostimare gli stessi, per questa ragione la categoria risulta essere suddivisa in due tipologie di frode:

- *Net Worth/Net Income Overstatements*;
- *Net Worth/Net Income Understatements*.

Tra le due, la tipologia che si verifica con più frequenza è quella di sopravvalutazione delle poste di bilancio e, in particolare dell'ammontare dei ricavi conseguiti nell'esercizio che molto spesso risultano essere completamente inventati e rilevati in contabilità per ottenere un dato dei ricavi migliore di quello effettivo[123].

L'albero delle frodi prevede cinque sottocategorie per ognuna delle due tipologie di frodi previste:

1. <u>*Net Worth/Net Income Overstatements*</u>:

- *Timing differences*;
- *Fictitious Revenues*;
- *Concealed Liabilities and Expenses*;
- *Improper Asset Valuations*;
- *Improper Disclosures.*

2. <u>*Net Worth/Net Income Understatements*</u>:

- *Timing differences*;

[121] ACFE, *Report to the Nations. 2020 Global Study on occupational fraud and abuse*, p. 11.

[122] POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 95; gli autori sottolineano la presenza dell'elemento della premeditazione nell'alterazione dei bilanci finalizzata a condizionare i giudizi e le decisioni degli utilizzatori, in particolar modo di finanziatori, creditori e investitori.

[123] SINGLETON T., SINGLETON A., *Fraud Auditing and Forensic Accounting*, Four Edition, John Wiley & Sons, Inc, 2010, p. 80.

- *Understated Revenues*;
- *Overstated Liabilities and Expenses*;
- *Improper Asset Valuations*;
- *Improper Disclosures*.

La tabella sottostante riassume le principali caratteristiche degli schemi di frode di questa categoria che si presentano con maggiore frequenza[124].

SINTESI DEI PRINCIPALI SCHEMI DI FRODE	
Timing differences	La frode è implementata per creare delle differenze temporanee e sovrastimare o sottostimare i valori di bilancio per l'anno corrente. Tra i metodi più comunemente impiegati rientra l'invio e la fatturazione di una quantità superiore di merce ai clienti che porta ad innalzare il fatturato nel periodo corrente e alla successiva restituzione della merce in eccesso nel/nei periodo/i successivo/i. In questo schema di frode rientrano anche le violazioni dei principi contabili che determinano forzature sulla competenza dei ricavi e la loro intenzionale errata rilevazione nel periodo corrente senza tener conto della correlazione con i relativi costi.
Fictitious Revenues	Gli schemi di questa categoria sono finalizzati a rilevare in contabilità ricavi fittizi per transazioni totalmente o parzialmente inventate dal frodatore. Nel primo caso l'operazione di cessione è completamente falsa e può riferirsi sia a clienti inventati sia a reali clienti della società. Nel secondo caso la frode si fonda sull'alterazione delle vendite effettivamente eseguite nei confronti di uno o più clienti. Le frodi così implementate necessitano della preparazione della documentazione fittizia posta a supporto delle transazioni e del successivo occultamento del credito rilevato in contabilità che non sarà mai compensato da entrate monetarie.
Concealed Liabilities and Expenses	In questo caso il frodatore agisce sottovalutando costi e passività. I casi più frequenti con cui viene implementata questa tipologia di frode sono i seguenti: - Differimento della rilevazione di fatture ricevute all'esercizio successivo.

[124] Il contenuto della tabella di sintesi è stato elaborato sulla base delle informazioni ottenute dalle seguenti fonti: SINGLETON T., SINGLETON A., *Fraud Auditing and Forensic Accounting*, Four Edition, John Wiley & Sons, Inc, 2010, p. 80 e ss; POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 98 e ss.

	- In presenza di società controllate, trasferimento del costo su una di queste società. - Sottostima dei fondi rischi mediante pratiche di *Cookie jars.* - Capitalizzazione di costi di intera competenza di un esercizio al fine di aumentare l'attivo patrimoniale e ripartire il costo in più esercizi.
Improper Asset Valuations	Valutazione fraudolenta delle attività di bilancio mediante applicazione dei criteri di stima e valutazione previsti dai principi contabili in modo tale da alterare i dati di bilancio e l'informativa economico-finanziaria.
Improper Disclosures	Gli schemi di questa categoria fanno riferimento alla falsa informativa di bilancio relativa agli aspetti qualitativi dell'informativa economica. In questo caso, l'alterazione non si riferisce ai dati quantitativi ma alle informazioni necessarie a specificare i dati di bilancio e a commentarli. Le più comuni frodi di questa categoria si riferiscono alle passività potenziali e ai rischi futuri, agli eventi successivi, alle parti correlate e all'entità delle operazioni svolte, ma la casistica risulta essere molto ampia.

Fonte: Ns elaborazione SINGLETON T., SINGLETON A., Fraud Auditing and Forensic Accounting, Four Edition, John Wiley & Sons, Inc, 2010, p. 80 e ss; POGLIANI G., PECCHIARI N., MARIANI M., Frodi aziendali. Forensic accounting, fraud auditing e litigation, Egea, 2012, p. 98 e ss.

Considerando quanto disposto dall'ISA Italia 240, la prima categoria di frode contemplata dal principio di revisione è proprio costituita dalle politiche di falsificazione dei bilanci. L'ISA Italia 240 fa riferimento alla falsa informativa finanziaria che deriva dalle azioni di manipolazione ordite dall'organo di governo aziendale il quale, in base alle caratteristiche e alle condizioni dell'azienda o alle circostanze ambientali, può avere l'obiettivo di espandere o di comprimere il reddito d'esercizio dell'azienda[125]. L'espansione del reddito d'esercizio e del collegato capitale di funzionamento è lo scopo maggiormente perseguito quando si pone in essere la tipologia di frode oggetto di esame: l'obiettivo, in questo caso, è rappresentare una situazione economica, finanziaria e patrimoniale migliore di quella effettiva. Meno rilevanza viene data dall'ISA Italia 240 al caso di compressione del reddito e del collegato capitale di funzionamento nonostante tale ipotesi si verifichi in modo frequente soprattutto se si guarda al contesto italiano. Questa seconda

[125] D'ALESSIO R., ANTONELLI V., BOZZA E., *Principi di Auditing. Concetti, modelli, metodologie, applicazioni*, Volume I, Edises, 2017, p. 266.

tipologia di falsa informativa finanziaria ha lo scopo di occultare la ricchezza prodotta dall'azienda e rappresentare una situazione economica, finanziaria e patrimoniale peggiore di quella reale[126]. L'ISA Italia 240, al paragrafo A.2 individua i seguenti scopi perseguiti tramite le politiche di falsificazione dei bilanci: *«La falsa informativa finanziaria include errori intenzionali, inclusa l'omissione in bilancio di importi o di adeguata informativa, al fine di trarre in inganno gli utilizzatori dello stesso. Essa può essere originata dalle iniziative della direzione volte a manipolare i risultati d'esercizio al fine di ingannare gli utilizzatori del bilancio, influenzando la loro percezione della performance e della redditività dell'impresa. Tale manipolazione dei risultati di esercizio può iniziare con azioni di modesto impatto o con l'indebita modifica delle assunzioni e delle valutazioni formulate dalla direzione. L'esistenza di pressioni ed incentivi può indurre ad ampliare la portata di tali azioni fino a produrre una falsa informativa finanziaria. Simili circostanze possono verificarsi quando la direzione, a causa di pressioni per il soddisfacimento delle aspettative del mercato o per il desiderio di massimizzare i compensi legati alla performance, assume intenzionalmente posizioni che conducono ad una falsa informativa finanziaria, alterando in modo significativo il bilancio. In alcune imprese, la direzione può essere indotta a ridurre i risultati di esercizio per un ammontare significativo al fine di minimizzare le imposte ovvero a gonfiarli per garantirsi i finanziamenti delle banche».*

Il principio di revisione prosegue al paragrafo A.3 individuando ed elencando i principali strumenti impiegati per implementare politiche di falsificazione dei bilanci:

- manipolazioni, falsificazioni (incluse le contraffazioni) o alterazioni delle registrazioni contabili, ovvero della relativa documentazione di supporto utilizzata nella redazione del bilancio;
- rappresentazioni fuorvianti o omissioni intenzionali in bilancio di fatti, operazioni o altre informazioni significative;
- applicazioni intenzionalmente errate dei principi contabili relativi agli importi, alle classificazioni delle voci, alle modalità di presentazione e all'informativa in bilancio.

Le politiche di falsificazione dei bilanci risultano essere particolarmente complesse da individuare in quanto spesso non sono eseguite da un unico soggetto ma implicano la collusione di più persone che operano all'interno dell'azienda. *«Le politiche di falsificazione dei bilanci non sono realizzate da un solo soggetto o da un sol organo, ma, di solito, coinvolgono più individui, più*

[126] D'ALESSIO R., ANTONELLI V., BOZZA E., *Principi di Auditing. Concetti, modelli, metodologie, applicazioni*, Volume I, Edises, 2017, p. 266; questa tipologia di frode è molto frequente nella realtà italiana, nasce prevalentemente con l'intenzione di evadere le imposte mediante l'occultamento della ricchezza creata dall'azienda o la costituzione di fondi neri mediante appostamento di costi fittizi.

organi, e, spesso, la stessa direzione generale dell'azienda, in un disegno comune e, di solito, "pensato a tavolino"[127]*».*

Le difficoltà di individuazione di questa tipologia di frode sono, quindi, correlate alla partecipazione di molteplici dipendenti aziendali e della stessa direzione e connesse alla frequente alterazione e forzatura delle procedure di controllo interno. Apparentemente le operazioni appaiono lecite poiché supportate da documentazione formalizzata ad hoc e/o alterata in modo da essere coerente con l'illecito commesso: tutti questi elementi rendono molto difficile riscontrare la presenza di frodi e manipolazioni di bilancio.

1.3.5 Riciclaggio di denaro

Il riciclaggio di denaro o *Money laundering* è il processo che consente di occultare l'origine illecita di una certa quantità di denaro, mediante attività che consentono di dissimularne la provenienza. L'ACFE stabilisce che *«Money laundering is a process which aims to disguise the existence, nature, source, control, beneficial ownership, location, and disposition of property derived from criminal activity. In this context property assumes the wider definition of that which is physical, intangible or represented in the form of rights or obligations such as a pension funds or trust fund*[128]*».*

Il denaro proveniente da attività illecita viene "riciclato" mediante attività e operazioni che consentono di conferire ad esso una provenienza lecita: il riciclaggio può essere considerato, in tal senso, come l'ultima fase di un atto illecito che genera profitti[129].

Il riciclaggio non può essere, quindi, considerato una frode, ma un'attività correlata ad essa, un crimine commesso per coprire altri crimini[130].

Il processo di *Money Laundering* può essere suddiviso in tre distinte fasi:

- *Placement;*
- *Layering;*
- *Integration*.

---

[127] D'ALESSIO R., ANTONELLI V., BOZZA E., *Principi di Auditing. Concetti, modelli, metodologie, applicazioni*, Volume I, Edises, 2017, p. 268.

[128] ASSOCIATION OF CERTIFIED FRAUD EXAMINERS, *Fraud Examiners Manual*, 2011, p. 2.501.

[129] POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 191.

[130] COENEN T.L., *Expert Fraud Investigation. A step by step guide*, John Wiley & Sons, Inc, 2009, p. 158; *«Money laundering is not a fraud scheme. It is a crime that is committed to cover up other crimes, but it is not the same thing as fraud».*

Il *Placement* è la fase in cui i fondi vengono collocati sul mercato e, quindi, convertiti in una forma più conveniente e più facile da utilizzare se ottenuti sottoforma di contanti[131]. In particolare, i fondi possono essere collocati presso intermediari finanziari (forma molto più frequente), impiegati nell'ambito di attività commerciali o utilizzati in modo diretto per l'acquisto di beni.

Il *Layering* è, invece, la fase in cui effettivamente sono poste in essere le attività che consentono l'occultamento dell'illecito. Si parla di "stratificazione" in quanto è necessario portare a termine molteplici operazioni per nascondere la fonte illecita del denaro: «*L'obiettivo finale del layering è rendere difficoltosa la ricostruzione investigativa del flusso, cioè impedire al financial investigator di ripercorrere la traccia documentale dei trasferimenti*[132]*».*

Per realizzare tali obiettivi sono eseguite numerose operazioni di trasferimento, prelievo e deposito tra molteplici conti correnti, operazioni di cambio valuta, acquisto di beni e investimenti.

L'ultima fase di *Integration* è, infine, quella che consente a chi ha prodotto illecitamente i profitti oggetto dell'operazione di riciclaggio, di ottenere nuovamente la disponibilità dei fondi. Al termine di questa fase i fondi risultano apparentemente leciti poiché "ripuliti" tramite reintegrazione in attività economiche (*justification*) o investimento in attività lecite in grado di generare profitti (*investment*).

Il fenomeno in esame è divenuto ancora più articolato e complesso a partire dalla fine degli anni '90 in poi a causa dell'importante evoluzione che hanno avuto le tecnologie informatiche impiegate in ambito bancario e finanziario. I servizi di home *banking* hanno, infatti, reso possibile impiegare nuovi strumenti per compiere tutte le operazioni di occultamento e di *layering* necessarie a riciclare i fondi illeciti, escludendo completamente il coinvolgimento di un intermediario finanziario. Le attività di riciclaggio condotte via internet sono collocate nella categoria del *cyberlaundering*, a sua volta distinto in "riciclaggio digitale strumentale" e "riciclaggio digitale integrale"[133].

Nel primo caso è sufficiente che una sola delle fasi del processo di riciclaggio sia svolta via internet, mentre nel secondo è l'intero processo ad essere realizzato online.

---

[131] SICIGNANO G.J., *Bitcoin e riciclaggio,* G Giappichelli Editore, 2019, p. 113.

[132] POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, pp. 200-201.

[133] SICIGNANO G.J., *Bitcoin e riciclaggio,* G Giappichelli Editore, 2019, p. 114; l'autore sottolinea che mentre in passato era necessario l'intervento di un intermediario istituzionale, oggi tutte le operazioni di riciclaggio possono essere realizzate sfruttando i canali via internet.

1.3.6 Cybercrime

Le nuove tecnologie e i computer, come brevemente accennato nella trattazione del riciclaggio e della sua evoluzione nel *cyberlaundering*, sono oggi utilizzati come strumenti per poter commettere crimini e frodi e, al contempo, hanno fornito le opportunità per dar vita a nuove tipologie di frode. Il *computer crime* si lega soprattutto agli *occupational crime* in quanto è più facile per un soggetto interno all'organizzazione economica avere accesso al sistema informativo aziendale per poter commettere un illecito.

I primi casi di *computer crime* sono stati registrati negli Stati Uniti dalla SRI (*Stanford Research International*) a partire dalla fine degli anni '60 e hanno subito una forte crescita nel decennio successivo ciò a causa sia dell'aumento dei casi rilevati, sia dell'incremento dell'utilizzo del computer da parte delle aziende e delle organizzazioni private.

La SRI, valutando i primi casi di criminalità informatica della fine degli anni '50, ha elaborato la seguente classificazione[134]:

- Vandalismo;
- Furto di informazioni e della proprietà intellettuale;
- Frode;
- Utilizzo non autorizzato o vendita di servizi informatici.

Oggi il *cybercrime* si colloca al secondo posto in termini di frequenza degli episodi di frode in base al *PwC's Global Economic Crime and Fraud Survey*, coinvolgendo la maggior parte dei settori economici di riferimento.

I principali strumenti impiegati per dar vita a frodi di questa tipologia, che occupa il 34% delle frodi totali, sono costituiti dalle email e dalle pagine web, ma, in termini generali, il *cybercrime* individua le *«attività criminose in cui computer, reti di computer o ogni altro dispositivo elettronico risultano coinvolti sia come strumenti che come obiettivi delle medesime[135]».*

Quando si parla di *computer crime* si fa riferimento alla teoria nota con l'acronimo di MOMM derivante dai termini *motivations*, *opportunities*, *means*, *methods*. *Motivazioni* e *opportunità* sono gli stessi elementi che caratterizzano il modello del triangolo delle frodi, mentre *strumenti* e *metodi* sono concetti che si legano in modo specifico a tale tipologia di frode. Gli strumenti si riferiscono alle opportunità, ai sistemi di controllo interno e all'uso delle nuove tecnologie per

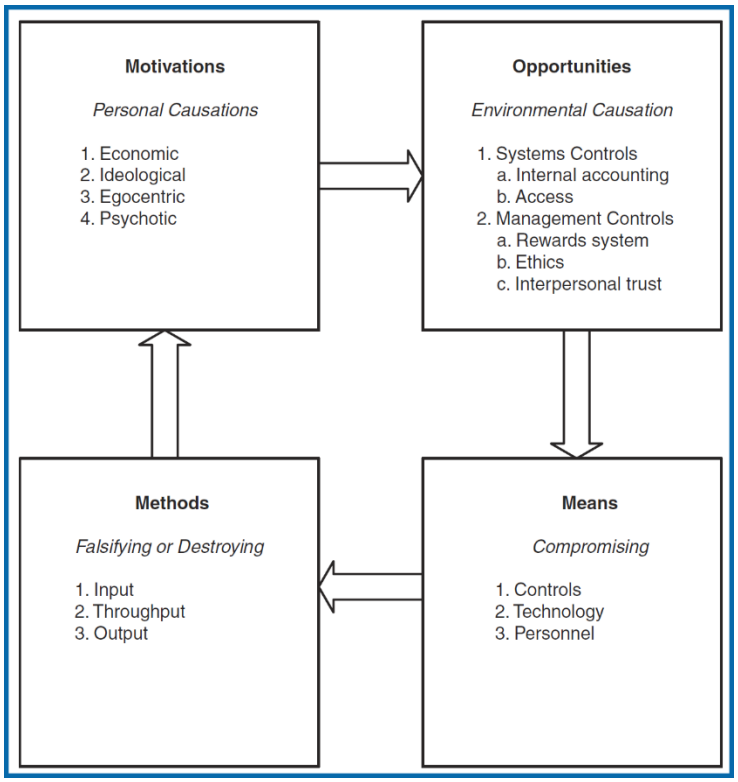
[134] Cfr. SINGLETON T., SINGLETON A., *Fraud Auditing and Forensic Accounting*, Four Edition, John Wiley & Sons, Inc, 2010, p. 176.

[135] POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 121.

l'implementazione di attività fraudolente, mentre i metodi agli schemi e alle tecniche di frode applicate ai *computer crime*. La teoria applicata alle frodi informatiche, quindi, è in parte aderente alla teoria generale relativa alle frodi e per altra parte specifica, in quanto fa riferimento a concetti prettamente legati alle nuove tecnologie e agli strumenti informatici.

Il seguente grafico mostra le interazioni e le caratteristiche di ciascuno degli elementi che caratterizzano la teoria del MOMM.

Figura 18 - Computer Theft Iteration



Fonte: SINGLETON T., SINGLETON A., Fraud Auditing and Forensic Accounting, Four Edition, John Wiley & Sons, Inc, 2010, p. 181.

Il computer può essere, quindi, l'oggetto della frode, lo strumento con cui viene implementata o un elemento che intervenire in modo secondario nelle attività fraudolente. In base a tali elementi, i *computer crime* possono essere oggetto di molteplici classificazioni non solo correlate alla perdita di dati conseguita, al tipo di perdita o alla tipologia di frode commessa, ma anche basate sulla valutazione della fase in cui interviene l'utilizzo del computer e sul soggetto che commette l'illecito.

Se si considera la fase dell'attività illecita in cui viene utilizzato il sistema informatico, la classificazione prevede le seguenti tre categorie di riferimento:

- *Input*: rientrano in questa categoria tutte le frodi nelle quali è utilizzato un computer per l'inserimento o l'archiviazione di dati alterati relativi al sistema informativo aziendale;
- *Process*: la categoria comprende tutte le frodi in cui sono i processi implementati tramite un sistema informatico ad essere alterati ai fini della realizzazione dell'illecito;
- *Output*: si riferisce ai casi in cui oggetto del furto o della frode siano i dati o i documenti di output prodotti grazie al sistema informatico.

Se, invece, la classificazione è effettuata sulla base del soggetto che commette l'illecito si fa riferimento alla tradizionale distinzione tra frodi interne, quindi commesse da soggetti che operano all'interno dell'organizzazione economica, ed esterne, se il frodatore è un soggetto terzo rispetto all'azienda. Come anticipato in precedenza, il *cybercrime* interno è di gran lunga superiore agli illeciti commessi da soggetti esterni alle organizzazioni economiche in quanto le opportunità di frode e di accesso ai sistemi informatici aziendali, così come la conoscenza dei punti di debolezza dei controlli interni, sono molto superiori.

I fattori che hanno incrementato e incrementano i rischi di frode e la frequenza degli episodi possono essere riassunti nei seguenti elementi[136]:

- Internet: la connessione a internet e l'utilizzo di reti di computer favoriscono gli attacchi informatici rendendo necessario prevedere sistemi e misure di sicurezza sempre più sofisticate e sistemi di archiviazione dei dati e di accesso che prevedano misure più stringenti.
- Concentrazione dei dati: i sistemi informativi centrali spesso archiviano e conservano la molteplicità dei dati prodotti da un'organizzazione. I dati possono essere persi o distrutti per errore umano ma, allo stesso tempo, essere oggetto di furto: si pensi ai documenti, ai programmi e a tutte le informazioni confidenziali in possesso di un'organizzazione.
- Possibilità di manipolare i dati: analisti, programmatori e soggetti che operano in azienda che siano in possesso delle necessarie competenze possono agire per alterare e manipolare i dati aziendali. Molto spesso questo rischio risulta correlato all'assenza di sistemi e procedure di controllo contabile che abbiano ad oggetto i processi informatici.

[136] SINGLETON T., SINGLETON A., *Fraud Auditing and Forensic Accounting*, Four Edition, John Wiley & Sons, Inc, 2010, p. 182 e ss.

Dopo aver analizzato le principali caratteristiche dei *computer crime* e dei fattori e dei rischi che ne influenzano la diffusione, poniamo l'attenzione sui principali schemi di frode che rientrano in questa categoria.

Innanzitutto, è necessario evidenziare come sia molto più complesso individuare i responsabili di reati commessi tramite l'utilizzo di internet in quanto si tratta di soggetti molto spesso "invisibili". Risulta, quindi, molto complesso riuscire a tracciare e identificare i responsabili, ciò anche perché spesso non sono presenti prove concrete a supporto delle attività investigative. Per le ragioni appena esposte, gli investigatori ritengono che sia molto importante definire il profilo di questa tipologia di criminali: *«Profiling is particularly necessary with Internet crime due to the invisibility, untraceability, and, often, lack of evidence*[137]*»*

L'attività di profilazione, inoltre, è particolarmente rilevante se si considera che le caratteristiche tipiche dei responsabili di *internet crime* siano molto differenti da quelle del frodatore tipico, soprattutto se si considera che l'età media è molto più bassa. Si tratta, infatti, prevalentemente di giovani in grado di porre in essere attacchi molto dannosi grazie alle competenze e alle capacità informatiche possedute.

Passando alla trattazione delle principali categorie di *cybercrime*, l'UNICRI - *United Nations Interregional Crime and Justice Research Institute* - individua le seguenti tipologie:

- *LAMER (Wannabe)*: l'obiettivo di questa categoria di reati è quello di danneggiare o distruggere informazioni aziendali. Si tratta di attacchi effettuati per pura soddisfazione personale dai responsabili che sono soprattutto giovani e con conoscenze informatiche non elevate.
- *SCRIPT KIDDIE*: molto simile alla categoria precedente, ma in questo caso gli attacchi informatici sono eseguiti da giovani che operano in modo isolato e non in gruppo. Le motivazioni sono, anche in questo caso, di natura personale in quanto le azioni sono tipicamente implementate per esibizionismo.
- *ETHICAL HACKER*: questa categoria comprende tutti i soggetti che lavorano per collaudare o verificare il funzionamento dei sistemi informatici. Operano, quindi, su disposizione di proprietari e aziende e implementano gli attacchi al solo fine di individuare i punti di debolezza dei sistemi e fornire i risultati raggiunti.
- *QPSH (Quiet, Paranoid, Skilled Hacker)*: agiscono in modo invisibile senza diffondere le azioni intraprese e i risultati raggiunti.

[137] SINGLETON T., SINGLETON A., *Fraud Auditing and Forensic Accounting*, Four Edition, John Wiley & Sons, Inc, 2010, p. 186

- *CRACKER*: l'obiettivo delle attività illecite dei *cracker* è quello di conseguire profitti a danno dalle organizzazioni economiche. Può trattarsi sia di soggetti interni sia esterni.
- *CYBER-WARRIOR*: si tratta di *cracker* assoldati da altri che commettono l'illecito per scopi finanziari.
- *INDUSTRIAL SPY*: questa categoria comprende lo spionaggio industriale ma eseguito grazie alle tecniche e alle tecnologie informatiche.
- *GOVERNMENT AGENT E MILITARY HACKER*: tipicamente operano al di fuori delle organizzazioni economiche.

Le categorie più pericolose per le aziende sono, senza dubbio, quelle di *Cracker*, *Cyber Warrior* e *Industrial Spy* sia per gli obiettivi perseguiti dai responsabili, sia perché tipicamente si tratta di soggetti con elevatissime capacità informatiche.

Passando, invece, alla vera e propria trattazione degli schemi di frode più frequenti e tenendo conto della situazione del nostro Paese, in base al *Global Economic Crime and Fraud Survey 2018 – Summary Italia* di PwC le tecniche di *cybercrime* più frequenti sono, nell'ordine, le seguenti[138]:

- *Malware*: rientra nella più ampia categoria del *phishing* ma presenta un maggior grado di complessità in quanto il furto di dati e informazioni avviene mediante un software installato all'interno del sistema informatico della vittima. In alcuni casi è la vittima ad installare involontariamente il *malware* dopo essere stata indotta a scaricare file o altri contenuti online, in altri il download del file avviene in modo del tutto inconsapevole per la vittima a seguito di una forzatura del sistema informatico.
- *Phishing*: rientra tra le tecniche che consentono di ottenere dati sensibili delle vittime per scopi illeciti. In questa ipotesi le vittime sono indotte a rilasciare i propri dati o informazioni personali che vengono, quindi, acquisiti dai responsabili della frode. Tra le più frequenti tipologie di *phishing* implementate rientra il *Deceptive Phishing* che prevede l'invio di una email contenente un link a cui si richiede di accedere per il rilascio di informazioni. Normalmente i messaggi contengono molteplici riferimenti ingannevoli quali loghi, indirizzi e dettagli che inducono in errore chi riceve l'email: ad esempio presentano come mittente una banca o un ente che richiede le informazioni per ragioni urgenti.

[138] Per i dettagli relativi alle caratteristiche degli schemi di *cybercrime* cfr. POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 134.

- *Brute Force Attack*: scopo di questa tecnica è quello di estrapolare le *password* impiegate per l'accesso a uno specifico servizio o sistema. Le *password* sono individuate tramite l'analisi di tutte le possibili combinazioni che è possibile associare ad un ID.
- *Network scanning*: ha come obiettivo quello di acquisire le informazioni di tutti i sistemi che sono collegati all'interno di una rete mediante l'identificazione dell'IP.
- *Man in the middle*: come suggerito dalla stessa denominazione, questo schema prevede che il frodatore intercetti il flusso dei dati proveniente da una vittima che intende collegarsi a un sito internet reale e sicuro. Il responsabile si interpone tra la vittima e il sito internet in modo da filtrare tutti i dati in ingresso e in uscita non alterando la reale comunicazione tra le parti. Questa tecnica, talvolta conclusa anche mediante l'utilizzo di *malware*, risulta di difficile individuazione in quanto nessun segnale di malfunzionamento o di anomalie è percepito dalla vittima.

CAPITOLO 2 – L'utilizzo dei sistemi esperti per la revisione contabile e per le frodi aziendali

2.1 Fraud audit e forensic accounting: prevenzione e investigazione dei fenomeni fraudolenti

2.1.1 Introduzione

Il primo capitolo è stato interamente dedicato alla trattazione delle principali tipologie di frode, delle teorie poste alla base del fenomeno e della sua interpretazione e delle caratteristiche tipiche dei frodatori che le commettono. Grazie alla disamina di questi elementi è stato possibile definire il contesto di riferimento in cui si collocano e nel quale sono nate le discipline che rientrano o sono correlate alla materia del *Forensic Accounting*.

Il *Forensic Accounting* ha rappresentato il punto di partenza della mia attività di ricerca, nata con l'obiettivo di indagare le opportunità di utilizzo dei Big Data ai fini dell'individuazione delle frodi. Il presente capitolo ripercorre le principali fasi di evoluzione degli studi intrapresi che, partendo da un ambito disciplinare più ampio si sono successivamente focalizzati sull'analisi delle tecniche di *fraud auditing* e *fraud investigation* fino ad arrivare alle procedure di analisi mirate ad individuare alterazioni e anomalie presenti nei dati bilancio. Gli approfondimenti trattati nel presente capitolo e su cui si basa lo sviluppo della ricerca applicativa che sarà esposta nel terzo, sono rappresentati dai test sul libro giornale e dalle analisi dei dati di bilancio che consentono di evidenziare *red flag* e anomalie sintomatiche della presenza di frodi. Tali analisi sono state supportate dallo studio delle funzionalità e dell'utilizzo dei principali *tool* di *audit* e *forensic analitycs*.

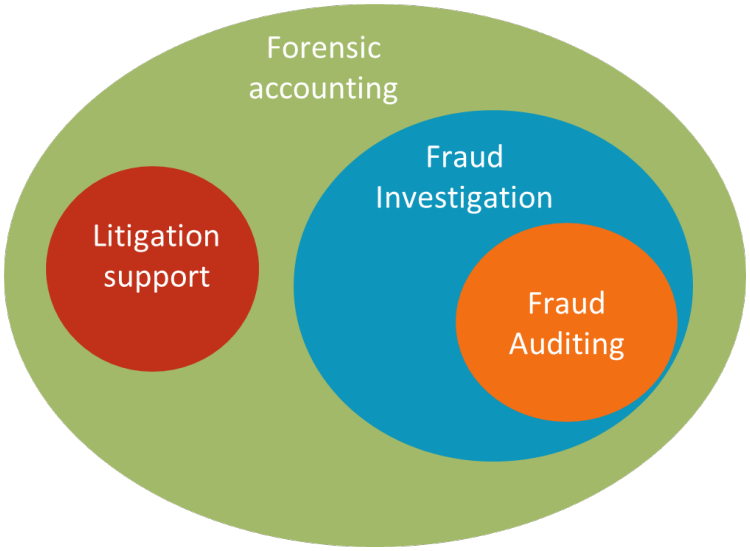
2.1.2 *Forensic Accounting* e *Fraud Examination*

Il *Forensic Accountig* può essere considerato come la macrocategoria di riferimento in cui rientrano ulteriori discipline specifiche correlate o non correlate all'individuazione delle frodi:

- *Litigation Support*;
- *Fraud Investigation* (o *Examination*);
- *Fraud Auditing*.

La materia, infatti, non si riferisce esclusivamente alle attività e alle tecniche di individuazione delle frodi, ma si estende all'ampia casistica delle problematiche che emergono in ambito legale e che presentano implicazioni o elementi di carattere economico o finanziario.
La seguente figura consente di rappresentare le discipline che afferiscono al *Forensic Accounting* in sottoinsiemi a loro volta disgiunti o inclusi reciprocamente.

Figura 19 - Le discipline del Forensic Accounting



Considerando le frodi, il *Forensic Accounting* comprende tutte le attività correlate alla loro individuazione e gestione e agli aspetti di carattere legale connessi alla loro risoluzione[139]. In particolare, nella materia rientrano le attività di prevenzione e di analisi dei controlli antifrode, le attività investigative, le attività di *Fraud Auditing* e *Fraud Investigation*.
Al contempo, il *Forensic Accounting* comprende anche tutte le attività correlate alle analisi dei dati non finanziari, al reporting destinato ai manager di un'azienda o al tribunale in caso di controversie e le attività di supporto nelle controversie di contabilità forense.
«Forensic accounting is the use of professional accounting skills in matters involving potential or actual civil or criminal litigation[140]».

[139] SINGLETON T., SINGLETON A., *Fraud Auditing and Forensic Accounting*, Four Edition, John Wiley & Sons, Inc, 2010, p. 20.
[140] ASSOCIATION OF CERTIFIED FRAUD EXAMINERS, *Fraud Examiners Manual (International)*, 2011, p. I-3; *«The word forensic is defined by Black's Law Dictionary as "used in or suitable to courts of law or public debate." Therefore, forensic accounting is actually litigation support involving accounting».*

La definizione è fornita dall'ACFE specifica che il lavoro di *Forensic Accounting* è svolto nella prospettiva di un futuro contenzioso (probabile o effettivo) che può riferirsi a molteplici tipologie di problematiche a cui può andare incontro un'azienda, ulteriori rispetto all'ipotesi di frode.
La seguente figura consente di riepilogare e schematizzare le principali attività che rientrano nel campo di indagine del *Forensic Accounting*.

Figura 20 - Campo di indagine del Forensic Accounting

In base alla definizione dell'ACFE, i servizi di *Forensic Accounting* possono essere suddivisi in due categorie di riferimento: consulenza in materia di contenzioso e servizi investigativi. In entrambi i casi, i servizi sono offerti applicando principi e teorie finanziarie a problematiche strettamente correlate a controversie legali e possono essere anche finalizzati a fornire una testimonianza in tribunale[141]. Tra le due categorie descritte, i servizi che si riferiscono alle attività investigative sono sicuramente quelli che maggiormente risultano correlati alle frodi e alla loro individuazione tramite l'applicazione di un approccio molto simile a quello impiegato dai *fraud examiner*.
Considerando l'attività complessivamente svolta dai *forensic accountant*, è importante evidenziare che tali professionisti possano essere coinvolti in indagini aziendali correlate a qualsiasi tipo di problematica forense: accuse o reati che coinvolgono il management o i

[141] KRANACHER M.J., RILEY R., *Forensic Accounting and Fraud Examination*, Wiley, 2020, p. 10.

dipendenti, cause di licenziamento, tangenti[142]. L'intervento del *forensic accountant*, in queste ipotesi, non solo è necessario a far luce sui reali fatti accaduti ma favorisce anche il contraddittorio tra le parti e la risoluzione della controversia.

Come evidenziato in *Figura 19*, l'attività del professionista forense si estende alla materia del *Litigation Support*, servizio attivato in risposta ad un'azione legale e finalizzato ad indagare e valutare l'integrità e l'entità di ciò che è oggetto della controversia: profitti, perdite, inadempimenti contrattuali, fallimenti[143]. Il termine "*litigation*" rimanda, quindi, alla presenza di un contenzioso che richiede un intervento di investigazione e attività di gestione e risoluzione della controversia mediante specifiche modalità di raccolta e di presentazione delle prove documentali raccolte[144]. L'AICPA fornisce la seguente definizione di *Litigation Services*: *«Litigation services are consulting services that ordinarily involve pending or potential formal legal or regulatory proceedings before a trier of fact in connection with the resolution of a dispute between two or more parties. A trier of fact may be a court, jury, regulatory body, or government authority or their agents; a grand jury; an arbitrator; or the mediator of a dispute[145].»* Lo stesso documento dell'AICPA identifica lo scopo di questi servizi che possono essere finalizzati a[146]:

- indagare i fatti accaduti e eseguire l'analisi dei dati raccolti;
- calcolare i danni ed eseguire valutazioni aziendali;
- gestire la raccolta e la presentazione dei documenti;
- gestire l'eventuale testimonianza da parte di esperti;
- fornire gli ulteriori servizi professionali richiesti.

Con riferimento alle controversie di carattere penale, il professionista forense ha lo scopo di prevenire tali crimini e di fornire in qualità di perito il proprio supporto in giudizio al fine di

[142] SINGLETON T., SINGLETON A., BOLOGNA J., LINDQUIST R., *Fraud Auditing and Forensic Accounting*, Third Edition, John Wiley & Sons, Inc, 2006, p. 45.
[143] SINGLETON T., SINGLETON A., BOLOGNA J., LINDQUIST R., *Fraud Auditing and Forensic Accounting*, Third Edition, John Wiley & Sons, Inc, 2006, p. 45.
[144] Cfr. POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 522.
[145] AICPA, *Litigation Services and Applicable Professional Standards, Consulting Services, Special Report 03-1*. Cfr. POGLIANI G., PECCHIARI N., MARIANI M., Frodi aziendali. Forensic accounting, fraud auditing e litigation, Egea, 2012, p. 522.
[146] AICPA, *Litigation Services and Applicable Professional Standards, Consulting Services*, Special Report 03-1; *«Litigation services may include fact-finding (including assistance in the discovery and analysis of data), damage calculations, business valuation, document management, expert testimony, and other professional services required by the client or counsel»*

valutare le transazioni finanziarie oggetto dei reati e delle accuse rivolte nei confronti di persone fisiche e società[147].

Il *forensic accountant* interviene, inoltre, nei reclami assicurativi e nelle attività di valutazione delle richieste di risarcimento per stimare danni, integrità della richiesta, verificare le questioni che si riferiscono a lesioni personali. Può essere coinvolto, infine, in attività di supporto ai governi nelle verifiche relative alla conformità normativa del comportamento e delle condotte delle società: si pensi ai controlli eseguiti per accertare che le società che hanno ricevuto particolari sovvenzioni abbiano agito nel rispetto della legislazione applicabile[148].

Considerando l'ampia casistica di controversie e problematiche in cui può essere coinvolto il professionista forense e l'esteso campo di indagine della materia, è facile constatare come le *skills* e le caratteristiche che il *forensic accountat* deve possedere siano molto differenti da quelle di un revisore o di un contabile.

Innanzitutto, è molto importante il profilo investigativo di tale professionista che, partendo dal problema potenziale o effettivo rilevato deve acquisire le informazioni e la documentazione necessaria ad analizzare la fattispecie e ottenere evidenze a supporto delle conclusioni raggiunte. In tal senso, pur partendo da elementi e considerazioni di carattere contabile, la disciplina deve necessariamente far riferimento a tecniche ulteriori e ben diverse da quelle tipiche dell'*accounting*: l'abilità del *forensic accountant* risiede nella capacità di intuire gli schemi utilizzati per attuare un illecito. La necessità di acquisire evidenze a supporto delle conclusioni raggiunte rende, inoltre, molto importante il lavoro di interpretazione della documentazione raccolta e la successiva comunicazione dei risultati raggiunti in termini legali.

Tenendo in considerazione esclusivamente l'attività del *forensic accountant* rivolta alle frodi è importante evidenziare che, oltre alle capacità investigative appena menzionate, il professionista debba essere in grado di identificare una frode sulla base di poche informazioni iniziali. Le informazioni minime acquisite devono essere utilizzate per individuare il possibile schema attuato

---

[147] SINGLETON T., SINGLETON A., BOLOGNA J., LINDQUIST R., *Fraud Auditing and Forensic Accounting*, Third Edition, John Wiley & Sons, Inc, 2006, p. 45; *«Efforts to prevent white-collar crime have consistently used accountants and auditors in attempts to sort out, assess, and report on financial transactions related to allegations against individuals and companies in a variety of situations, such as arson, scams, fraud (e.g., kickbacks or embezzlement), vendor frauds, customer frauds, investment scams, and stock market manipulations. In criminal matters, accountants and auditors as expert witnesses are increasingly important in court cases».*

[148] SINGLETON T., SINGLETON A., BOLOGNA J., LINDQUIST R., *Fraud Auditing and Forensic Accounting*, Third Edition, John Wiley & Sons, Inc, 2006, p. 45.

e le procedure che è necessario implementare per poter provare l'esistenza di una frode potenziale[149].

Altri aspetti di fondamentale importanza sono rappresentati dalla capacità del professionista di identificare prontamente i problemi e gli scostamenti significativi presenti in bilancio e l'attenzione alla corretta interpretazione dell'informativa finanziaria. Su tale ultimo punto è interessante notare che *«It is unusual for a transaction or a series of events to have only one interpretation[150]»*, di conseguenza è fondamentale che il professionista consideri tutti gli aspetti del fenomeno senza tralasciare alcun elemento o informazione.

«Forensic accountants are experienced, trained, and knowledgeable in all the different processes of fraud investigation including: how to interview people (especially the suspect) effectively, how to write effective reports for clients and courts, how to provide expert testimony in court, and rules of evidence. The ACFE refers to this definition of forensic accounting as fraud examination[151]».

In base alla definizione appena riportata, il *forensic accountant* che si rivolge ai processi di individuazione delle frodi può essere assimilato al *fraud examiner* (o *fraud investigator*). Tale ultima figura professionale si occupa di *fraud investigation*, materia che rappresenta una sottocategoria del *forensic accounting* (vedi *Figura 19*). Allo stesso tempo, il campo di indagine del *fraud investigation* si differenzia da quello del *fraud auditing* in quanto la materia comprende molteplici attività ulteriori che hanno ad oggetto la raccolta e l'analisi di elementi probativi di tipo non finanziario e l'esecuzione di indagini ed interviste.

2.1.3 Fraud Auditing

Come evidenziato nel precedente paragrafo, la disciplina del *Fraud Auditing* può essere considerata come un sottoinsieme della più ampia categoria del *Fraud Investigation*, a sua volta ricompreso nel campo di indagine del *Forensic Accounting*. Il *Fraud Auditing*, infatti, si riferisce agli approcci e alle metodologie impiegate in modo specifico per poter individuare una frode e raccogliere gli elementi probativi necessari a dimostrarne l'esistenza: il *forensic accountant*

[149] VONA L.W., Fraud Risk Assessment. Building a Fraud Audit Program, John Wiley & Sons, Inc., 2008, p. 36.

[150] SINGLETON T., SINGLETON A., BOLOGNA J., LINDQUIST R., *Fraud Auditing and Forensic Accounting*, Third Edition, John Wiley & Sons, Inc, 2006, p. 47.

[151] SINGLETON T., SINGLETON A., *Fraud Auditing and Forensic Accounting*, Four Edition, John Wiley & Sons, Inc, 2010, p. 12.

interviene, in tal senso, in un momento successivo, quando i sospetti di frode sono stati già tradotti in un'azione legale.

L'attività di *Fraud Auditing* può essere svolta da un professionista in possesso delle conoscenze e della preparazione tipica di un revisore a cui devono affiancarsi ulteriori *skill*, esperienze e capacità in grado di rilevare e documentare le frodi presenti nelle rilevazioni contabili e contenute nell'informativa finanziaria della società[152]. Un *fraud auditor* deve essere in grado di gestire una frode e valutarla sotto molteplici prospettive e punti di vista, in particolare tenendo conto degli aspetti legali e contabili: *«Fraud auditors must know what a fraud is from a legal and audit perspective, an environmental perspective, a perpetrator's perspective, and a cultural perspective. They also need both general and specific kinds of experience[153]».*

Il *Fraud Auditing* può essere considerato come un'attività in grado di migliorare le procedure finalizzate alla prevenzione dei fenomeni fraudolenti e all'individuazione delle frodi: *«(…) fraud auditing is the process of detecting, preventing, and correcting fraudulent activities»[154]*.

Il *fraud auditor* deve essere, innanzitutto, in grado di distinguere le anomalie individuate nelle scritture contabili e nell'informativa finanziaria che sono state generate esclusivamente da un errore umano da quelle che, al contrario, possono costituire un elemento probativo utile all'individuazione di una frode. Frequentemente errori e omissioni sono commessi in modo involontario dai soggetti che svolgono le molteplici mansioni correlate ai differenti cicli aziendali di produzione: in tali ipotesi, mancano l'elemento dell'intenzionalità e le altre caratteristiche tipiche di una frode.

Aspetto di fondamentale importanza per poter indagare la presenza di frodi, è la conoscenza del sistema di controllo interno aziendale e delle debolezze delle procedure di controllo: in questo modo è possibile stabilire quali siano le opportunità di frode presenti in uno specifico contesto aziendale. Un frodatore, infatti, sfrutterà tali debolezze e carenze per implementare il proprio schema di frode, tenendo conto della presenza di un sistema di controllo interno in cui le procedure e i controlli sono assenti o non operano efficacemente.

---

[152] Cfr. COENEN T.L., Expert Fraud Investigation. A step by step guide, John Wiley & Sons, Inc, 2009, p. 14.
[153] SINGLETON T., SINGLETON A., *Fraud Auditing and Forensic Accounting*, Four Edition, John Wiley & Sons, Inc, 2010, p. 14.
[154] SINGLETON T., SINGLETON A., *Fraud Auditing and Forensic Accounting*, Four Edition, John Wiley & Sons, Inc, 2010, p. 14.

In tale contesto, il *fraud auditor* deve essere dotato sia delle capacità tipiche di un revisore, sia di ulteriori capacità di tipo investigativo. L'attività di investigazione delle frodi deve essere svolta mediante l'applicazione di un duplice approccio[155]:

- l'approccio induttivo tipico del revisore che si basa sull'analisi del particolare per arrivare a formulare delle osservazioni di carattere generale;
- l'approccio deduttivo dell'attività investigativa di tipo *top-down* che procede dall'universale al particolare.

Un incarico di *fraud audit* è svolto allo scopo di rispondere a un rischio di frode e può costituire una parte di un'attività di revisione più ampia o rappresentare la finalità per la quale l'intera revisione viene svolta[156].

Vona definisce le attività di *Fraud Auditing* come l'applicazione di procedure di revisione implementate per innalzare le probabilità di individuazione delle frodi, in base ad un processo suddiviso in quattro fasi[157]:

- *Fraud risk identification*: identificazione dei rischi inerenti e dei possibili schemi di frode attuabili.
- *Fraud risk assessment*: valutazione del rischio di frode e dei collegamenti con il sistema di controllo interno e le debolezze presenti nei controlli.
- *Fraud audit procedure*: implementazione delle procedure di revisione necessarie alla raccolta degli elementi probativi.
- *Fraud conclusion*: al termine del processo è possibile determinare la presenza di una o più evidenze di frode o, al contrario, l'assenza di *red flag*.

Fraud risk identification

L'identificazione dei rischi di frode è un'attività particolarmente importante per poter svolgere un incarico di *fraud audit* in quanto consente di delimitare il campo di indagine e di analisi ai soli *inherent fraud schemes*. Il *fraud audit program* è, infatti, sviluppato solo in riferimento a tali rischi di frode identificati e non a tutti i possibili rischi. In tal senso, è opportuno, dapprima, identificare

---

[155] *«Financial auditors tend to use the inductive approach, whereas investigators tend to use the deductive approach. Fraud auditors may have to use both approaches in developing their investigative mentality»*; SINGLETON T., SINGLETON A., *Fraud Auditing and Forensic Accounting*, Four Edition, John Wiley & Sons, Inc, 2010, p. 14.

[156] VONA L.W., *The Fraud Audit. Responding to the Risk of Fraud in Core Business Systems*, John Wiley & Sons, Inc, 2011, p. 5.

[157] Il riferimento al processo suddiviso in step e la successiva descrizione di ciascuna delle quattro fasi sono tratti da VONA L.W., *The Fraud Audit. Responding to the Risk of Fraud in Core Business Systems*, John Wiley & Sons, Inc, 2011, pp. 5 e ss.

la struttura del rischio di frode al fine di individuare la tipologia di schema che può essere implementata in considerazione dei sistemi coinvolti e delle opportunità che è possibile sfruttare. In secondo luogo, è importante stabilire a che livello si può determinare lo scenario di frode secondo ciò che viene definito *drill-down process*: a livello aziendale, a livello di classe di transazioni o in riferimento a uno specifico conto presente in contabilità generale, a un dipendente o a elementi che coinvolgono il sistema di controllo interno. A questo punto è necessario approfondire l'analisi stabilendo le correlazioni presenti tra le opportunità di frode e il sistema aziendale e, infine, stabilire le possibili strategie di occultamento e di attuazione dello scenario di frode delineato.

Nella seguente tabella sono riepilogate le caratteristiche e il significato dei principali termini utilizzati nell'ambito del processo di identificazione dei rischi di frode[158].

Terminologia	Significato
Fraud Risk Structure	Strumento utilizzato per definire la portata e gli scopi dell'attività di *fraud auditing*. Consente di definire la classificazione primaria di frode, le sottoclassi di frode, gli schemi inerenti e i possibili scenari di frode relativi alla realtà aziendale considerata.
Drill-Down Process	È un processo che consente di definire a che livello, dal generale allo specifico, può essere presente una frode. In base al livello individuato sarà possibile avere maggiori o minori scenari di frode: a livello azienda avremo il massimo numero di scenari identificabili.
Permutation Analysis	Analisi dell'entità e delle transazioni al fine di comprendere l'organizzazione e i processi aziendali e le correlazioni con i soggetti impiegati nello svolgimento delle molteplici mansioni. Grazie a tale analisi è possibile delimitare il contesto in cui possono presentarsi i possibili scenari di frode.
Fraud Opportunity	Si riferisce all'abilità e alle possibilità che un individuo interno e esterno all'azienda possano commettere una frode. La specifica mansione svolta da un individuo, la mancanza di efficaci procedure di controllo o la possibilità di accedere facilmente a un bene aziendale rendono possibile implementare uno schema di frode (a

[158] Le definizioni e la spiegazione della terminologia impiegata è tratta da VONA L.W., *The Fraud Audit. Responding to the Risk of Fraud in Core Business Systems*, John Wiley & Sons, Inc, 2011, pp. 43 e ss.

	prescindere dalla sua effettiva riuscita o dalla successiva individuazione).

Grazie all'identificazione dei rischi e alla determinazione della struttura di frode, il *fraud auditor* è in grado di definire i possibili scenari di frode. Per poter raggiungere utilmente questi obiettivi e non commettere errori, è molto importante che in questa fase non si tenga conto della capacità del sistema di controllo interno di mitigare i rischi di frode identificati, tale aspetto deve essere considerato nell'ambito delle attività di valutazione dei rischi. Inoltre, è fondamentale non focalizzare l'attenzione né sul *conversion cycle*, quindi sulle modalità di acquisizione dei benefici da parte del frodatore, né sulle possibilità di occultamento della frode: in entrambi i casi il rischio è quello di perdere informazioni necessarie a delineare ulteriori scenari di frode. Infine, l'identificazione degli scenari di frode non può prescindere dalla conoscenza dell'azienda, dell'attività svolta, del suo settore di appartenenza e dell'ambiente in cui essa opera.

Fraud risk assessment

La seconda fase del processo di *Fraud Auditing* è rappresentata dalle attività di valutazione dei rischi individuati. L'elenco di tutti i rischi di frode relativi ad un'organizzazione economica deve essere accompagnato dalla valutazione della probabilità che ciascun rischio si verifichi e dall'impatto associato a ciascuna tipologia di frode individuata. Come evidenziato da Vona, le due distinte analisi sono finalizzate all'ottenimento di due *score* da utilizzare per determinare la valutazione finale del rischio. Grazie a tali attività è possibile stimare e gestire il costo sostenuto dall'organizzazione in presenza di frode e determinare il programma di revisione da implementare per poter rispondere efficacemente ai rischi identificati. Probabilità e impatto sono, quindi, le variabili di riferimento da utilizzare nel corso dell'intera analisi dei rischi e del lavoro di *audit* da svolgere.

Tra le due componenti, quella che richiede un maggiore sforzo in termini di analisi e che presenta maggiori complessità di definizione è sicuramente la probabilità di accadimento. Vona chiarisce che tale aspetto è correlato alle difficoltà di valutare la probabilità che una persona sia intenzionata e/o riesca a commettere una frode, in quanto ciò dipende in gran parte dalle pressioni e dalle giustificazioni che incentivano e spingono all'azione. «*The fraud triangle indicates that individuals commit fraud because of opportunity, pressures, and rationalization. The opportunity aspect can be easily determined through understanding the internal controls in the*

core business processes. Unfortunately, determining the individual pressures or rationalizations in a fraud risk assessment is not as easy given the judgment of fraud likelihood necessary[159]*».*

L'autore, oltre a formulare importanti considerazioni in merito alla difficoltà insita nel determinare la probabilità di accadimento di una frode, specifica come possano essere utilizzati due differenti approcci per la sua stima: l'analisi dei dati tramite tecniche di *data mining* e l'analisi del sistema di controllo interno. L'analisi dei dati consente di valutare se i dati e le informazioni a disposizione siano coerenti con la presenza di una frode, mentre la valutazione del sistema di controllo interno di stabilire la capacità dei controlli di mitigare i rischi di frode: i due approcci possono essere utilizzati separatamente o simultaneamente in base alle specifiche esigenze.

Fraud audit procedure

Le procedure di *fraud audit* sono configurate e implementate per rispondere ai rischi identificati e finalizzate a individuare i possibili scenari di frode. La scelta delle procedure da svolgere dipende dalla strategia di occultamento che si intende individuare: in base allo schema implementato dal frodatore, infatti, è necessario eseguire verifiche differenti per raccogliere evidenze di revisione necessarie e sufficienti. In tal senso, Vona evidenzia come sia necessario implementare procedure di revisione sia finalizzate a testare e verificare i *red flag* individuati nell'ambito di uno scenario di frode, sia ulteriori procedure implementate in risposta ai rischi inerenti individuati.

Infine, è importante considerare, ai fini dello svolgimento delle procedure di revisione, che gli schemi di frode attuabili sono legati alla struttura dell'azienda e del suo sistema di controllo interno. Per le ragioni descritte è fondamentale che il revisore esegua, innanzitutto, l'attività di verifica della società, del suo sistema di controllo interno e del livello di separazione delle mansioni presente.

2.1.4 La revisione contabile e le frodi aziendali

Come descritto nei paragrafi precedenti, le attività di *Fraud Auditing* rientrano pienamente tra le discipline del *Forensic Accounting*. Considerazioni analoghe non possono essere effettuate, invece, per la revisione contabile, quindi per tutte le attività di verifica che rientrano nel campo di azione del *Financial Audit*.

[159] VONA L.W., *The Fraud Audit. Responding to the Risk of Fraud in Core Business Systems*, John Wiley & Sons, Inc, 2011, p. 70.

Anche se le procedure impiegate nello svolgimento di incarichi di *fraud audit* sono spesso molto simili a quelle eseguite nel corso degli incarichi di revisione contabile, le due attività non possono essere tra loro sovrapposte in quanto differenti sono gli obiettivi perseguiti.

La revisione contabile, infatti, ha come scopo quello di esprimere un giudizio sull'informativa economico finanziaria prodotta dalla società, giudizio che non garantisce in assoluto che il bilancio non sia inficiato da errori o frodi. L'ISA Italia 200 afferma, infatti, che *«La finalità della revisione contabile è quella di accrescere il livello di fiducia degli utilizzatori nel bilancio. Ciò si realizza mediante l'espressione di un giudizio da parte del revisore in merito al fatto se il bilancio sia redatto, in tutti gli aspetti significativi, in conformità al quadro normativo sull'informazione finanziaria applicabile».*

Presupposto della formazione del giudizio di revisione, in base a quanto definito dall'ISA Italia 700, è che il revisore abbia acquisito una ragionevole sicurezza che il bilancio nel suo complesso non contenga errori significativi, dovuti a frodi o a eventi o comportamenti non intenzionali. Molto importante è il significato da attribuire all'espressione "ragionevole sicurezza" che si discosta dal concetto di certificazione del bilancio e di "certezza" che lo stesso non presenti errori o frodi. Come definito dallo stesso ISA Italia 700, per ragionevole sicurezza si intende *«un livello elevato di sicurezza che tuttavia non fornisce la garanzia che una revisione contabile svolta in conformità ai principi di revisione internazionali (ISA Italia) individui sempre un errore significativo, ove esistente»*. Il lavoro del revisore contabile, infatti, nasce allo scopo di identificare tutti gli scostamenti significativi d'informativa, ovvero gli scostamenti che considerati singolarmente o nel loro insieme siano in grado, ragionevolmente, di influenzare le decisioni economiche assunte dagli utilizzatori del bilancio. Proprio sulla base del concetto di significatività, il revisore pianifica le attività e i controlli da svolgere, considerando, simultaneamente i rischi individuati. La significatività è, quindi, un dato quantitativo che può essere stimato sulla base di differenti tipologie di calcolo e metodologie e che viene utilizzato come parametro per determinare l'estensione delle attività da svolgere e, contestualmente, identificare tutti gli errori da considerare rilevanti[160]. Nella fase conclusiva del processo di revisione e ai fini della redazione

[160] POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 46; *«Per quanto l'enfasi posta non sia tanto su semplici elementi di tipo quantitativo ma anche su aspetti squisitamente qualitativi, cioè facenti perno sulla natura e sulla genesi di uno scostamento piuttosto che solo sul suo ammontare, è in ogni caso indubitabile che tale approccio lasci comunque spazi di manovra a coloro i quali vogliano realizzare degli atti illeciti oppure abbiano la volontà di occultarne l'effetto e ciò è tanto più vero quanto più costoro hanno una ben solida conoscenza di come sono poste in atto le procedure di controllo fondate su sopra citato principio».*

della relazione di revisione, la significatività rappresenta il *benchmark* di riferimento per poter determinare la tipologia di giudizio da emettere[161].

L'estensione del lavoro di revisione si lega, quindi, al concetto di significatività e alla valutazione dei rischi operata in fase di pianificazione: si tratta dei criteri alla base della determinazione dei programmi di lavoro relativi alle attività da svolgere. Anche in considerazione dei tempi e dei costi del lavoro, i controlli e le attività di revisione da svolgere non possono riferirsi a tutte le operazioni e le procedure aziendali, ma a un campione rappresentativo delle stesse. L'utilizzo delle tecniche di campionamento è, di conseguenza, fondamentale per consentire al revisore di acquisire sufficienti e appropriati elementi probativi per esprimere un giudizio sull'informativa finanziaria dell'azienda sottoposta a revisione. Limitare le verifiche svolte dal revisore esclusivamente a un campione di elementi determinato in base al rischio valutato, consente di rendere efficiente il lavoro del revisore in quanto sarebbe impossibile verificare interamente tutte le operazioni aziendali. *«Il campionamento è uno dei tratti caratteristici del lavoro di revisione in quanto l'azzeramento del rischio di individuazione (con il quale annullare anche il rischio di revisione) sarebbe possibile soltanto in presenza di un controllo dell'universo delle operazioni e delle rilevazioni aziendali, il che richiederebbe un tale consumo di risorse e, di conseguenza, genererebbe un così elevato costo di svolgimento delle attività di controllo, da rendere qualsiasi incarico di revisione molto costoso e, probabilmente, non profittevole[162]».*

Le verifiche a campione svolte dal revisore sono finalizzate, quindi, a ottenere gli elementi probativi necessari a supportare adeguatamente il giudizio di revisione e non a raggiungere la sicurezza e l'assoluta certezza che l'informativa aziendale sia priva di errori o frodi. L'approccio metodologico e procedurale impiegato nelle attività di audit non è, quindi, utile ed efficace nel caso in cui la revisione si ponga come obiettivo quello di individuare una frode: *«Per verificare la presenza di una frode, infatti, è necessario che le analisi siano effettuate avendo quale riferimento l'intero novero di operazioni contraddistinte da peculiari caratteristiche; in sostanza è imprescindibile, per tale scopo, passare al vaglio tutte le transazioni effettuate in un certo periodo, di un ammontare particolarmente "anomalo", chiuse con un soggetto terzo definito, che risultino approvate da un determinato funzionario ecc.[163]».* Gli autori (Pogliani et al.) mettono in evidenza come un frodatore potrebbe utilmente "diluire" le operazioni anomale all'interno delle numerose

[161] Cfr. D'ALESSIO R., ANTONELLI V., BOZZA E., *Principi di Auditing. Concetti, modelli, metodologie, applicazioni*, Volume I, Edises, 2017, p. 298.
[162] D'ALESSIO R., ANTONELLI V., BOZZA E., *Principi di Auditing. Concetti, modelli, metodologie, applicazioni*, Volume I, Edises, 2017, p. 315.
[163] POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 45.

transazioni che derivano dalle relazioni aziendali, rendendo impossibile la loro rilevazione tramite gli strumenti utilizzati dai revisori.

Storicamente il ruolo del revisore è mutato nel corso del tempo in base alle specifiche esigenze di ciascuna epoca di riferimento. All'inizio del XIX secolo, ad esempio, la funzione del revisore era quella di verificare che l'informativa finanziaria di un'impresa fosse corretta e attendibile, mentre alla fine del secolo i revisori erano sempre più orientati a svolgere attività finalizzate all'individuazione delle frodi[164]. Il ruolo del revisore è mutato nuovamente nel corso dei primi decenni del '900 grazie al contributo dei revisori inglesi che sostenevano che scopo dell'attività fosse quello di esprimere un giudizio sulla veridicità e correttezza del bilancio[165]. I temi delle funzioni del *financial audit* e del ruolo del revisore sono stati ampiamente dibattuti nel corso del tempo, fino all'emanazione dei principi di revisione SAS 99 e ISA 240 che si è avuta nel corso dei primi anni del 2000. Con riferimento alle frodi, tali principi hanno stabilito che i revisori sono tenuti a identificare la *«presenza di frodi che alterino in modo significativo il sistema dei valori d'azienda»*[166].

Dalla lettura dell'ISA Italia 240 si evince chiaramente che a causa dei limiti intriseci dell'attività di revisione, non può essere eliminato il rischio che alcuni errori significativi presenti in bilancio possano non essere individuati e che *«Il rischio di non individuare un errore significativo dovuto a frodi è più elevato rispetto al rischio di non individuare un errore significativo derivante da comportamenti od eventi non intenzionali»*.

Anche se l'attività di revisione non nasce con la finalità di individuare una frode, in base al principio appena citato, i revisori sono comunque responsabili di mantenere lo scetticismo professionale durante l'intera attività di audit al fine di considerare le possibili forzature messe in atto dalla direzione. Inoltre, il revisore deve tener conto del fatto che l'individuazione delle frodi richiede l'implementazione di un programma e di procedure mirate che differiscono da quelle normalmente utilizzate ai fini dell'individuazione degli errori non intenzionali.

In base a quanto premesso, il potenziamento delle attività di revisione svolte ai fini dell'individuazione delle frodi costituisce un punto di forza molto importante per abbassare il

---

[164] Cfr. GOLDEN T.W., SKALAK S. L., CLAYTON M.M., *A guide to forensic accounting investigation*, John Wiley & Sons, Inc., Hoboken, New Jersey, 2006, pp. 7 e ss.

[165] Cfr. PORTER B., *An Empirical Study of the Audit Expectation – Performance Gap*, Accounting and Business Research, Vol. 24, N. 93, 1993; Gli autori (Pogliani et al.) motivano tale cambiamento facendo riferimento al pensiero di Porter secondo il quale questo mutamento sia stato causato dall'aumento delle dimensioni delle aziende e della numerosità delle transazioni compiute che rendevano difficile poter verificare e controllare la totalità delle operazioni.

[166] POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 51.

rischio che il revisore non sia in grado di individuare un errore intenzionale. Ciò ha importanti ricadute sul livello di affidabilità e sulla qualità dell'attività professionale, concorrendo, tra l'altro, ad abbassare l'*expectation gap* presente tra le attese degli utilizzatori di bilancio e le effettive finalità e possibilità della professione[167].

Poiché non è pensabile ampliare le attività di controllo rendendole simili a quelle previste nell'ambito del *fraud audit*, né venir meno alla metodologia di lavoro sancita dai principi di revisione, il punto di svolta per il potenziamento delle attività di audit è sicuramente costituito dall'utilizzo delle nuove tecnologie e dell'intelligenza artificiale.

L'analisi di intere popolazioni di dati svolta tramite *software* e procedure automatizzate, consente al revisore di estendere la portata del lavoro e incrementare le possibilità di identificare anomalie, in particolare grazie all'utilizzo di strumenti predittivi della presenza di anomalie e *tool* specializzati nei *Journal Entries Test* e nelle analisi di bilancio. Tali strumenti consentono di indagare in modo approfondito le frodi che rientrano tra le politiche di falsificazione dei bilanci aziendali, implementate dal frodatore tramite schemi che prevedono l'utilizzo di numerose transazioni finalizzate ad occultarne gli effetti.

Nei prossimi paragrafi analizzeremo le possibilità di prevenzione e investigazione dei fenomeni fraudolenti nell'era dei *Big Data*, valutando i principali *tools* di *Forensic Analytics* e di gestione dei *Journal Entries Test*.

2.2 La prevenzione e l'investigazione dei fenomeni fraudolenti nell'era dei *Big Data*

2.2.1 *Big Data* – definizione ed evoluzione del termine

Per poter approfondire le tematiche e le analisi relative all'utilizzo dei *Big Data* e dei sistemi esperti nelle attività di *audit* e ai fini dell'individuazione delle frodi aziendali, è opportuno soffermarsi sulle caratteristiche, le teorie e l'evoluzione che hanno caratterizzato i due elementi oggetto di indagine.

Innanzitutto, è importante analizzare le definizioni che nel tempo sono state attribuite al termine *Big Data*, per poter delimitare gli elementi e gli aspetti che tale termine sottende.

[167] POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012, p. 41; gli autori mettono in evidenza come il problema sia stato rilevato già a partire dalla metà degli anni '70 e riconosciuto dalla Commissione Cohen che lo ha definito come divergenza tra "ciò che il pubblico si aspetta e ciò che i revisori possono ragionevolmente realizzare".

Le definizioni di *Big Data* sono numerose e ciò rende complesso avere una descrizione sintetica ed incisiva di tale concetto poiché in costante e continua evoluzione. Al 2001 risale il modello delle "3V" di Douglas Laney basato su tre variabili: *volume, velocity, variety*. Le tre variabili intendono fare riferimento alle tre caratteristiche fondamentali dei *Big Data*[168]:

- Volume: fa riferimento alla quantità dei dati prodotta e alla dimensione dei dati che attualmente sono misurabili in *zettabyte*. Come mostrato nella seguente tabella, uno *zettabyte* presenta un ordine di grandezza di 10^{21}

Nome	Simbolo	Multiplo
Kilobyte	KB	10^3
megabyte	MB	10^6
Gigabyte	GB	10^9
Terabyte	TB	10^{12}
Petabyte	PB	10^{15}
Exabyte	EB	10^{18}
Zettabyte	ZB	10^{21}
Yottabyte	YB	10^{24}

- Velocità: descrive la frequenza di produzione dei dati e la velocità di estrazione degli stessi.
- Varietà: fa riferimento alla provenienza dei dati e alle molteplici tipologie di dati generati.

Alle "3V" codificate da Lane si è poi aggiunta una quarta "V" costituita dalla *Veridicità* dei dati, quindi dalla loro affidabilità, ma molti studiosi fanno riferimento anche modelli caratterizzati dalla presenza di 5 e 6 "V".

«Big data refers to datasets whose size is beyond the ability of typical database software tools to capture, store, manage, and analyze[169]».

[168] ASK U., MAGNUSSON J., BREDMAR K., *Big Data Use in Performance Measurement and Management: A Call for Action*, Journal of Business and Economics, Marzo 2016, Volume 7, No. 3, pp. 402-417; ALLES M., GRAY G. L., *The pros and cons of using big data in auditing: a synthesis of the literature and a research agenda*, Settembre 2015.

[169] MCKINSEY, *Big data: The next frontier for innovation, competition, and productivity*, McKinsey Global Institute, Giugno 2011.

In base a quanto esposto, possiamo affermare che i *Big Data* si riferiscono a volumi di dati molto ampi, caratterizzati da una frequenza di produzione elevata e da una varietà tale da non poter essere elaborata dai tipici supporti informatici[170].

I *Big Data* possono essere definiti come un nuovo strumento in grado di fornire informazioni dettagliate su fenomeni molto complessi, sono, inoltre, fondamentali nel prevenire eventi quali crisi economiche, epidemie, diffusione delle risorse economiche e delle opinioni[171]. Tali obiettivi possono essere perseguiti dai *Big Data* in ragione della loro diffusione in ogni ambito e settore, non solo della vita economica, in quanto sono in grado di incidere sui livelli di produttività e delle potenzialità di sviluppo economico, ma anche in riferimento alla sfera sociale e personale di ogni comunità.

Il maggior impiego dei *Big Data* si è avuto, ad oggi, soprattutto in ambito medico-sanitario, in particolare nel campo dell'innovazione farmaceutica e nell'epidemiologia, settori in cui è necessario ottenere informazioni tempestive e dettagliate. In ambito aziendale sono stati, invece, dapprima impiegati nelle aree vendita e marketing, con la finalità di individuare in tempi rapidi e in modo specifico e particolareggiato quali siano le esigenze e i bisogni dei clienti e i nuovi settori o *target* da raggiungere[172], successivamente il loro impiego si è diffuso notevolmente anche nell'area della contabilità e della finanza.

Tra le principali opportunità di impiego dei *Big Data* in ambito aziendale, *l'Accountancy Futures Academy* individua il loro utilizzo ai fini della gestione del rischio. In particolare, i *Big Data* consentirebbero un ampliamento del campo di indagine grazie alle maggiori informazioni disponibili e renderebbero più semplice l'identificazione di alcuni rischi, tra cui quello di frode e i rischi derivanti dall'investimento in nuovi mercati e prodotti[173]. Nel medesimo documento dell'*Accountancy Futures Academy* si fa riferimento alla necessità sempre crescente di disporre

---

[170] *«Big Data è un nuovo concept di conoscenza aziendale degli oggetti e degli eventi di business che fa leva sull'attuale varietà dei dati, in termini di formati (strutturati e non strutturati) e fonti (interne ed esterne), sull'aumentata velocità di generazione, raccolta, aggiornamento ed elaborazione dei dati (in tempo reale, in streaming, dati "tracciati") e sul crescente volume dei dati stessi, al fine di generare nuove analisi e insight, in ogni settore economico, in imprese di ogni dimensione, precedentemente considerate oltre le capacità tecniche e interpretative disponibili e per scoprire infine un nuovo potenziale valore di business; per ottenere questi risultati le imprese devono gestire gli appropriati fattori abilitanti, di tipo organizzativo, tecnologico e normativo»*; così PASINI P., PEREGO A., *Big Data: nuove fonti di conoscenza aziendale e nuovi modelli di management*, Rapporto di ricerca per IBM, SDA Bocconi, 2012.

[171] GIANNOTTI F., *Big Data e Social Mining*, KDDLAB; Giannotti definisce i Big Data come *«il nuovo microscopio che rende misurabile la società"*.

[172] PASINI P., PEREGO A., *Big Data: nuove fonti di conoscenza aziendale e nuovi modelli di management*, Rapporto di ricerca per IBM, SDA Bocconi, 2012.

[173] ACCOUNTANCY FUTURES ACADEMY, *Big Data: its power and perils*, The Association of Chartered Certified Accountants, Novembre 2013, Table 3.1, p.14.

di dati integrati di differenti tipologie e all'esigenza crescente nei settori della contabilità, della revisione, degli intermediari bancari e degli investitori istituzionali di analizzare indicatori non tradizionali[174]. In tal senso, cresce l'importanza dei *Big Data* e dell'Intelligenza Artificiale da utilizzare nel contesto aziendale per migliorare la gestione e il controllo dei rischi.

In tale ottica, le società di revisione hanno iniziato ad investire sempre di più in nuove tecnologie al fine di modificare le modalità di svolgimento delle attività di *audit*[175]. All'aumento della complessità gestionale delle aziende anche le attività di *audit* hanno dovuto modificare il proprio approccio, ciò anche alla luce dei cambiamenti che stanno interessando il mercato della revisione contabile e la crescente importanza che sta assumendo tale attività. Si pensi, ad esempio, che a partire dall'approvazione dei bilanci 2021, in Italia anche le c.d. Nano imprese, caratterizzate da parametri dimensionali particolarmente ridotti, in presenza di specifiche condizioni saranno obbligate alla nomina dell'organo di controllo o del revisore[176]. Tali considerazioni ci permettono di comprendere quanto l'attività di revisione stia diventando importante nel contesto nazionale e internazionale in quanto l'organo di controllo aziendale viene considerato fondamentale ai fini della prevenzione e della gestione della crisi aziendale. L'attività di revisione sta acquisendo sempre maggiore importanza nel sistema economico finanziario anche alla luce delle recenti crisi economiche e degli scandali finanziari che si sono susseguiti nel corso degli ultimi anni. In considerazione di tali aspetti, la revisione contabile può garantire sulla sicurezza e la veridicità della solidità finanziaria delle imprese e di conseguenza incidere positivamente sulla creazione di un tessuto sociale più sano[177].

L'utilizzo dei *Big Data* rappresenta, quindi, un'opportunità fondamentale al fine di formulare delle previsioni più accurate sul cliente revisionato e giungere a un più elevato livello di comprensione dell'azienda grazie allo studio e all'analisi delle correlazioni esistenti tra grandi volumi di dati derivanti da molteplici fonti informative.

---

[174] ACCOUNTANCY FUTURES ACADEMY, *Big Data: its power and perils*, The Association of Chartered Certified Accountants, Novembre 2013, Table 3.1, p.25.

[175] EY, *Big Data and analytics in the audit process: mitigating risk and unlocking value*, EY Center for Board Matters, Settembre 2015.

[176] La norma rientra nell'ambito dell'introduzione del nuovo Codice della crisi di impresa e dell'insolvenza e delle misure da implementare per prevenire e contenere lo stato di crisi aziendale. L'obbligo di nomina è previsto, in base all'art. 2477 c.c., per tutte le società che abbiano superato per due esercizi consecutivi uno dei seguenti limiti: 1) totale dell'attivo dello stato patrimoniale: 4 milioni di euro; 2) ricavi delle vendite e delle prestazioni: 4 milioni di euro; 3) dipendenti occupati in media durante l'esercizio: 20 unità.

[177] LIBRO VERDE, *La politica in materia di revisione contabile: gli insegnamenti della crisi*, 13 ottobre 2010.

La mole di dati e di informazioni disponibili, così come gli importanti progressi tecnologici impongono al mondo della revisione di adeguarsi e progredire al fine di poter cogliere nuove opportunità e rafforzare il proprio ruolo e le proprie funzionalità[178].

2.2.2 Analisi dei dati

La prima attività che un revisore è tenuto a svolgere per poter implementare un programma di revisione efficace in risposta a possibili rischi di frode è quella di *fraud risk assessment.* Scopo di questa attività svolta in fase di pianificazione è quello di individuare e valutare la possibile presenza di uno o più rischi di frode nell'ambito dell'organizzazione economica oggetto di revisione. L'attività presuppone, non solo l'individuazione di tali rischi, ma anche la stima dell'impatto che gli stessi andrebbero a determinare a livello di bilancio.

Più nel dettaglio, mediante il *fraud risk assessment* è possibile ottenere i seguenti risultati che saranno utili al revisore per definire il programma di *audit* da svolgere[179]:

- Elencazione completa dei rischi di frode relativi a una specifica organizzazione economica.
- La valutazione della probabilità che i rischi di frode individuati possano verificarsi.
- La stima dei possibili impatti generati dal verificarsi dei rischi di frode individuati.
- Definizione delle responsabilità del rischio di frode per il sistema di controllo interno e per il revisore.

Il processo di individuazione e valutazione dei rischi di frode è, quindi, particolarmente articolato e presuppone lo svolgimento di attività finalizzate a determinare compiti, responsabilità e procedure da svolgere in fase di risposta al rischio. Le attività appena descritte devono essere eseguite dal revisore sulla base di analisi qualitative e quantitative mediante le quali stimare la probabilità che il rischio di frode possa effettivamente manifestarsi e valutando, contestualmente, l'operatività e l'efficacia del sistema di controllo interno aziendale.

Eseguire un'attività di *fraud risk assessment* è molto complesso soprattutto poiché risulta particolarmente difficile determinare la probabilità che una frode sia effettivamente presente e che un individuo interno o esterno alla realtà aziendale abbia implementato un simile schema.

---

[178] AGNEW H., *Revisioni contabili, battaglia campale per le Big Four della consulenza*, Il Sole 24 ore, 23 maggio 2016.

[179] Il dettaglio dei risultati che è possibile ottenere tramite l'esecuzione del *fraud risk assessment* sono tratti da VONA L.W., *The Fraud Audit. Responding to the Risk of Fraud in Core Business Systems*, John Wiley & Sons, Inc, 2011, p. 69.

Per poter raggiungere tali obiettivi, il revisore opera, tipicamente, mediante due approcci distinti che possono essere implementati congiuntamente o in modo alternativo:

- Analisi dei dati tramite tecniche di *data mining*;
- Analisi del sistema del controllo interno aziendale.

«Common to both approaches is the goal of identifying fraud scenarios and understanding how the fraud scenarios occur in the core business systems. Once identified and understood, the process of building the fraud audit program can commence. Both approaches have their respective strengths and weaknesses. Control identification is widely practiced and utilizes fraud auditing red flags. To the contrary, data mining is a new approach to assessing the likelihood of fraud risk and is presented here as an integral component of the fraud audit program. The approaches can operate simultaneously or separately and are chosen based on the intended use of the risk document[180]*».*

L'analisi del sistema di controllo interno aziendale è un'attività sempre eseguita nell'ambito delle procedure di pianificazione di un incarico di revisione, ciò in quanto consente di definire il livello dei rischi, non solo di frode, presenti a livello aziendale e a livello di singola area di bilancio. Tale approccio è, quindi, sempre seguito nelle attività di *audit* e fornisce importanti informazioni sui punti di debolezza dei controlli e sulla loro effettiva capacità di prevenire o individuare errori o frodi.

Il secondo approccio descritto è, invece, quello di analisi dei dati. Si tratta di una metodologia che verifica la presenza di transazioni e dati coerenti con uno scenario di frode o che, al contrario, confermano l'assenza di una frode. *«(…) data mining is the process of analyzing selected data by finding patterns or anomalies in patterns, then organizing those resulting patterns or anomalies for interpretation*[181]*».* Vona propone dapprima una definizione generale di *data mining*, soffermandosi poi sulle connotazioni che assume nell'ambito del *fraud audit*. In tale contesto, infatti, il *data mining* deve essere percepito come il processo che consente di organizzare e analizzare i dati che derivano dalle transazioni aziendali e gli ulteriori dati di tipo descrittivo disponibili al fine di indentificare eventuali operazioni sospette o anomalie.

La tipologia di analisi dei dati da eseguire dipende dal tipo di rischio di frode identificato durante l'attività di *fraud risk assessment* e, quindi, dallo scenario di frode che deve essere verificato. Se da una *routine* di *data mining* emergono transazioni che corrispondono al rischio di frode

[180] VONA L.W., *The Fraud Audit. Responding to the Risk of Fraud in Core Business Systems*, John Wiley & Sons, Inc, 2011, p. 72

[181] VONA L.W., *The Fraud Audit. Responding to the Risk of Fraud in Core Business Systems*, John Wiley & Sons, Inc, 2011, p. 112.

identificato, la probabilità che si verifichi lo scenario di frode deve essere considerata elevata: in questa ipotesi tutte le transazioni identificate devono essere accuratamente testate per ottenere evidenze in merito allo scenario di frode considerato[182].

Affinché l'analisi dei dati possa risultare attendibile ed efficace, è molto importante valutare l'integrità e la disponibilità dei dati e la possibilità che gli stessi possano essere suddivisi in categorie omogenee. Le analisi devono essere, quindi, eseguite su dati selezionati e mediante funzionalità di ricerca efficaci e adatte a identificare *red flag* in riferimento alla particolare tipologia di scenario di frode che si sta indagando[183].

Altro elemento da considerare quando si esegue una *routine* di *data mining* è il grado di sofisticazione della strategia di occultamento in quanto maggiore è tale livello, maggiore è il numero delle transazioni che è necessario analizzare: si parla di correlazione diretta tra grado di sofisticazione e numero di transazioni che soddisfano il profilo dei dati.

Vona identifica otto step da seguire per poter rendere efficace l'utilizzo delle tecniche di *data mining* ai fini dell'individuazione di una frode[184]:

1. *Understanding the ''what,'' ''where,'' and ''how much'' of data*.
2. *Mapping the data fields to the fraud scenario*.
3. *Understanding the integrity of the data*.
4. *Applying inclusion/exclusion theory*.
5. *Understanding false positives*.
6. *Understanding the ''norm'' of the data*.
7. *Data correlations*.
8. *Entity structures and search routines*.

<u>*Understanding the ''what,'' ''where,'' and ''how much'' of data*</u>

Il revisore deve, innanzitutto, valutare i dati e i campi di cui si compone il database che ha a disposizione per l'esecuzione delle proprie analisi. A tal fine, è molto utile identificare le informazioni di cui si ha bisogno e individuare la loro corrispondenza all'interno dei campi presenti

[182] Cfr. SINGLETON T., SINGLETON A., BOLOGNA J., LINDQUIST R., Fraud Auditing and Forensic Accounting, Third Edition, John Wiley & Sons, Inc, 2006, pp. 152 e ss.

[183] VONA L.W., *The Fraud Audit. Responding to the Risk of Fraud in Core Business Systems*, John Wiley & Sons, Inc, 2011, p. 115; *«For data mining to be effective, audit software search features need to be adapted to coincide with the fraud scenario. Therefore, the starting point is the identification of a fraud scenario followed by the building of a fraud data profile»*.

[184] L'elencazione degli step e la successiva spiegazione presente nei sotto-paragrafi seguenti è tratta da VONA L.W., *The Fraud Audit. Responding to the Risk of Fraud in Core Business Systems*, John Wiley & Sons, Inc, 2011, pp. 117 e ss.

nel database aziendale in modo che gli stessi siano univocamente identificati prima dell'estrazione.

In secondo luogo, è necessario individuare "dove" si trovano le tabelle contenenti i campi dati da estrarre e identificare *primary* e *foreign keys* che collegano le stesse. Questa attività è particolarmente importante in quanto i dati contenuti all'interno delle tabelle possono riferirsi a campi che presentano caratteristiche molto differenti tra loro: identificare la collocazione dei dati assicura che vengano estratte le informazioni che effettivamente si riferiscono allo scenario di frode considerato.

Infine, il revisore deve conoscere la quantità di dati effettivamente elaborata e il numero di rilevazioni presenti.

Mapping the data fields to the fraud scenario

L'attività di *mapping* dei dati deve essere eseguita allo scopo di identificare le correlazioni esistenti tra lo scenario di frode e le informazioni estratte. *«The mapping process includes the identified patterns that would exist in each data element and what type of data exists in each field*[185]*»*.

Understanding the integrity of the data

Il terzo step di esecuzione di *routine* di *data mining* consiste nella selezione dei dati tramite la scrematura delle incongruenze e degli errori che inevitabilmente risultano presenti. Può trattarsi di errori all'interno del database, di campi vuoti, di incongruenze derivanti dai dati di input caricati o da cambiamenti nei sistemi utilizzati. A prescindere da quale sia la causa si tali incongruenze, le stesse devono essere accuratamente isolate ed eliminate al fine di evitare che possano essere causa della rilevazione di "false" anomalie.

Gli errori e le incongruenze rilevate devono essere, comunque, oggetto di separata analisi e valutazione in quanto la loro entità influenza le successive attività di test eseguite. Se il numero di errori e incongruenze risulta di entità lieve, tali elementi potranno essere eliminati all'interno del database. Al contrario se gli errori sono di entità rilevante dovranno formare oggetto di separata valutazione.

[185] VONA L.W., *The Fraud Audit. Responding to the Risk of Fraud in Core Business Systems*, John Wiley & Sons, Inc, 2011, p. 118

Applying inclusion/exclusion theory

Tale approccio consente di eseguire le attività di verifica su gruppi di transazioni suddivisi in categorie tra loro omogenee. In questo modo è possibile facilitare il lavoro di analisi grazie all'utilizzo di un set ridotto di transazioni che possiedono caratteristiche e attributi comuni e che siano correlate allo scenario di frode che si sta indagando. Ad esempio, è possibile utilizzare gruppi di transazioni suddivisi in base ad un criterio territoriale o geografico, classi di transazioni, specifiche categorie di transazioni, costi o ricavi e così via.

Understanding false positives

Le analisi effettuate sui dati possono dar vita ai c.d. falsi positivi. Si tratta di transazioni che risultano tra le anomalie e corrispondono allo scenario di frode indagato ma che, in realtà, non sottendono alcun illecito. È, quindi, molto importante valutare questi elementi e le ragioni per le quali si presentano che possono essere costituite da errori o incongruenze, duplicazione di dati, unione di database differenti, modifiche intervenute nel corso del tempo.

Understanding the ''norm'' of the data

Per poter identificare un'anomalia è fondamentale identificare i valori "normali" da riscontrare all'interno della popolazione oggetto di analisi. La norma può essere definita in termini di numerosità delle transazioni o in termini di valori medio, minimo o massimo: tutti i dati che non rientrano nei *range* ritenuti standard per una determinata popolazione saranno identificati tra le anomalie riscontrate.

Data correlations

L'attività di correlazione dei dati rappresenta un punto fondamentale nel *data mining* in quanto consente di definire i test più efficaci da implementare e di analizzare correttamente i risultati ottenuti. Mediante questa attività vengono, innanzitutto, eseguite analisi di primo livello tramite le quali individuare gli opportuni collegamenti esistenti tra le caratteristiche dello scenario di frode e la struttura aziendale. I dati presenti nel database sono suddivisi in gruppi che consentono di isolare dati mancanti, dati duplicati, dati corrispondenti, modificati e non descrittivi.

Le analisi di secondo livello sono finalizzate ad individuare specifici *pattern* che contraddistinguono un campo di dati e indagare la frequenza con cui si verifica un evento in relazione allo scenario di frode, nonché di valutare l'ordine logico in cui si susseguono le transazioni, i range numerici e le sequenze numeriche che si configurano nei dati, la distinzione

tra errori volontari e involontari. Nelle analisi di secondo livello rientrano anche i controlli sul numero e la tipologia di caratteri presenti all'interno di un campo, la verifica della norma positiva o negativa che contraddistingue uno specifico campo, la presenza di transazioni intenzionalmente suddivise in più parti al fine di eludere un controllo, l'individuazione di rilevazioni eseguite al di fuori del normale orario di attività o da persone differenti da quelle normalmente preposte a quel tipo di attività.

Le analisi di terzo livello sono eseguite, invece, per correlare il modello di frode all'individuo che ha posto in essere lo schema fraudolento. Le transazioni sono, infatti, abbinabili a uno o più soggetti che materialmente hanno potuto agire per implementare materialmente lo schema analizzato. Nella maggior parte dei casi non sarà possibile individuare un singolo soggetto ma un gruppo ristretto di potenziali frodatori all'interno del quale indagare per risalire al vero responsabile.

Infine, le analisi di quarto livello sono implementate allo scopo di determinare l'entità della frode in termini monetari e di correlare tale valore alla struttura dell'entità e all'autore della frode.

Entity structures and search routines

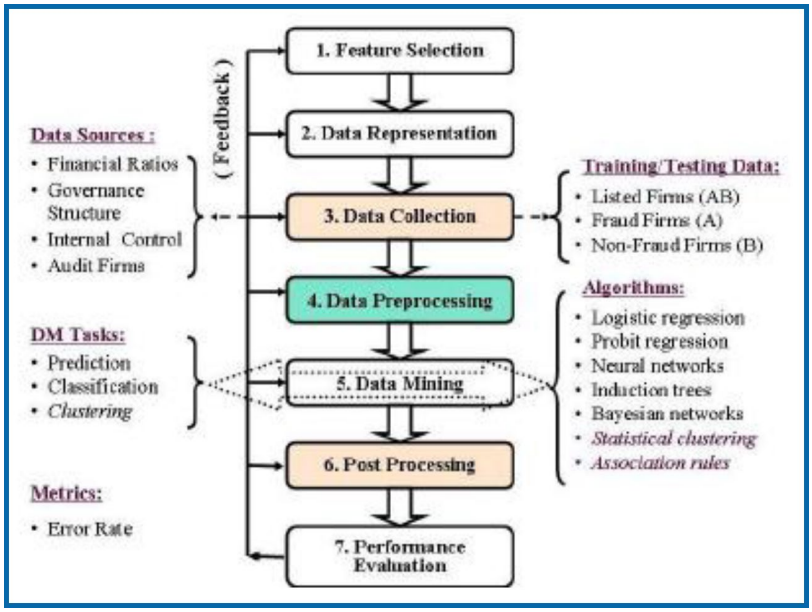
La fase finale del processo consiste nell'implementazione effettiva delle *routine* di ricerca. È fondamentale in questa fase determinare se si intende testare esclusivamente le entità attive o anche quelle inattive. Normalmente le entità inattive, quindi per la quali non sono presenti attività finanziarie (come clienti o fornitori per i quali non sono presenti esposizioni monetarie) vengono escluse dall'analisi poiché potrebbero generare falsi positivi.

Nell'eseguire le attività di ricerca il revisore deve considerare che il frodatore normalmente può agire creando una nuova entità (reale o finta) o assumendo l'identità di un'entità già esistente e inclusa nel business dell'organizzazione economica.

Gli algoritmi di *data mining* utilizzati per l'individuazione delle frodi, seguono il flusso di informazioni tradizionale, suddiviso nelle fasi di selezione, rappresentazione, raccolta e gestione dei dati, pre-elaborazione, data mining, post-elaborazione e valutazione delle prestazioni[186]. Lo schema seguente, riassume il flusso informativo appena descritto.

[186] YUE D., WU X., WANG Y., LI Y., CHU C., *A Review of Data Mining-Based Financial Fraud Detection Research*, International Conference on Wireless Communications, Networking and Mobile Computing, Shanghai, 2007, pp. 5519-5522.

Figura 21 - Processo di elaborazione data mining



Fonte: YUE D., WU X., WANG Y., LI Y., CHU C., A Review of Data Mining-Based Financial Fraud Detection Research, International Conference on Wireless Communications, Networking and Mobile Computing, Shanghai, 2007, pp. 5519-5522.

Come si evince dal precedente grafico, gli algoritmi associati al *data mining* sono molteplici e utilizzati come tecniche in grado di supportare il revisore nell'analisi e nella valutazione di grandi volumi di dati. I processi di *prediction*, *classification* e *clustering* eseguiti congiuntamente alle tecniche di data mining conferiscono al revisore l'opportunità di identificare tutti gli elementi che potenzialmente possono sottendere la presenza di una frode.

2.2.3 Forensic analytics tools

I controlli e le analisi eseguite in ambito *Forensic* sono supportati dall'utilizzo di software che impiegano tecniche di *data mining* per poter individuare anomalie, modelli e *trend* insoliti nelle popolazioni oggetto di indagine. L'uso di software di analisi è favorito dalla presenza di dati e informazioni in formato digitale e dall'esistenza di sistemi informatici che rappresentano *data warehouses* in cui confluiscono informazioni di tipo finanziario, contabile, provenienti dal reparto marketing e dalle attività di gestione del personale[187].

[187] GOLDEN T.W., SKALAK S. L., CLAYTON M.M., *A guide to forensic accounting investigation*, John Wiley & Sons, Inc., Hoboken, New Jersey, 2006, p. 385; Cfr. ALBRECHT W.S., ALBRECHT C.O., ALBRECHT C.C., ZIMBELMAN M.F., *Fraud Examination*, Fourth edition, South-Western Cengage Learning, 2011, p. 169.

«Data analysis is often the fastest and most effective tool at the forensic accounting investigator's disposal for gathering much of the evidential material needed to support findings[188]». Non solo l'analisi dei dati consente di svolgere il lavoro di *forensic accounting* in modo più veloce ed efficace, ma anche di analizzare dati, soprattutto di tipo non finanziario, che possono costituire un importante punto di partenza per le attività di investigazione.

L'integrazione del *data mining* nelle attività di *forensic accounting investigation* comporta numerosi vantaggi connessi alla possibilità di analizzare ampi volumi di dati, identificare *trend*, individuare dati e documenti che necessitano di una *review* più approfondita[189]. Contestualmente, l'utilizzo di software specializzati rende il lavoro più conveniente, in termini di tempi e costi, e completo grazie alla possibilità di analizzare il 100% delle popolazioni oggetto di verifica.

L'utilizzo di tecniche di analisi di *data mining* e di software specializzati deve essere, comunque, accompagnato dall'esecuzione di procedure "tradizionali" costituite da attività di ispezione documentale, indagini e interviste.

L'importanza dell'utilizzo delle nuove tecnologie nell'attività forense deriva anche dal fatto che il frodatore deve necessariamente utilizzare, anche se solo parzialmente, il sistema informatico aziendale per poter occultare la propria attività – senza considerare che sta sempre di più crescendo il numero di frodi appartenenti alla categoria del *cybercrime*. *«Tech-savvy fraudsters often make use of email and instant messaging, they access networks, they create and manipulate all sorts of files, and they work with databases and general ledger systems. They may also use printing, scanning, and fax technology to create all types of fictitious documents, many of which have the look and feel of the real thing[190]»*.

I file archiviati all'interno dei database e delle reti aziendali, sono contraddistinti dalla presenza di metadati che consentono di identificare le principali informazioni relative al loro contenuto, all'autore del documento e all'organizzazione di appartenenza. Molti sistemi informatici, inoltre, generano e archiviano una grande quantità di informazioni relative al "traffico dati", al momento

---

[188] GOLDEN T.W., SKALAK S. L., CLAYTON M.M., *A guide to forensic accounting investigation*, John Wiley & Sons, Inc., Hoboken, New Jersey, 2006, p. 386.

[189] Cfr. ANASTASI J., The new forensics. *Investigating Corporate Fraud and the Theft of Intellectual Property*, John Wiley & Sons, Inc., Hoboken, New Jersey, 2003, p. 149.

[190] GOLDEN T.W., SKALAK S. L., CLAYTON M.M., *A guide to forensic accounting investigation*, John Wiley & Sons, Inc., Hoboken, New Jersey, 2006, p. 388; gli autori mettono in evidenza come oggi le attività aziendali presentino necessariamente una componente di tipo informatico e digitale e l'interazione con i sistemi informativi aziendali.

in cui vengono eseguite determinate azioni all'interno di un computer o di una rete e agli utenti che hanno svolto tali attività[191].

«Many types of traffic data may be available to the forensic accounting investigator. For example, most general ledger systems can be configured to record the user name associated with the most recent change to any value in the system. Some systems allow users to record the user names responsible for every change to a value over time. Similarly, many e-mail systems retain information about the dates and times associated with transmissions of each e-mail and attachment. Some of these systems also record the date and time of message deletions. Operating systems may maintain dates associated with accessing, moving, or deleting files. All of this information can be useful in the course of an investigation[192]».

Golden (et al.) mettono, quindi, in evidenza come il *forensic accounting investigator* sia in grado di trarre una ingente quantità di informazioni dai dati e dalle informazioni archiviate all'interno del sistema informatico aziendale. L'analisi dei messaggi e delle email può, inoltre, fornire importanti indicazioni relative allo stato di soddisfazione o alla presenza di malessere nel/nei dipendenti aziendali, informazioni particolarmente rilevanti per poter individuare le giustificazioni e gli incentivi che hanno spinto un individuo a commettere una frode.

2.2.4 Computer Assisted Auditing Tools and Techniques

I *Computer Assisted Auditing Tools and Techniques,* identificati generalmente con l'acronimo di CAATT, costituiscono l'insieme delle tecniche, dei tool e dei software che utilizzano l'intelligenza artificiale al fine di automatizzare procedure e funzioni tipiche delle attività di *audit*. I CAATT sono parte degli strumenti utilizzati nelle analisi forensi e si identificano nelle tecniche di *audit computer-assisted* definite dai principi di revisione.

Grazie a tali strumenti le procedure di revisione possono contare su analisi estese a interi set di dati in grado di fornire evidenza di anomalie, rischi specifici e risultati di verifiche mirate. La famiglia dei CAATT è particolarmente vasta in quanto al suo interno rientrano differenti tipologie di strumenti che variano dai semplici file excel utilizzati per lo svolgimento di analisi, fino a sofisticati software dotati di intelligenza artificiale.

---

[191] ANASTASI J., The new forensics. Investigating Corporate Fraud and the Theft of Intellectual Property, John Wiley & Sons, Inc., Hoboken, New Jersey, 2003, pp. 18 e ss.

[192] GOLDEN T.W., SKALAK S. L., CLAYTON M.M., *A guide to forensic accounting investigation*, John Wiley & Sons, Inc., Hoboken, New Jersey, 2006, p. 390.

Grazie all'utilizzo dei *tool*, i revisori hanno la possibilità di ottenere analisi molto accurate ed esaustive potendo, tra l'altro, utilizzare informazioni diversificate e fonti eterogenee di dati. In base al proprio giudizio professionale, il revisore può configurare i dati e programmare test mirati in grado di rispondere adeguatamente alla tipologia di rischi identificata.

In tal senso, l'utilizzo dei CAATT consente di incrementare notevolmente il livello di individuazione delle frodi presenti in bilancio: *«The effective implementation and use of CAATT can help auditors in exercising not only a greater level of due diligence and due professional care, but more importantly, greater fraud detection during various audit activities*[193]*»*.

L'utilizzo dei CAATT è divenuto sempre più importante nel corso del tempo, all'aumentare dell'impiego dei sistemi informatici per la gestione dei processi aziendali, infatti, si sono presentati al revisore nuovi rischi e nuovi possibili scenari di frode.

L'impiego di software finalizzati all'individuazione delle frodi risulta particolarmente efficace per identificare i fenomeni di alterazione dell'informativa finanziaria: le procedure di revisione tradizionali, infatti, non sono in grado di eseguire controlli completi e verifiche accurate sui processi che coinvolgono funzioni IT e procedure digitali.

«This means that transparent financial statement reviews and business operations are the most critical and important steps in building confidence among the stakeholders and decreasing instances of fraud[194]*».*

Solo grazie all'utilizzo di sistemi CAATT è possibile analizzare in breve tempo ampi volumi di dati e interi set di transazioni aziendali in modo che il revisore possa identificare anomalie e individuare le operazioni e le rilevazioni eseguite per occultare una frode. Le anomalie e i risultati che emergono dai test devono essere, comunque, opportunamente valutati e interpretati dal revisore in quanto l'intelligenza artificiale non deve intendersi come strumento sostitutivo dell'apporto intellettuale umano e dell'esercizio del giudizio professionale. Le nuove tecnologie e l'intelligenza artificiale devono essere, quindi, sempre intese come strumenti posti a supporto del lavoro svolto dal revisore, fornendo un importante sostegno nella fase di pianificazione delle attività, in particolare grazie alla facilitazione dell'individuazione delle aree di bilancio che presentano maggiori e più alti rischi.

Le tecniche di analisi dei dati utilizzate nei CAATT sono molteplici, le principali possono essere così riassunte:

---

[193] S. AGHILI, *Fraud Auditing Using CAATT. A Manual for Auditors and Forensic Accountants to Detect Organizational Fraud*, CRC Press, 2019, p. 141.

[194] S. AGHILI, *Fraud Auditing Using CAATT. A Manual for Auditors and Forensic Accountants to Detect Organizational Fraud*, CRC Press, 2019, p. 144.

- Unione: tecnica utilizzata per unire due *file* differenti in uno solo.
- Duplicazione: tecnica di individuazione di transazioni, valori o item duplicati.
- *Gaps*: tecnica che consente di identificare *item*, serie o sequenze mancanti all'interno di una popolazione di dati.
- Ordinamento: ordinamento dei dati in senso ascendente o decrescente.
- Esportazione: funzione che consente di esportare dati in specifici formati.
- Legge di *Benford*: consente di individuare duplicazioni anomale di numeri e cifre.
- *Aging*: determinazione dell'anzianità di una transazione.
- Campionamento: estrazione di un campione statistico da una popolazione di riferimento.
- Stratificazione: possibilità di suddividere una popolazione di riferimento in intervalli aventi caratteristiche omogenee.
- *Summarize*: riepilogo di dati in specifiche categorie.
- Calcoli statistici: esecuzione di calcoli statistici come la media e la varianza.
- *Merge*: unione di *file* aventi i medesimi campi all'interno di un database o di altro supporto informatico.
- *Cross tabulate*: ordinamento dei dati in righe e colonne al fine di indagarne specifiche caratteristiche.

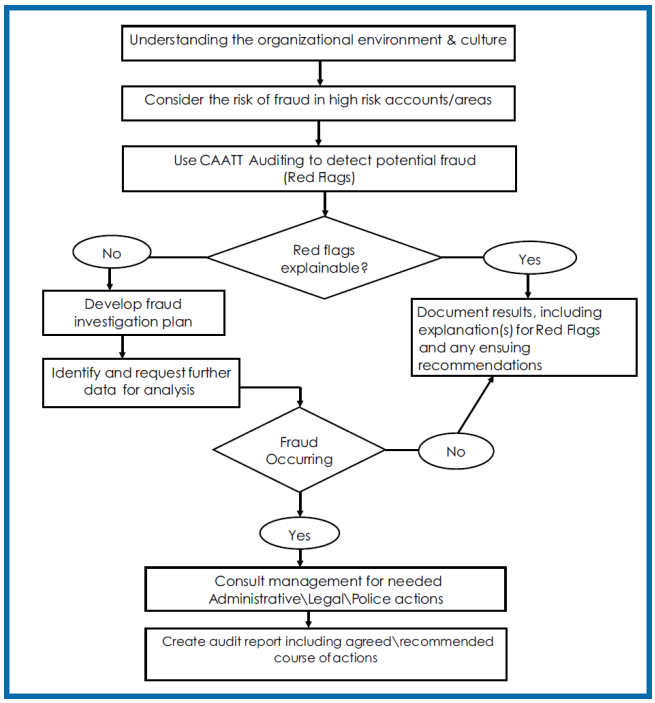
Software coma *Idea*, *ACL* e *Active Data* possiedono la maggior parte delle funzioni appena descritte, mentre altre tipologie di *tool* non dispongono di un set così ampio di test.

In fase di pianificazione di un incarico di revisione, è fondamentale acquisire una conoscenza approfondita dell'azienda e dell'ambiente in cui essa opera al fine di formulare una prima valutazione delle possibili aree di rischio. Sulla base delle informazioni acquisite in merito all'azienda, all'attività svolta e ai principali processi interni, il revisore è, inoltre, in grado di stabilire se siano o meno presenti dei rischi di frode e quali sono le aree e le poste di bilancio che possono essere colpite da tali rischi. È a questo punto che i CAATT vengono utilizzati per poter individuare eventuali segnali di frode e raccogliere indizi di anomalie e *red flags* che dovranno essere successivamente analizzati e investigati sulla base di un preciso piano di revisione se non giustificabili. Queste tecniche riducono notevolmente i tempi di esecuzione delle attività consentendo di massimizzare i risultati ottenuti dal lavoro.

Il seguente grafico consente di identificare tutti gli step di cui si compone il ciclo di investigazione delle frodi nell'ambito delle attività di audit e il ruolo chiave svolto dai CAATT nell'individuazione dei *red flags* su cui basare la successiva attività di analisi.

Osservando il grafico è possibile notare come, in più fasi del processo di investigazione descritto, il revisore è tenuto ad analizzare le anomalie rilevate tramite le attività di test e verificare se le stesse siano effettivamente ascrivibili a una frode. È possibile, infatti, che i *red flag* possano avere una giustificazione differente e derivare da altre circostanze o da errori non intenzionali. Ciò che è fondamentale ai fini della conclusione delle attività di investigazione è la possibilità di individuare una spiegazione chiara del perché siano state riscontrate le anomalie oggetto di analisi e che le conclusioni raggiunte siano adeguatamente documentate. Nel caso in cui i segnali di frode non possano essere supportati da una spiegazione ragionevole, sarà fondamentale identificare gli ulteriori dati che dovranno essere sottoposti a verifica e che si considerano utili per poter individuare la frode sospetta.

Figura 22 - Fraud investigation using CAATT



Fonte: S. AGHILI, Fraud Auditing Using CAATT. A Manual for Auditors and Forensic Accountants to Detect Organizational Fraud, CRC Press, 2019, p. 150.

Se dai dati analizzati il revisore è in grado di individuare l'effettiva presenza di una frode, egli dovrà coinvolgere il management della società per intraprendere le dovute azioni di tipo legale e amministrative necessarie. Anche in tale ipotesi è fondamentale che il revisore documenti adeguatamente e in modo approfondito le analisi svolte, gli elementi probativi raccolti e le conclusioni raggiunte.

Il ciclo di investigazione delle frodi appena descritto, si basa sull'individuazione e l'analisi dei *red flags* che non sono altro che sintomi o segnali della possibile presenza di frodi. Tali elementi sono di fondamentale importanza per il revisore in quanto la frode è accuratamente occultata da parte del frodatore: l'unica possibile modalità di detenzione della frode risiede, quindi, nella corretta individuazione e analisi di tali anomalie. *«Fraud perpetrators are often savvy enough to hide their tracks from auditors aiming to detect the existence of fraud. As such, auditors must watch for fraud symptoms or red flags in the fraud identification process*[195]*».*

I *red flags* sono elementi che consentono di segnalare al revisore la possibile presenza di frodi in quanto indicano la potenziale presenza di uno schema di frode. I segnali di frode hanno un diverso peso e significato che varia anche in base alle altre anomalie a cui essi sono associati e sottendono la presenza di specifiche strategie di occultamento che il revisore sarà tenuto a verificare in quanto la presenza di red flags non implica necessariamente che sia presente uno scenario di frode.

2.3 Journal entries test e individuazione delle frodi

2.3.1 Journal Entries Test

Le frodi che afferiscono alla categoria della falsa informativa finanziaria sono, normalmente, riflesse nelle transazioni riportate all'interno del libro giornale aziendale. Per poter alterare i dati di bilancio, infatti, il frodatore dovrà agire manipolando le rilevazioni contabili al fine di registrare operazioni fittizie o alterate.

Per questo motivo, una delle maggiori tecniche impiegate nell'ambito delle attività di individuazione di questa tipologia di frode risulta essere costituita dai Journal Entries Test.

Questa tipologia di test presuppone che siano identificati e delineati i possibili scenari di frode e i conseguenti schemi attuati dal frodatore: *«Establishing a fraud risk structure is the starting point for identifying the fraud scenarios that can occur through manipulation of journal entries. In other words, how schemes are structured within an entity's accounting system*[196]*».*

---

[195] S. AGHILI, *Fraud Auditing Using CAATT. A Manual for Auditors and Forensic Accountants to Detect Organizational Fraud*, CRC Press, 2019, p. 155; l'autore sottolinea come i red flags siano indispensabili in quanto consentono di accrescere notevolmente le possibilità di individuazione di una frode all'interno del processo di audit.

[196] VONA L.W., *The Fraud Audit. Responding to the Risk of Fraud in Core Business Systems*, John Wiley & Sons, Inc, 2011, p. 253.

In base a quanto stabilito dal Public Company Accounting Oversight Board (PCAOB), le transazioni aziendali possono essere suddivise in tre categorie. La prima si riferisce a tutte le transazioni di tipo routinario che derivano dal normale svolgimento delle attività aziendali. La seconda categoria racchiude, invece, tutte le transazioni non routinarie che sono svolte soltanto in alcuni periodi dell'esercizio sociale, come l'inventario di magazzino e le scritture di assestamento. Infine, l'ultima categoria comprende le stime effettuate dal management in relazione a determinate poste di bilancio.

In relazione alla tipologia di transazioni considerate e con riferimento alle particolari caratteristiche dell'azienda e del suo sistema informativo è possibile definire quali test eseguire sul libro giornale.

Innanzitutto, è fondamentale partire dalla conoscenza dei controlli che operano sulle rilevazioni contabili e che dovrebbero garantire la corretta rilevazione delle operazioni all'interno del libro giornale. Tramite l'individuazione dei punti di debolezza del sistema di controllo interno è possibile stabilire quali schemi di frode presentano maggiori probabilità di implementazione.

«An understanding of the control points for journal entries is critical. These control points occur:

- *At origination: A control that creates a basis for a journal entry, including criteria, rate calculations, identification of transactions, and estimates.*
- *With authorization: The approval process in place for the processing, recording, and documentation of a journal entry.*
- *Through processing: The steps from initiation through recording of the journal entry.*
- *When recording: Posting of the journal entry into the general ledger.*
- *Documentation: Creating and retaining documentation supporting a journal entry*[197]*».*

Dalla descrizione appena enunciata, si evince chiaramente come i controlli possano agire lungo molteplici direzioni a partire dalla definizione dei criteri di calcolo, di identificazione e di stima correlati a una transazione e fino a ricomprendere tutti i processi di rilevazione e di documentazione delle registrazioni eseguite.

I rischi di frode correlati alle rilevazioni presenti nel libro giornale si differenziano in base alla tipologia di transazione considerata. Vona fornisce una descrizione dettagliata della tipologia di rischio associata a ciascuna categoria di transazioni[198]:

---

[197] VONA L.W., *The Fraud Audit. Responding to the Risk of Fraud in Core Business Systems*, John Wiley & Sons, Inc, 2011, p. 254.

[198] La descrizione delle tipologie di rischio è tratta da VONA L.W., *The Fraud Audit. Responding to the Risk of Fraud in Core Business Systems*, John Wiley & Sons, Inc, 2011, pp. 254 e ss.

- Rilevazioni contabili: le rilevazioni contabili eseguite giornalmente e in modo routinario possono contenere transazioni fittizie o importi di ammontare alterato.
- *Adjusting*: rilevazioni eseguite per correggere o modificare stime o registrazioni effettuate in precedenza. In tale ipotesi le rilevazioni di *adjusting* potrebbero essere eseguite da soggetti differenti dai primi allo scopo di occultare uno schema di frode.
- Riclassificazione: si tratta di rilevazioni eseguite per riclassificare una transazione oggetto di una registrazione precedente al fine di trasferire i relativi importi in conti differenti. Anche in tale ipotesi, la rilevazione potrebbe essere nata allo scopo di alterare intenzionalmente i dati di bilancio.
- Consolidamento: le rilevazioni di questa categoria si riferiscono alle registrazioni eseguite per rettificare o movimentare conti interaziendali che potrebbero essere oggetto di frodi avvenute sfruttando i rapporti con parti correlate.
- Storno: rilevazioni eseguite per stornare o rettificare rilevazioni di fine periodo.

Il programma di revisione deve essere definito, quindi, tenendo in considerazione le differenti categorie di transazioni che possono essere contenute all'interno di un libro giornale e le molteplici tipologie di transazioni fraudolente che lo stesso può contenere.

Tra le più comuni forme di alterazione delle rilevazioni contabili, è sicuramente presente la sovrastima o sottostima dei valori di bilancio finalizzata a innalzare il livello delle attività o del risultato conseguito dall'azienda al termine dell'esercizio o a comprimere tali grandezze. Questo tipo di frode può incidere su molteplici poste di bilancio: immobilizzazioni, ricavi, costi, debiti, crediti.

Altri elementi da analizzare con particolare attenzione sono costituiti dalla data e dell'orario in cui le rilevazioni sono eseguite, ciò allo scopo di verificare se siano presenti registrazioni eseguite in giorni di chiusura dell'attività o al di fuori del normale orario di lavoro.

Rilevazioni che possono costituire facilmente oggetto di frode sono, inoltre, quelle eseguite al termine dell'esercizio o di un periodo intermedio, in particolar modo in concomitanza alla predisposizione dei bilanci consuntivi o previsionali e per gonfiare il risultato di esercizio realizzato: *«Management is pressured to meet analysts' forecasts for earnings and so fictitiously inflate profits with endof-period entries or adjustments*[199]*».*

[199] VONA L.W., *The Fraud Audit. Responding to the Risk of Fraud in Core Business Systems*, John Wiley & Sons, Inc, 2011, p. 257.

Il rischio di frode aumenta, inoltre, in presenza di rilevazioni contabili eseguite manualmente o da dipendenti aziendali che sono posti ai vertici della scala gerarchica: in tali ipotesi le possibilità di eseguire forzature e di aggirare i controlli sono molto più elevate.

L'individuazione di frodi presenti all'interno del libro giornale è un processo che Vona suddivide in molteplici fasi. La prima di queste fasi è rappresentata dalla considerazione di quanto prescritto dalla teoria del triandolo delle frodi in relazione agli incentivi, alle pressioni e alle opportunità che contraddistinguono la presenza di una frode. Nel caso delle frodi relative alla falsa informativa finanziaria, l'opportunità è sempre rappresentata dalla possibilità di aggirare i sistemi di controllo interno al fine di alterare le rilevazioni contabili[200].

2.3.2 MindBridge

MindBridge rientra tra i *software* di revisione più avanzati nel campo dell'intelligenza artificiale applicata alle attività di *audit*.

Il *software* è pensato per supportare le attività dei professionisti e delle società di consulenza in quattro principali settori di riferimento[201]:

- *Audit & Assurance*;
- *Enterprise*;
- *Government*;
- *Financial services*.

I punti di forza del sistema sono caratterizzati dalla possibilità di identificare rischi e frodi tramite l'analisi automatizzata di intere popolazioni di dati grazie all'uso dell'intelligenza artificiale e del *machine learning*. Con l'analisi di set di dati completi è possibile ottenere un elevato livello di accuratezza dei risultati raggiunti e delle eventuali frodi e anomalie riscontrate dall'analisi, eliminando completamente i rischi di errore correlati alle procedure di campionamento[202].

L'*Intelligent automation* utilizzata dal software non è espressione di un unico algoritmo di analisi, ma la combinazione di molteplici di essi, il c.d. *Ensemble AI* finalizzato a creare un dettagliato

[200] Cfr. GOLDEN T.W., SKALAK S. L., CLAYTON M.M., *A guide to forensic accounting investigation*, John Wiley & Sons, Inc., Hoboken, New Jersey, 2006, p. 28.

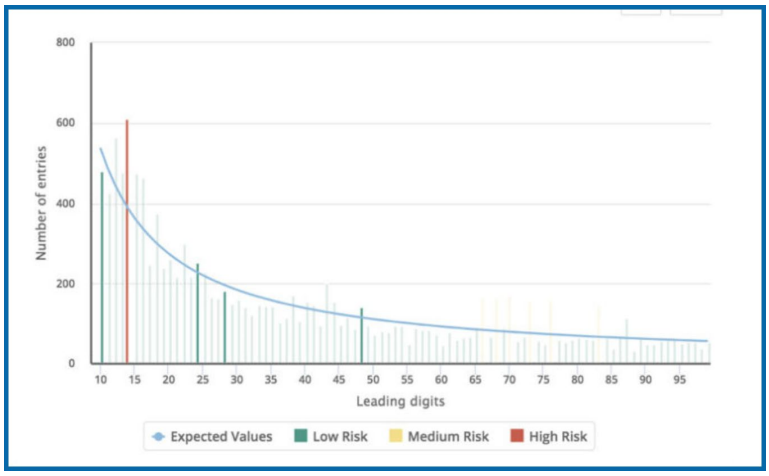
[201] https://www.mindbridge.ai

[202] JOHANSSON E., SUTINEN K., LASSILA J., LANG V., MARTIKAINEN M., LEHNER O.M., *Regtech-a necessary tool to keep up with compliance and regulatory changes?*, ACRN Journal of Finance and Risk Perspectives 8, Special Issue Digital Accounting, 2019, 71-85, p. 78.

modello di *risk assessment*. L'attività di analisi del rischio è eseguita combinando i risultati ottenuti dall'utilizzo congiunto di 28 funzioni denominate "*control points*".

Sulla base di questa tipologia di analisi, il software è in grado di effettuare controllare tutte le transazioni contenute nei dati caricati a sistema che è possibile estrarre anche direttamente dai sistemi aziendali. Le transazioni sono analizzate contestualmente ai conti mediante algoritmi di calcolo avanzati che confrontano i dati con quelli già contenuti all'interno del database del sistema in un'ottica di apprendimento continuo. Le transazioni così analizzate vengono classificate in base al livello di rischio stimato che tiene conto del livello di significatività calcolato e della presenza di anomalie riscontrate, ad esempio, tramite l'applicazione della legge di *Benford* per la valutazione della frequenza della prima cifra[203].

Figura 23 - Applicazione della Legge di Benford



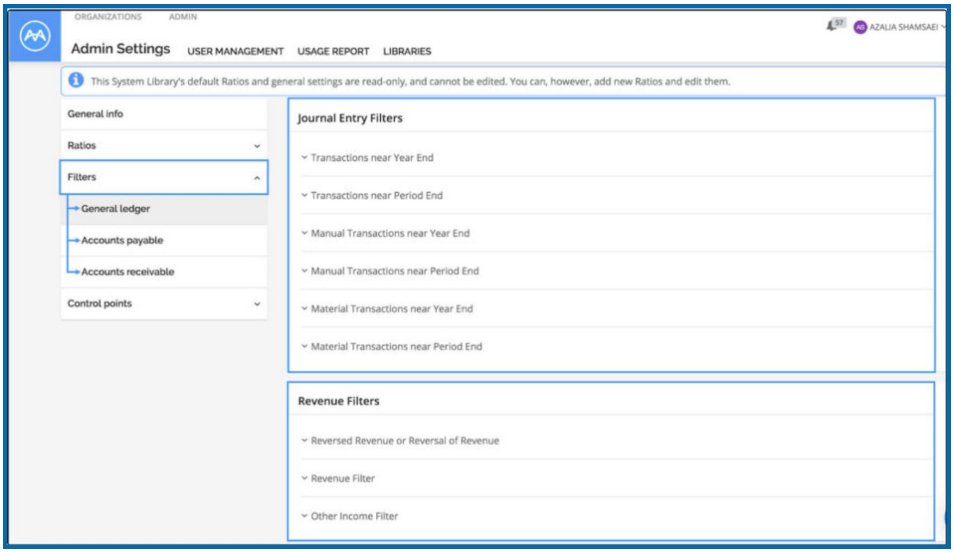
Fonte: MindBridge. New Ai Auditor release: August 2019. https://www.mindbridge.ai/ai-auditor-releaseaugust-2019/

In questo modo, il software è in grado di segnalare tutte le operazioni o gli elementi che necessitano di maggiori approfondimenti e analisi maggiormente accurate che consentano di verificare se i *red flag* rappresentino effettive anomalie presenti nel sistema aziendale.

Ai Auditor di *MindBridge* è dotato di funzioni avanzate che consentono di eseguire analisi personalizzate sulla base del settore di appartenenza della società sottoposta a revisione e di focalizzare l'attenzione esclusivamente su specifici set di transazioni o dati. Questa funzionalità avanzata è gestita mediante un sistema di filtri da applicare all'analisi che è possibile differenziare in base al cliente oggetto dell'analisi e personalizzare in base alle specifiche esigenze.

[203] NUNES T., LEITE J., PEDROSA I., *Intelligent Process Automation: An Overview over the Future of Auditing*, 2020 15th Iberian Conference on Information Systems and Technologies (CISTI), 24 – 27 June 2020, Seville, Spain, p. 4.

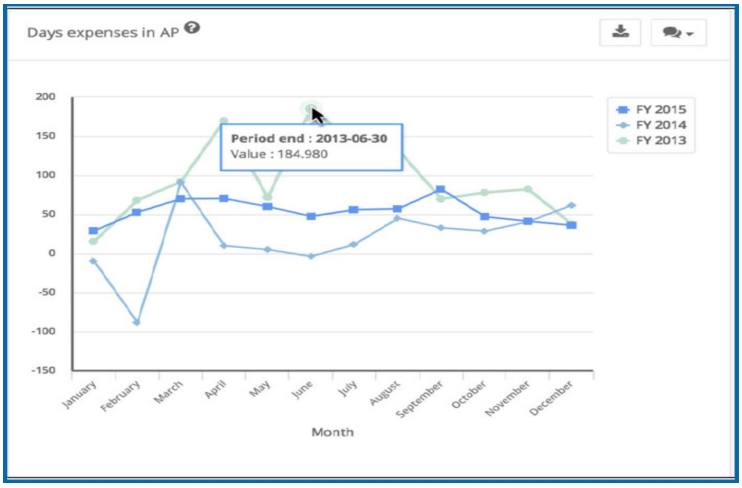
Figura 24 - Ai Auditor - MindBridge



Fonte: MindBridge. New Ai Auditor release: August 2019. https://www.mindbridge.ai/ai-auditor-releaseaugust-2019/

Il software consente anche di creare indicatori personalizzati mediante una funzione denominata *Ratio Builder* che, non solo calcola l'indicatore configurato dall'utente, ma genera anche il relativo grafico di riferimento.

Figura 25 - Creazione indicatori personalizzati



Fonte: MindBridge. New Ai Auditor release: August 2019. https://www.mindbridge.ai/ai-auditor-releaseaugust-2019/

2.3.3 Inflo

Tra i principali software utilizzati per lo svolgimento delle attività di revisione e per le attività di individuazione delle frodi di bilancio è presente *Inflo.* Il software, molto diffuso in Inghilterra, negli Stati Uniti e in Australia, si compone di molteplici moduli che rispondono alle differenti esigenze connesse all'esecuzione di un incarico di revisione.

Tra i moduli presenti, *Inflo Ingest* consente alla società cliente sottoposta a revisione di trasferire direttamente i dati dai propri sistemi informatici al *software*. Tramite appositi connettori, infatti, il revisore ha la possibilità di acquisire esclusivamente i dati necessari che il sistema sottopone a una verifica automatica di validità. I dati ottenuti sono, quindi, già puliti e non necessitano di ulteriori attività di scrematura.

La funzione di trasferimento dei dati è utilizzata sia per l'import del *Trial Balance*, sia per il caricamento del libro giornale. Il software è in grado di riconoscere e gestire i dati provenienti da un set predeterminato di sistemi di contabilità, identificando automaticamente le strutture che essi impiegano per la gestione dei dati e il piano dei conti utilizzato.

I dati così importati possono essere così elaborati e utilizzati per lo svolgimento delle molteplici procedure rese disponibili dall'utilizzo degli altri moduli di cui si compone il software.

In particolare, il modulo *Inflo Detect* utilizza i dati provenienti dal libro giornale e i dati importati tramite il bilancio di verifica per eseguire test automatici finalizzati all'individuazione delle frodi. Il sistema, infatti, è in grado di individuare in modo istantaneo le transazioni che presentano caratteristiche inusuali e anomalie all'interno della popolazione. Il modulo consente, inoltre, di identificare, tramite l'elaborazione dei dati importati, i principali segnali e indicatori di frode calcolando la probabilità che siano presenti forme di *management override of controls* o problemi, inefficienze e debolezze nei processi e nelle procedure di controllo.

Le verifiche appena descritte sono svolte dal software mediante *InfloHI – Inflo Hybrid Intelligence* basata sull'utilizzo congiunto delle nuove tecnologie e dell'intelligenza umana ai fini della massimizzazione dei risultati. L' *Hybrid Intelligence* sfrutta l'intelligenza artificiale, forme di *data analytics* avanzate, *machine learning*, *process mining* e *predictive analytics* per verificare e analizzare ampi volumi di transazioni in pochissimi secondi[204].

Il modulo *Inflo Metrics*, inoltre, consente di generare in modo del tutto automatico indici di bilancio, indicatori di performance e matrici, confrontando i risultati ottenuti con gli standard specifici del settore di riferimento.

[204] Per approfondimenti https://inflosoftware.com.

CAPITOLO 3 – Risultati della ricerca applicativa: ERA e Revisya

3.1 L'investimento in innovazione tecnologica di RSM

3.1.1 Introduzione

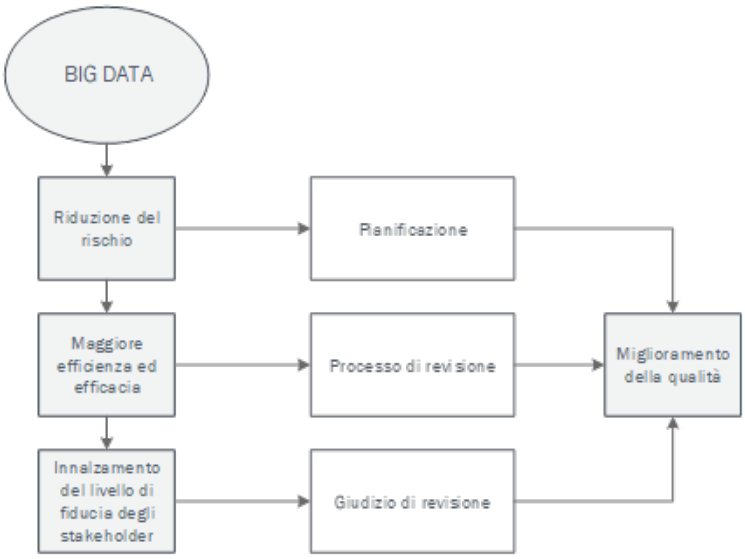
Il mio percorso di ricerca è nato con l'obiettivo di individuare e progettare strumenti e tecniche innovative da impiegare nell'attività di audit e revisione contabile al fine di migliorare l'efficienza e l'efficacia delle procedure e delle attività di revisione.

John Verver, vice presidente della società ACL che si occupa di sviluppo tecnologico dell'attività di audit, individua i tre obiettivi perseguiti dalle società di revisione che stanno sempre di più investendo in nuove tecnologie[205]:

- Miglioramento della qualità della revisione;
- Riduzione del rischio;
- Accrescimento dell'efficacia e dell'efficienza dell'attività.

Proprio su questi tre elementi si basa l'attività di ricerca condotta i cui obiettivi di partenza possono essere riassunti nel seguente grafico.

Figura 26 - Obiettivi del progetto di ricerca



[205] WHITHOUSE T., *Auditing in the Era of Big Data*, Compliance Week, Aprile 2014; Cfr. D'ALESSIO R., ANTONELLI V., BOZZA E., *Principi di Auditing. Concetti, modelli, metodologie, applicazioni*, Volume I, Edises, 2017, pp. 165 e ss.

Il grafico mostra come il miglioramento della qualità di un incarico di revisione può essere raggiunto se è possibile ottenere una riduzione del rischio di incarico stimato in fase di pianificazione e, contestualmente, impiegare strumenti di lavoro in grado di rendere più efficiente ed efficace il lavoro svolto. Il miglioramento del livello qualitativo dell'attività svolta consente di ottenere come risultato un forte aumento della fiducia riposta dagli utilizzatori di bilancio nel giudizio espresso dal revisore.

Tenendo conto delle considerazioni svolte nel precedente paragrafo 2.1.4, gli obiettivi appena delineati non possono che essere raggiunti tramite la progettazione di strumenti innovativi da utilizzare nello svolgimento dell'attività di revisione e sulla base dei quali modificare le procedure e i processi generalmente eseguiti. L'attività di ricerca teorica effettuata nel corso degli anni di dottorato non poteva che essere, quindi, accompagnata da un'esperienza di ricerca applicativa che mi consentisse di conoscere da vicino e testare i processi di digitalizzazione delle procedure e delle funzioni di revisione.

È con riferimento a tali presupposti che è iniziata la mia attività di collaborazione al progetto sviluppato da RSM Società di Revisione e Organizzazione Contabile S.p.A. dal quale sono nati due software di revisione: ERA (Effective Revolutionary Audit) e Revisya.

RSM Società di Revisione e Organizzazione Contabile S.p.A. è membro di RSM, sesto network internazionale nell'ambito delle società specializzate in revisione, organizzazione contabile e consulenza fiscale, societaria e finanziaria, che opera in oltre 120 paesi del mondo.

RSM Italy, da sempre all'avanguardia con riferimento all'innovazione e alle nuove tecnologie, ha deciso di investire, nel corso degli ultimi anni, nel digitale e nell'intelligenza aumentata, al fine di realizzare un software in grado di svolgere in modo automatico molte delle funzioni operative tipiche di un processo di revisione, consentendo al revisore di occuparsi in modo prevalente delle attività valutative e di completamento dell'incarico. Il software è nato, quindi, al fine di portare le nuove tecnologie al servizio del revisore fornendogli l'opportunità di valutare e verificare quantità di dati estremamente superiori a quanto accaduto fino ad ora con il fine ultimo di creare, tramite le attività di audit, valore aggiunto per i clienti.

RSM ha deciso di implementare questo progetto anche allo scopo di dar vita ad un software che fosse realizzato sulla base delle specifiche esigenze dettate dalla normativa e dai principi contabili nazionali, dall'utilizzo del sistema di fatturazione elettronica e dalla maggiore incidenza di frodi depressive e non espansive del reddito nel contesto delle PMI italiane.

Nei seguenti paragrafi sarà presentato esclusivamente il software Revisya, brevettato e commercializzato, mentre non si entrerà nel dettaglio di ERA in quanto utilizzato internamente da RSM e contenente le carte di lavoro e la metodologia di revisione internazionale della società.

3.1.2 Caratteristiche distintive e *plus* di Revisya

Revisya è la versione del software pensata per incontrare le esigenze dei professionisti italiani e delle società di revisione di piccole e medie dimensioni che necessitano di sistemi in grado di ottimizzare il lavoro e le attività svolte e, contestualmente, guidare l'utente nell'ambito dell'intero processo di revisione. Nella prospettiva di raggiungere i *deliverable* appena descritti, la progettazione di Revisya si è mossa lungo le seguenti direzioni:

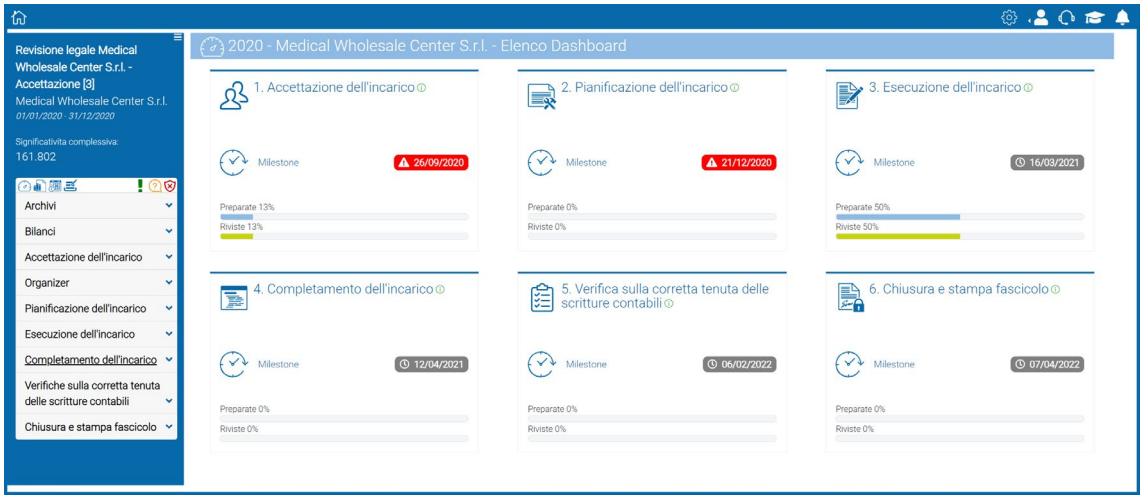
- Automazione dei processi;
- Impiego dell'intelligenza artificiale per il potenziamento delle attività ad alto valore aggiunto;
- Impiego di processi automatizzati e dell'intelligenza aumentata per creare una struttura logica di "flusso".

I primi due punti soprariportati saranno ampiamente trattati nell'ambito dei successivi paragrafi, ci soffermeremo, quindi, sull'analisi del terzo *deliverable* elencato.

La creazione di una struttura logica di "flusso", ottenuta mediante l'utilizzo dell'intelligenza aumentata e l'impiego di processi automatizzati, è stata pensata al fine di rendere il *software* uno strumento in grado di guidare il revisore lungo l'intero processo di audit. Tale risultato è stato raggiunto grazie alla suddivisione delle attività in fasi sequenziali e *step* riepilogati all'interno di *dashboard* di sintesi delle procedure e carte di lavoro fondamentali e obbligatorie da svolgere.

La *Figura 27* mostra una della *dashboard* principali del *software* in cui vengono riportate tutte le fasi del processo di *audit*, ciascuna delle quali darà accesso ad ulteriori *dashboard* di dettaglio. Come è possibile constatare dalla schermata sotto riportata, per ciascuna fase sono indicate le *deadline* suggerite in automatico dal software, ma modificabili dall'utente, che segnalano il termine utile al completamento del lavoro di ogni singola *milestone*. Il sistema segnala, mediante apposita simbologia e con colori differenziati, le fasi non completate nella tempistica prevista e, quindi, in ritardo rispetto alla *roadmap* programmata.

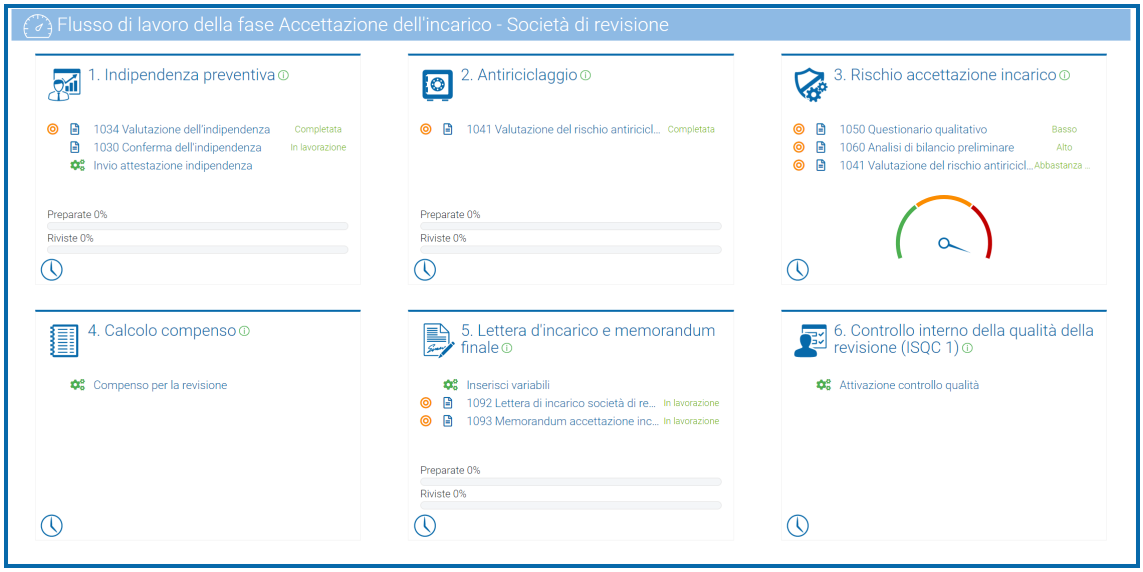
Figura 27 - Dashboard principale



All'interno delle singole *tile* della *dashboard* sono riportate, inoltre, le percentuali di completamento e di *review* di tutte le carte di lavoro obbligatorie contenute in ciascuna fase. Il sistema di scadenze e stato avanzamento lavori così predisposto, facilita notevolmente l'organizzazione delle attività da parte dell'utente e l'individuazione delle aree che richiedono maggior lavoro e attenzione.

Come già accennato, ogni fase è, a sua volta, collegata ad una seconda *dashboard* che riporta le *tile* riepilogative delle sottofasi di lavoro. Ogni *step* contiene il dettaglio delle procedure automatizzate e delle carte di lavoro minimali che devono essere completate ai fini della corretta gestione del lavoro.

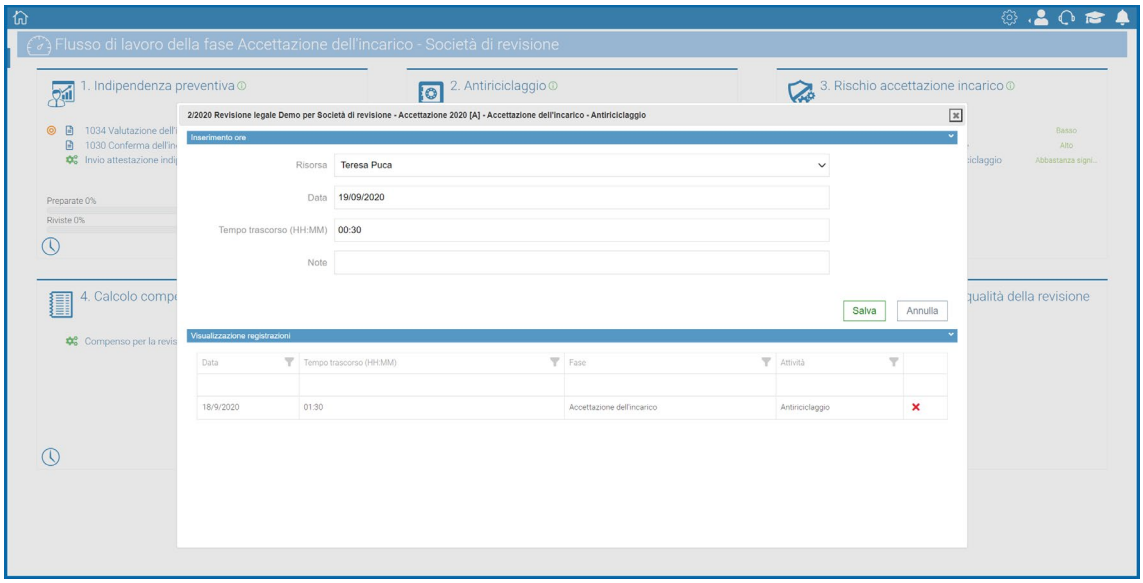
Figura 28 - Flusso di lavoro per fase



La struttura appena descritta, oltre a favorire lo svolgimento dell'incarico in base a un *workflow* predefinito, agevola il lavoro in team e il monitoraggio delle attività. Per prima cosa, il *software* è dotato di un sistema di controlli che consente a più utenti di lavorare simultaneamente all'interno di un incarico evitando che il lavoro di un utente sia sovrascritto o modificato inconsapevolmente da un altro membro del team di revisione. Operando *online*, infatti, tutte le modifiche sono salvate in tempo reale senza necessità di utilizzare un sistema di sincronizzazione dei dati. Di conseguenza, Revisya concede a un solo utente alla volta di poter entrare in modifica su una singola carta di lavoro, bloccando l'accesso ad altri a cui viene segnalato il motivo del blocco. Solo quando sarà terminata l'attività sulla carta di lavoro svolta dal primo utente sarà possibile l'accesso da parte di altri. Il lavoro in team è, inoltre, favorito dalla possibilità di monitorare le ore impiegate a consuntivo per lo svolgimento delle attività previste per ogni fase in modo che possa essere agevolmente controllato l'andamento dell'incarico da parte del responsabile.

Le ore svolte da ciascuna risorsa possono essere, infatti, caricate sulla singola *milestone* e agganciate al tipo di attività svolta e alla data di esecuzione.

Figura 29 - Caricamento ore milestone



Il responsabile della revisione è in grado, quindi, sia di verificare giornalmente il lavoro svolto dal suo *team,* sia di eseguire periodicamente un confronto tra le ore caricate all'interno del *budget,* preparato in base alla stima eseguita in fase di preventivazione, e le ore effettive lavorate.

La logica di flusso con cui è strutturato Revisya risulta fortemente potenziata dall'automatizzazione dei processi e dall'utilizzo dell'Intelligenza Aumentata.

L'Intelligenza Aumentata è considerata come "estensione" dell'Intelligenza Artificiale e impiegata allo scopo di potenziare l'intelligenza umana senza sostituirsi ad essa. Le decisioni e le valutazioni umane non risultano, quindi, alterate o rimpiazzate dall'operatività dei sistemi informatici ma supportate dalle analisi e dalle elaborazioni eseguite grazie all'intelligenza artificiale. In tal senso, il *software* è impiegato per svolgere le attività che presentano un maggior grado di ripetitività o che richiedono analisi che non potrebbero essere svolte manualmente dall'essere umano, ciò al fine di proporre un piano di controllo ottimizzato finalizzato a rendere efficienti le attività svolte. Ad esempio, considerando le fasi di accettazione e di pianificazione di revisione, gli algoritmi di intelligenza artificiale sono in grado di analizzare e calcolare il rischio associato a un nuovo cliente e delineare, di conseguenza, la tempistica di esecuzione e il compenso necessario a coprire i costi di svolgimento dell'incarico. Analogamente, Revisya esegue analisi quantitative sui dati di bilancio i cui risultati, elaborati congiuntamente agli esiti derivanti dalle valutazioni svolte dal revisore, sono utilizzati per determinare in modo automatico programmi di lavoro *ad hoc* contenenti le procedure più appropriate per minimizzare i controlli da eseguire e contestualmente potenziare le attività di risposta al rischio.

Tutte le attività appena descritte rientrano pienamente nel concetto di Intelligenza Aumentata introdotto poc'anzi in quanto operano costantemente in sinergia con le valutazioni e le decisioni dell'utente che mantiene sempre il controllo sulle scelte finali rimandate all'esercizio del suo giudizio professionale.

A completamento del quadro appena delineato, è importante sottolineare che l'Intelligenza Aumentata opera in modo da proporre un flusso di lavoro che sia coerente con la metodologia di revisione scelta dall'utente: può trattarsi della metodologia del Consiglio Nazionale dei Dottori Commercialisti ed Esperti Contabili proposta da Revisya o di una metodologia personalizzata configurata dall'utente.

Infine, il software è dotato di una funzione automatica di codificazione e archiviazione delle carte di lavoro e di storicizzazione delle attività svolte dagli utenti. Ciò consente di tenere sempre traccia del lavoro svolto da tutti i soggetti che hanno accesso al software e "certificare" il momento di esecuzione delle verifiche dimostrando, anche in vista dei controlli che saranno eseguiti dal MEF, la correttezza delle procedure adottate.

3.1.3 Fasi di progettazione e sviluppo del software

Il processo di realizzazione di Revisya ha richiesto lo svolgimento di numerose fasi di analisi, progettazione e sviluppo e la creazione di uno staff di lavoro in grado di coniugare conoscenze e capacità di tipo tecnico-informatico, di progettazione *software*, di analisi dei flussi operativi e logici, di *audit*, contabilità e dei principali aspetti giuridici rilevanti.

Attività fondamentale per un progetto di questo tipo, propedeutica alla successiva pianificazione del processo di sviluppo, è la scelta della *software-house* secondo un *iter* di *software-selection* mediante il quale individuare la società in possesso delle *skill* più idonee alla realizzazione del *software*.

In riferimento al progetto Revisya, oltre alle tecniche di programmazione, due sono stati gli elementi principali su cui si è basata tale scelta:

- La capacità di archiviazione e gestione di grandi volumi di dati;
- La capacità di garantire alti livelli di protezione dei dati.

In riferimento al primo punto, la valutazione è stata effettuata in base alla stima della quantità di dati da archiviare in fase di utilizzazione del software. Tenendo conto della quantità di documenti e di carte di lavoro impiegate per lo svolgimento delle attività di revisione e della mole di incarichi da gestire, è stato necessario prevedere l'archiviazione di oltre 10 Tera di dati per almeno 10 Gigabyte a fascicolo.

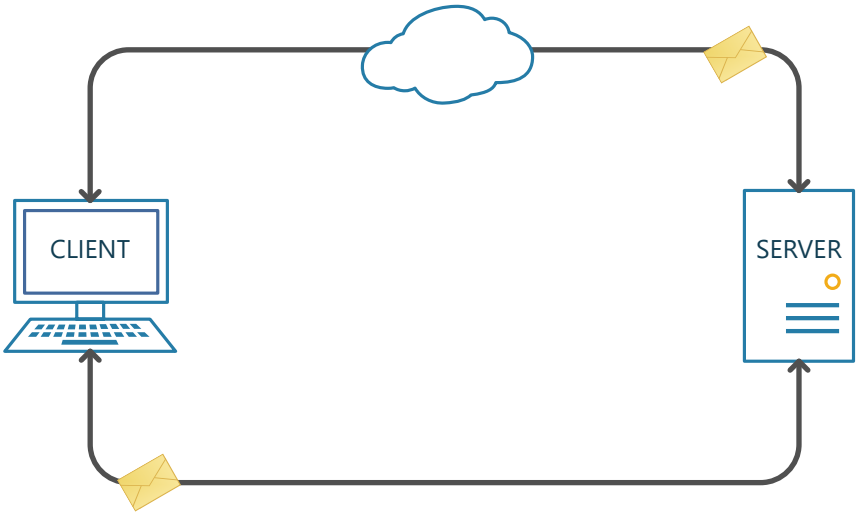
Analizzando il secondo aspetto relativo alla protezione dei dati, è fondamentale considerare quanto disposto dal Regolamento Ue 2016/679 (GDPR - *General Data Protection Regulation*) e dalla normativa nazionale ed internazionale, che impongono l'implementazione di processi di crittografia dei dati e precise regole per la gestione dei *database* e la collocazione dei *server* all'interno dei confini europei.

Revisya, *software* di tipo *web service*, presenta un sistema di crittografia dei dati che utilizza il protocollo *http* per il trasporto delle informazioni: si tratta del protocollo SOAP basato su *http* e *xml* e un sistema di messaggi di richiesta e di risposta.

La richiesta (SOAP *request*) viene inviata dal *client* e "ascoltata" dal *server* che la accetta ed esegue il servizio inoltrando il risultato al richiedente (SOAP *response*).

L'immagine seguente schematizza il processo di richiesta e di risposta appena descritto.

Figura 30 - SOAP



L'archiviazione e la gestione in *cloud* sono supportati da un sistema di protezione dei dati dotato di crittografia 256-bit TLS: si tratta di un sistema che conferisce una protezione dei dati e dei file estremamente superiore a quella che si avrebbe mediante archiviazione in locale o su computer. Il protocollo crittografico TLS dà la possibilità di ottenere una comunicazione e trasmissione sicura dei dati tra sorgente e destinatario. Le applicazioni *client/server* hanno, infatti, la possibilità di comunicare tra loro mediante una rete in grado di prevenire il c.d. "*tampering*" ossia la manomissione dei dati, la falsificazione degli stessi o la loro intercettazione nel corso delle transazioni. Il meccanismo di prevenzione agisce interrompendo la connessione con il *server* in caso di rilevamento di manomissioni e di accessi non autorizzati.

L'architettura *web service in cloud*, quindi, consente di crittografare i dati sia quando sono in transito, per evitare la lettura da parte di soggetti non autorizzati, sia quando non lo sono e di garantire la comunicazione tra *client* e *server* mediante controlli amministrativi e di sicurezza.

Per prevenire accessi indesiderati e assicurare la massima protezione della documentazione prodotta o archiviata all'interno del software, Revisya è dotato di un sistema di generazione automatica di *password* agganciate a username alfanumerici creati per i proprietari delle licenze e comunicati esclusivamente sull'email fornita in fase di attivazione. Sistema analogo di generazione delle *password* e delle utenze è previsto anche per tutti gli utenti che hanno accesso al *software* e per i clienti che accedono al portale loro riservato. Questa tipologia di gestione degli utenti e delle *password* conferisce al proprietario della licenza di avere il pieno controllo degli

accessi ai singoli incarichi creati e di monitorare le attività svolte da ciascun soggetto autorizzato grazie al sistema di registrazione e archiviazione dei *log*.

Il tema della protezione dei dati personali è di particolare rilievo per le società che operano nel campo della consulenza e della revisione contabile, poiché, nell'ambito dello svolgimento delle proprie attività, entrano in possesso di dati, documenti e informazioni sensibili relative ai propri clienti, che necessitano di alti livelli di protezione, in particolar modo se si tratta di soggetti sottoposti alla disciplina del *market abuse*. Per queste ragioni, la gestione della documentazione, la redazione e la conservazione delle carte di lavoro effettuate mediante il *software* sono dotate di specifiche procedure di firma, *review*, chiusura e *lockdown*. In questo modo, non solo Revisya è in grado di storicizzazione gli accessi e le modifiche effettuate ai file, ma anche di provvedere all'autenticazione del personale autorizzato a lavorare su specifici fascicoli in base al ruolo e alla posizione ricoperta.

Il *software* è stato progettato e implementato interamente su tecnologia *Microsoft*, mediante l'utilizzo di:

- SQL *Server* per i *database*;
- ASP NET MVC e C# per la parte applicativa.

Revisya, infine, utilizza i migliori componenti disponibili per l'*editing on-line* dei documenti *office* e per il calcolo dei complessi algoritmi eseguiti lato *server*.

3.2 Analisi di bilancio automatizzata e indicatori predittivi

3.2.1 L'Analisi di bilancio automatizzata Revisya

La soluzione *software* è nata dall'analisi e dalla reingegnerizzazione delle procedure di revisione contabile allo scopo di dar vita a strumenti digitali in grado di supportare le attività umane. In tale ottica, le principali procedure di *audit* sono state reinterpretate in chiave tecnologica e trasformate in processi informatici attivabili e realizzabili mediante specifiche attività di *import* dei dati di partenza e configurazione delle impostazioni essenziali all'ottenimento degli *output*.

Tra le più importanti funzioni automatizzate presenti in Revisya rientra, senza dubbio, la generazione del *report* di analisi di bilancio preliminare. Il *tool* di gestione e realizzazione dell'analisi è in grado di fornire un *report* completo e dettagliato di oltre 30 pagine grazie al solo caricamento, da parte dell'utente, del bilancio depositato in formato *.xbrl*.

XBRL è acronimo di *eXtensible Business Reporting Language*, linguaggio informatico di tipo *Xml* (*eXtensible Markup* - linguaggio *standard* di *markup* in cui il formato e la struttura di un documento sono tenuti separati tra loro) utilizzato come standard per l'elaborazione e il deposito dei bilanci presso il Registro delle Imprese. La prima tassonomia *XBRL* è stata pubblicata in Italia nel 2009, basata sui Principi Contabili Nazionali è oggetto di aggiornamento periodico. Lo standard elettronico è nato allo scopo di rendere fruibili e favorire la circolazione dei dati finanziari affinché possano essere facilmente leggibili e utilizzabili da tutti i soggetti interessati. L'utilizzo di una tassonomia unica consente, inoltre, di snellire le pratiche di deposito dei bilanci e garantire l'automazione dei processi.

La tassonomia *XBRL* e gli strumenti utilizzati per preparare e generare un bilancio sottoforma di "Istanza *Xbrl*", consentono di verificare la validità formale dei dati prima del deposito presso il Registro delle Imprese e di ottenere, contestualmente, una rappresentazione del bilancio in formato *pdf* o *html*[206].

L'analisi di bilancio preliminare generata grazie al caricamento dell'*XBRL* è utilizzata da Revisya per potenziare le attività di valutazione del rischio incarico propedeutiche alla sua accettazione. Prima di ottenere mandato professionale, infatti, il revisore non ha la possibilità di accedere ai dati e alla contabilità del potenziale cliente e, quindi, di ottenere una conoscenza approfondita e dettagliata della realtà aziendale. Questa è la ragione per cui egli avrà la possibilità esclusivamente di consultare i dati ufficiali resi noti dalla società tramite il deposito dei bilanci approvati. Per questo motivo, il *tool* che genera l'analisi di bilancio in Revisya è stato progettato in modo da essere in grado di leggere il bilancio in formato *XBRL* e di produrre il report basandosi esclusivamente su tale fonte dei dati.

In fase di accettazione il revisore effettua, quindi, attività che gli consentono di acquisire una conoscenza di massima del cliente e dell'ambiente in cui opera al fine di determinare il rischio incarico. In conformità alla normativa nazionale applicabile, ai principi di revisione e alla metodologia del CNDCEC, Revisya esegue la stima del rischio incarico sulla base della determinazione preliminare di tre rischi:

- Rischio antiriciclaggio.
- Rischio qualitativo.
- Rischio quantitativo.

[206] Oltre ai molteplici *tool* e *software* gestionali in grado di generare Istanze *Xbrl*, InfoCamere fornisce a tutti i professionisti e le imprese uno strumento gratuito di generazione dei bilanci d'esercizio e consolidati, di validazione dei dati e loro conversione in *pdf* o *html*, scaricabile dalla pagina dedicata del sito istituzionale.

Il software riprende, quindi, la determinazione del rischio preliminare del modello italiano della revisione sintetizzabile nella seguente formula[207]:

RPI=f(Rqa, Rql, Ra)

con:

RPI= Rischio preliminare dell'incarico;

Rqa=Componente quantitativa del rischio preliminare;

Rql= Componente qualitativa del rischio preliminare;

Ra: *Notching* del rischio che deriva dall'analisi antiriciclaggio sul cliente.

La componente **Ra** può essere utilizzata come *notching*, cioè come correttivo tramite somma algebrica rispetto al prodotto **Rqa x Rql**. In alternativa, la valutazione può essere eseguita come prodotto tra i tre fattori **Rqa**, **Rql** e **Ra**.

È proprio questa seconda alternativa che viene utilizzata da Revisya per determinare il rischio preliminare incarico secondo il prodotto logico evidenziato nella seguente tabella[208].

Figura 31 - Parametri di valutazione del rischio cliente

Rischio Antiriciclaggio	Rischio Qualitativo	Rischio Quantitativo	
Abbastanza significativo	Alto	Alto	Alto
Molto significativo	Alto	Alto	Alto
Non significativo	Alto	Alto	Moderato
Poco significativo	Alto	Alto	Moderato
Abbastanza significativo	Basso	Alto	Alto
Molto significativo	Basso	Alto	Alto
Non significativo	Basso	Alto	Moderato
Poco significativo	Basso	Alto	Moderato
Abbastanza significativo	Moderato	Alto	Alto
Molto significativo	Moderato	Alto	Alto

Pagina 1 di 4 (36 elementi) 1 2 3 4

[207] La formula del rischio preliminare della revisione e la successiva spiegazione del suo utilizzo metodologico sono tratte da D'ALESSIO R., ANTONELLI V., *Principi di Auditing. Concetti, modelli, metodologie, applicazioni*, Volume I, Edises, 2021, p. 400.

[208] Revisya consente agli utilizzatori di modificare la configurazione dei rischi e adattare il prodotto logico delle tre componenti alla metodologia di revisione impiegata che potrebbe prevedere una quantificazione differente del rischio incarico.

La componente antiriciclaggio del rischio preliminare di incarico è determinata sulla base della valutazione antiriciclaggio eseguita sul cliente in conformità alle norme che obbligano i professionisti all'adeguata verifica della clientela e all'identificazione del titolare effettivo[209].

La componente qualitativa del rischio preliminare è, invece, determinata sulla base della valutazione delle principali informazioni ottenute sul cliente e sulla valutazione dell'adeguatezza organizzativa del revisore. In particolare, la valutazione qualitativa è determinata da Revisya tramite la ponderazione delle risposte fornite dal revisore a un questionario che funge da guida nella determinazione del livello di impatto stimato in riferimento ai principali rischi connessi all'incarico: contiene, ad esempio, riferimenti ai rischi relativi alla continuità aziendale, all'integrità del cliente, alle *performance* realizzate.

L'ultima componente, quella del rischio quantitativo viene, invece, determinata sulla base dell'informativa economico-finanziaria e, quindi, sull'analisi dei dati di bilancio del potenziale cliente. Gli algoritmi di calcolo presenti e l'intelligenza artificiale Revisya, una volta ottenuti i dati estratti dal bilancio importato, sono in grado in pochi secondi di:

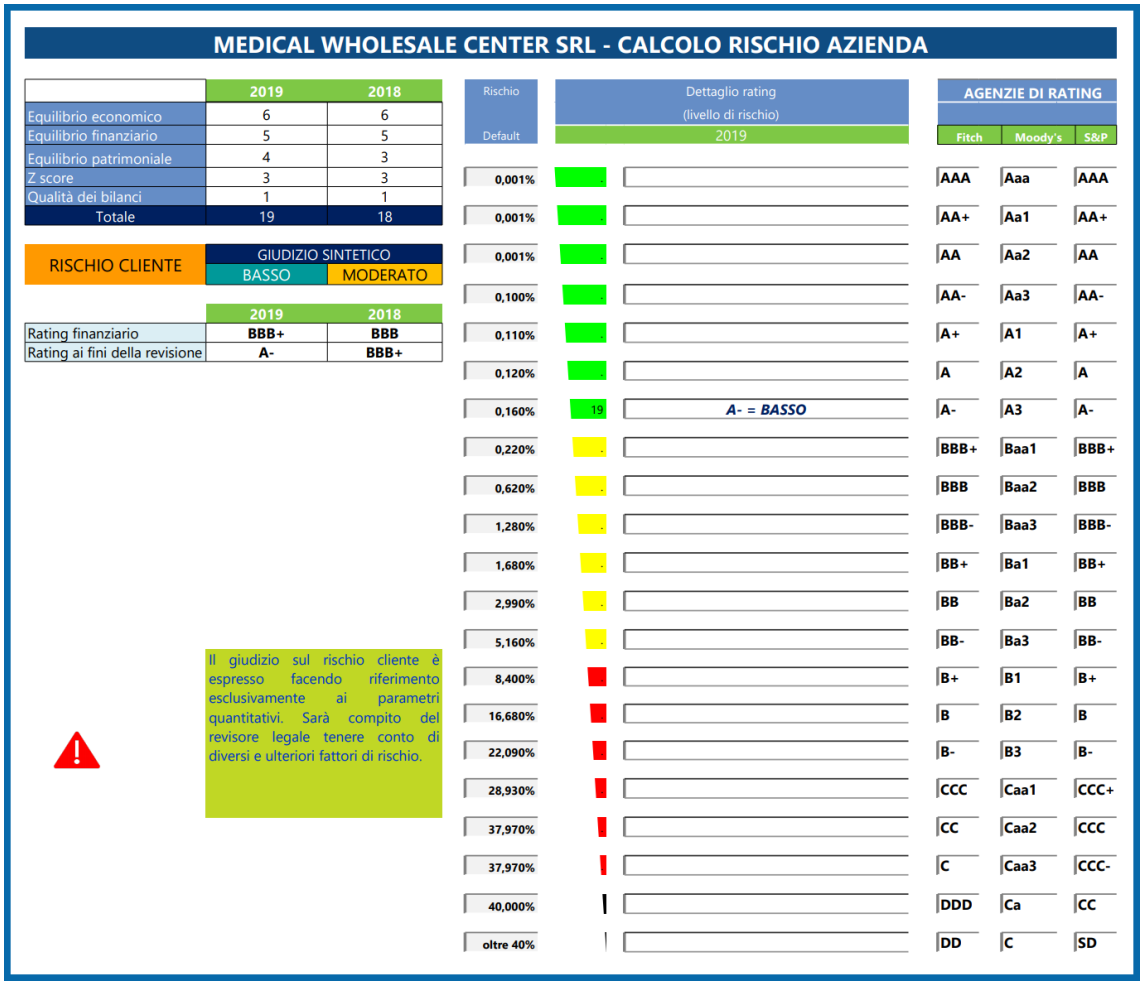
- Riportare i dati dell'*Xbrl* all'interno degli schemi di bilancio in IV Direttiva;
- Proporre una sintesi dei principali indicatori economici, patrimoniali e finanziari;
- Stimare la qualità del bilancio importato;
- Predisporre gli schemi di bilancio riclassificato;
- Calcolare i principali indici di bilancio;
- Determinare l'equilibrio finanziario e il *rating* di rischio;
- Calcolare la posizione finanziaria netta;
- Calcolare la continuità aziendale;
- Determinare il *rating* finanziario mediante il metodo *Standard & Poor's* e tramite *Damodaran*;
- Calcolare la componente quantitativa del rischio preliminare dell'incarico sintetizzando gli *score* ottenuti in merito all'equilibrio economico, finanziario, patrimoniale, al calcolo dello *Z-score* e della qualità dei bilanci.

---

[209] L'art. 18 del d.lgs. 231/2007, rubricato *Contenuto degli obblighi di adeguata verifica della clientela* stabilisce che *«Gli obblighi di adeguata verifica della clientela consistono nelle seguenti attività:*
a) identificare il cliente e verificarne l'identità sulla base di documenti, dati o informazioni ottenuti da una fonte affidabile e indipendente;
b) identificare l'eventuale titolare effettivo e verificarne l'identità;
c) ottenere informazioni sullo scopo e sulla natura prevista del rapporto continuativo o della prestazione professionale;
d) svolgere un controllo costante nel corso del rapporto continuativo o della prestazione professionale.»

In modo del tutto automatizzato, Revisya propone, quindi, il proprio rischio quantitativo determinato come risultato di sintesi di tutte le analisi eseguite per la produzione del *report*. Il giudizio sintetico proposto dal *software* è accompagnato anche dalla stima di dettaglio del livello di *rating* da utilizzare ai fini della revisione e della sua collocazione all'interno della scala di *rating* utilizzata dalle principali agenzie.

Figura 32 - Valutazione quantitativa del rischio cliente



Nei successivi paragrafi andremo ad approfondire i test contenuti nell'analisi preliminare di bilancio automatizzata svolta da Revisya che si rivolgono all'individuazione di segnali di frode e anomalie presenti nel bilancio relativo all'esercizio precedente rispetto a quello di accettazione dell'incarico.

3.2.2 La valutazione della qualità dei bilanci

Come indicato nel precedente paragrafo, l'analisi preliminare di bilancio contiene una sezione dedicata alla valutazione della qualità dei bilanci che segnala la presenza di anomalie e alterazioni nei dati importati.

Innanzitutto, il software esegue in automatico un'attenta analisi dei dati di bilancio mediante la quale vengono eseguiti i seguenti controlli:

- Controlli di quadratura: il *tool* effettua un ricalcolo delle voci di bilancio al fine di evidenziare se siano presenti squadrature tra attivo e passivo di bilancio.
- Controlli di congruenza: questa sezione dei controlli è finalizzata a individuare possibili incongruenze tra i dati presenti in bilancio e le medie di settore e la normativa di riferimento. Ad esempio, è in grado di segnalare se l'incidenza dei contributi appostati in bilancio sia in linea con le percentuali medie fissate dalle tabelle INPS o INAIL e a verificare se il TFR sia coerente con quanto prescritto dal Codice civile.
- Controlli di esistenza: verifica la presenza di eventuali poste con saldo pari a zero che, invece, dovrebbero risultare con saldo differente da zero riportandone le relative motivazioni.
- Controlli sui comportamenti contabili inconsueti: questa tipologia di controlli punta a verificare probabili anomalie dovute, ad esempio, alla mancata movimentazione di una o più poste di bilancio da un esercizio all'altro.
- Controlli sulle politiche di bilancio: controlla possibili anomalie derivanti da errata applicazione delle politiche di bilancio nella determinazione dei saldi.
- Altri controlli: sezione residuale in cui vengono segnalate ulteriori anomalie eventualmente riscontrate nel corso dell'analisi dei dati.

È evidente che la sezione appena descritta costituisca un importante punto di partenza per le successive considerazioni del revisore in quanto consente di ottenere evidenza delle principali incongruenze presenti nei dati di bilancio. Per un revisore sarebbe molto complesso e dispendioso in termini di tempo e di risorse eseguire controlli similari in modo autonomo e senza l'ausilio di strumenti informatici.

Altra sezione di particolare importanza per il revisore, risulta costituita dai controlli finalizzati all'individuazione di possibili manipolazioni di bilancio. Questa tipologia di alterazioni di bilancio viene identificata come *earnings management,* termine che sottende tutte le manipolazioni di bilancio implementate dai manager di una società al fine di alterare il livello degli utili conseguiti

e migliorare i principali indicatori di performance aziendale. *«The quality of a company's earnings is often defined as the degree to which earnings reflect the actual economic reality of the business. Earnings management rises to the level of fraud when companies intentionally misstate information»*[210].

I manager possono essere spinti ad alterare i dati di bilancio per molteplici ragioni, ad esempio per ottenere bonus o incentivi correlati ai risultati raggiunti dall'azienda o per migliorare gli indicatori di performance aziendale e presentare ad analisti e stakeholder una migliore situazione economica.

I possibili rischi correlati a tale fenomeno devono essere tempestivamente rilevati dal revisore nel corso delle attività di individuazione e valutazione dei rischi eseguite in fase di pianificazione. In base agli elementi raccolti, il revisore è in grado di definire le attività di investigazione del fenomeno da eseguire e programmare le necessarie procedure di risposta al rischio da attuare in fase di esecuzione. Mediante il calcolo di specifici indicatori e l'utilizzo di algoritmi matematici, Revisya è in grado di rielaborare i dati di bilancio allo scopo di formulare un giudizio sulla presenza di probabili alterazioni. L'analisi delle anomalie e delle variazioni rispetto a una situazione considerata in linea con le aspettative viene mostrata all'utente come nella seguente figura.

Figura 33 – Valutazione della probabilità di manipolazione del bilancio

MEDICAL WHOLESALE CENTER SRL
- Probabilità di manipolazione del bilancio-

Descrizione	2019
Rotazione dei clienti	0,9121694878
Incidenza del costo del venduto	0,9120146225
Incidenza attività immateriali sull'attivo	1,871768993
Tasso di ammortamento	0,8275455928
Grado di indebitamento	0,749336927
Risultato	Manipolazione poco probabile

L'utente può visualizzare le principali variabili utilizzate dal software e i valori da esse assunti in riferimento al bilancio dell'anno precedente con evidenza del risultato derivante dall'analisi automatizzata.

[210] GOLDEN T.W., SKALAK S. L., CLAYTON M.M., *A guide to forensic accounting investigation*, John Wiley & Sons, Inc., Hoboken, New Jersey, 2006, p. 378

Si mette in evidenza come Revisya suggerisca il risultato calcolato all'utente specificando che lo stesso deriva dall'applicazione di elaborazioni matematiche e statistiche che non possono sostituirsi al giudizio professionale del revisore. In linea con la filosofia di utilizzo e lo scopo dell'Intelligenza Aumentata, è compito del professionista verificare il risultato sulla base delle caratteristiche aziendali e valutare la necessità di eseguire ulteriori indagini e approfondimenti.

3.2.3 L'applicazione della legge di Benford

La terza tipologia di analisi di cui si compone la sezione dedicata alla qualità dei bilanci deriva dall'applicazione della Legge di *Benford* ai dati importati tramite caricamento dell'*XBRL*.
La Legge di *Benford*, conosciuta anche come legge della prima cifra significativa, afferma che in una sequenza di numeri generati in modo casuale, le loro prime cifre si presentano con una determinata frequenza che si differenzia in base alla cifra considerata.
La prima scoperta del fenomeno si ebbe per la prima volta ad opera dell'astronomo *Simon Newcombe* che osservò come le pagine delle tavole logaritmiche fossero consumate in modo differente. Le prime pagine, infatti, contenenti le cifre significative più piccole, risultavano più consumate di quelle contenenti i numeri maggiori. Fu da questa semplice constatazione che *Newcombe* scoprì e descrisse nel 1881 in un articolo pubblicato sull' *American Journal of Mathematics* quella che oggi conosciamo come *Benford's Law*. La portata della scoperta di *Newcombe* non fu compresa ma, addirittura, dimenticata nel tempo tanto che si parla di una nuova scoperta avvenuta grazie a *Frank Benford* nel 1938.
Benford analizzò la frequenza della prima cifra significativa contenuta in 20 elenchi di numeri tratti da molteplici fonti di dati, come la numerosità delle popolazioni o la lunghezza dei fiumi, per un totale di 20.229 numeri.
Per cifra significativa si intende la cifra posta più a sinistra non nulla di un numero positivo. Ad esempio il numero 123 ha come prima cifra significativa l'1, come seconda cifra significativa il 2, come terza cifra significativa il 3.
Sfruttando le 20 popolazioni selezionate, *Benford* riuscì a dimostrare che le cifre significative, per i numeri da 1 a 9, non si presentano con la medesima frequenza ma che la stessa diminuisce per i numeri maggiori. Il valore 1 come prima cifra significativa si presenta, infatti, con una frequenza del 30,1% mentre per i numeri seguenti diminuisce fino ad arrivare ad una percentuale del 4,6%

per il numero 9. La seguente tabella riporta le frequenze per tutti i numeri da 0 a 9 in riferimento alla prima, seconda, terza e quarta cifra significativa occupata.

Tabella 1 - Frequenze della Legge di Benford

Cifra	*1ª posizione*	*2 ª posizione*	*3 ª posizione*	*4 ª posizione*
0	—	0,11968	0,10178	0,10018
1	0,30103	0,11389	0,10138	0,10014
2	0,17609	0,10882	0,10097	0,10010
3	0,12494	0,10433	0,10057	0,10006
4	0,09691	0,10031	0,10018	0,10002
5	0,07918	0,09668	0,09979	0,09998
6	0,06695	0,09337	0,09940	0,09994
7	0,05799	0,09035	0,09902	0,09990
8	0,05115	0,08757	0,09864	0,09986
9	0,04576	0,08500	0,09827	0,09982

Fonte: Ns. rielaborazione Nigrini, M.J. 1996. A taxpayer compliance application of Benford's Law. The Journal of the American Taxation Association. 18, Spring:72-91.

La formula per il calcolo della frequenza della prima cifra significativa è la seguente:

$$P(D_1 = d_1) = \log\left(1 + \frac{1}{d_1}\right) \qquad \text{con } d_1 \in \{1, 2, \dots, 9\}$$

La formula è costruita usando un logaritmo in base 10 e si riferisce esclusivamente al calcolo della frequenza relativa alla prima cifra significativa. Per le altre cifre significative o per calcolare la frequenza di due cifre combinate sono state elaborate ulteriori formule di calcolo[211].
In particolare, il calcolo della frequenza della seconda cifra significativa può essere determinato sulla base della seguente formula:

[211] Cfr. DRAKE P.D., NIGRINI M.J., *Computer assisted analytical procedures using Benford's Law*, Journal of Accounting Education, Ed. 18 (2000) 127-146.

$$P(D_2 = d_2) = \sum_{d_1=1}^{9} \log\left(1 + \frac{1}{d_1 d_2}\right) \qquad \text{con } d_2 \in \{0, 1, \ldots, 9\}$$

Infine, la formula per il calcolo della frequenza di prima e seconda cifra combinate è la successiva:

$$P(D_1 D_2 = d_1 d_2) = \log\left(1 + \frac{1}{d_1 d_2}\right) \qquad \text{con } d_1 d_2 \in \{10, 11, \ldots, 99\}$$

Grazie al contributo di *Pinkham* del 1961 è stato possibile, inoltre, dimostrare che la legge è invariante per cambiamenti di scala, ad esempio se la medesima popolazione è misurata in chilometri o metri[212]. «*Pinkham showed that if a set of numbers followed Benford's Law perfectly, and these numbers were all multiplied by a (nonzero) constant, the new list would also follow Benford's Law*[213]*».* Drake e Nigrini sottolineano come sia proprio tale caratteristica della Legge di *Benford* a renderla applicabile a popolazioni numeriche di dati economici e finanziari che utilizzano differenti valute.

La legge di *Benford* può essere applicata a popolazioni in possesso di specifiche caratteristiche. È necessario, infatti, che gli elementi della popolazione si riferiscano tutti al medesimo fenomeno oggetto di osservazione, che i numeri non rientrino in un *range* predefinito costituito da un numero minimo e un numero massimo di variazione e che non si tratti di numeri assegnati, come codici o password[214].

La Legge di *Benford* può essere, quindi, applicata anche ai dati economici e finanziari prodotti da un'azienda, ma a condizione che siano presenti ulteriori caratteristiche nei dati considerati[215]:

- I dati contabili devono riferirsi a un *report* infrannuale o di esercizio facilmente riconciliabile con i saldi totali derivanti dalla contabilità aziendale.
- I dati devono far riferimento ad un'unica realtà aziendale in quanto, in caso di unione di dati derivanti da più realtà aziendali non correlate tra loro, le anomalie e le duplicazioni presenti potrebbero perdersi.
- I dati devono essere analizzati ad un livello quanto più specifico possibile.

---

[212] Cfr. NIGRINI M.J., *Forensic Analytics. Methods and Techniques for Forensic Accounting Investigations*, Wiley, First Edition, p. 110.

[213] DRAKE P.D., NIGRINI M.J., *Computer assisted analytical procedures using Benford's Law*, Journal of Accounting Education, Ed. 18 (2000) 127-146, p. 132.

[214] ANASTASI J., *The new forensics. Investigating Corporate Fraud and the Theft of Intellectual Property*, John Wiley & Sons, Inc., Hoboken, New Jersey, 2003, pp. 184 e ss.

[215] La sintesi delle condizioni necessarie all'applicazione della Legge di Benford ai dati economici e finanziari è tratta da DRAKE P.D., NIGRINI M.J., *Computer assisted analytical procedures using Benford's Law*, Journal of Accounting Education, Ed. 18 (2000) 127-146, p. 132 e ss.

- I dati devono essere puliti dai valori inferiori a 10, poiché di entità non significativa per i test da eseguire e dai valori pari a zero o negativi che dovranno essere testati separatamente.

In presenza di tutte le condizioni descritte, i risultati derivanti dall'applicazione della Legge di *Benford* costituiscono un importante punto di riferimento per poter evidenziare anomalie all'interno dei dati e possibili indizi di frode o di altri errori significativi. Si tratta di una vera e propria tecnica di investigazione che consente di confrontare i dati reali oggetto di analisi con le frequenze attese in modo da identificare tutte le anomalie da approfondire e valutare con ulteriori verifiche[216].

Tra i test che è possibile implementare sulla frequenza delle cifre significative, uno dei più importanti è sicuramente quello che ha ad oggetto la valutazione della prima cifra. Data una popolazione di riferimento, il test consiste nel verificare quante volte ciascun numero da 1 a 9 è presente in termini assoluti e percentuali. I valori così ottenuti devono essere poi sottoposti a confronto con le frequenze di *Benford* al fine di determinare lo scostamento esistente e valutare se lo stesso risulta accettabile o meno.

Questa tipologia di test è integrata all'interno dell'analisi di bilancio preliminare svolta in automatico sui dati importati tramite caricamento del bilancio in formato *XBRL* relativo all'anno precedente rispetto a quello di accettazione dell'incarico. L'intelligenza artificiale calcola quindi:

- Il numero di volte in cui i numeri da 1 a 9 si presentano nei dati di bilancio come prima cifra significativa;
- La distribuzione reale della prima cifra significativa;
- La differenza tra la distribuzione attesa e la distribuzione reale;
- La percentuale cumulata delle differenze tra distribuzione attesa e distribuzione cumulata.

I calcoli appena descritti sono effettuati per entrambe le annualità contenute all'interno del bilancio importato e sono finalizzati a determinare se lo scostamento cumulato possa essere considerato accettabile rispetto a un *range* predefinito ritenuto appropriato.

[216] NIGRINI M.J., *Forensic Analytics. Methods and Techniques for Forensic Accounting Investigations*, Wiley, First Edition, p. 110; *«Benford's Law gives the expected frequencies of the digits in tabulated data. As a fraud investigation technique Benford's Law also qualifies as a high-level overview. Nonconformity to Benford's Law is an indicator of an increased risk of fraud or error. Nonconformity does not signal fraud or error with certainty. Further work is always needed».*

Considerando i valori di *cut-off* ritenuti appropriati e ricalcolati per ciascuno dei bilanci importati e in relazione ad entrambe le annualità considerate, *Revisya* propone la sua conclusione in merito alla possibilità che il bilancio contenga una frode.

Figura 34 - Esempio di applicazione della Legge di Benford in Revisya

MEDICAL WHOLESALE CENTER SRL - Legge di Benford

Prima Cifra	Conteggio	Distribuzione reale	Distribuzione attesa	Differenza cumulativa	Conteggio	Distribuzione reale	Distribuzione attesa	Differenza cumulativa
1	20	23,0%	30,1%	7,1%	19	21,6%	30,1%	7,1%
2	17	19,5%	17,6%	5,2%	20	22,7%	17,6%	5,2%
3	10	11,5%	12,5%	6,2%	14	15,9%	12,5%	6,2%
4	8	9,2%	9,7%	6,7%	3	3,4%	9,7%	6,7%
5	6	6,9%	7,9%	7,7%	13	14,8%	7,9%	7,7%
6	10	11,5%	6,7%	2,9%	3	3,4%	6,7%	2,9%
7	9	10,3%	5,8%	1,6%	6	6,8%	5,8%	1,6%
8	4	4,6%	5,1%	1,1%	4	4,5%	5,1%	1,1%
9	3	3,4%	4,6%	0,0%	6	6,8%	4,6%	0,0%
Totale	87		KS	7,7%	88		KS	7,7%

Cut-off 14,6%
Cut-off 14,5%

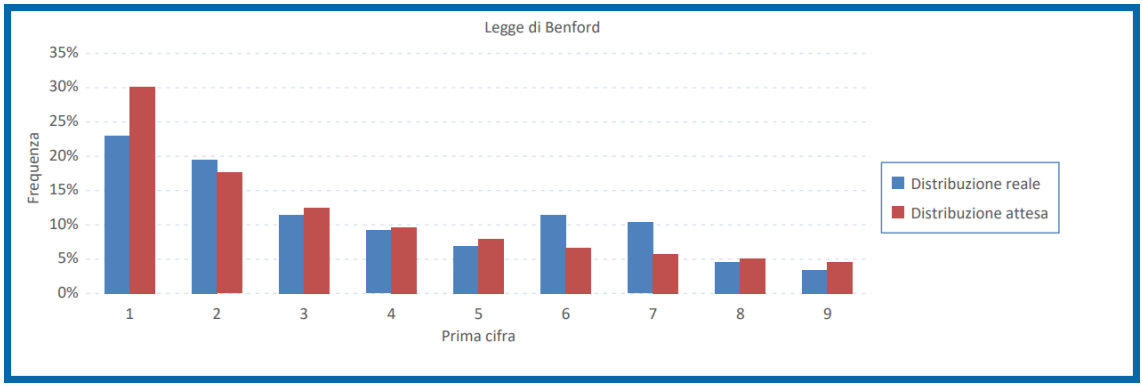
Bilancio: 2019 — Frode improbabile

Bilancio: 2018 — Frode improbabile

Nell'esempio appena riportato le elaborazioni statistiche e matematiche eseguite da *Revisya* suggeriscono al revisore che la presenza di una frode per entrambe le annualità considerate risulta improbabile. Tale constatazione deriva dal fatto che le differenze percentuali riscontrate sono ritenute non significative.

L'utente può verificare la variazione presente sia analizzando i dati della distribuzione attesa e di quella reale, sia osservando il grafico generato dal *software* che pone a confronto le grandezze considerate.

Figura 35 - Grafico sui risultati del test sulla prima cifra significativa



Come precisato all'interno dell'analisi, i test eseguiti dall'intelligenza artificiale *Revisya* costituiscono uno strumento a supporto del revisore che, in base ai risultati proposti dal *software*, dovrà validarne l'attendibilità in base alla conoscenza del cliente e alla valutazione degli elementi probativi raccolti.

Di seguito i risultati ottenuti dall'alterazione dei dati di bilancio dell'azienda di test utilizzata con simulazione di una frode in atto per le due annualità di incarico considerate.

Figura 36 - Risultati derivanti dalla simulazione di una frode

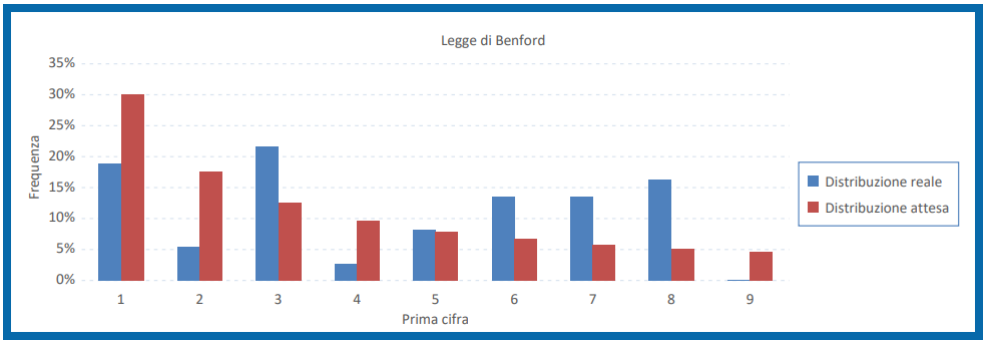
MEDICAL WHOLESALE CENTER SRL - Legge di Benford

Prima Cifra	Conteggio	Distribuzione reale	Distribuzione attesa	Differenza cumulativa	Prima Cifra	Conteggio	Distribuzione reale	Distribuzione attesa	Differenza cumulativa
1	7	18,9%	30,1%	11,2%	1	8	22,9%	30,1%	11,2%
2	2	5,4%	17,6%	23,4%	2	5	14,3%	17,6%	23,4%
3	8	21,6%	12,5%	14,3%	3	3	8,6%	12,5%	14,3%
4	1	2,7%	9,7%	21,2%	4	1	2,9%	9,7%	21,2%
5	3	8,1%	7,9%	21,1%	5	4	11,4%	7,9%	21,1%
6	5	13,5%	6,7%	14,2%	6	5	14,3%	6,7%	14,2%
7	5	13,5%	5,8%	6,5%	7	3	8,6%	5,8%	6,5%
8	6	16,2%	5,1%	4,6%	8	5	14,3%	5,1%	4,6%
9	0	0,0%	4,6%	0,0%	9	1	2,9%	4,6%	0,0%
Totale	37		KS	23,4%	Totale	35		KS	23,4%
			Cut-off	22,4%				Cut-off	23,0%
			Frode Probabile					Frode Probabile	

Per entrambe le annualità il totale della differenza cumulativa supera il livello di *Cut-off* calcolato sui dati importati: ciò implica la presenza di segnali della possibile presenza di una frode in bilancio.

Le anomalie presenti nei dati sono ancora più evidenti dalla lettura del grafico che riepiloga le differenze riscontrate.

Figura 37 - Grafico differenze in presenza di frode



3.2.2 Intelligenza artificiale e procedure automatizzate Journal Entries Test

3.3.1 Journal Entries Test Revisya

Revisya è dotato di un sistema avanzato di lettura del libro giornale ed elaborazione *dei Journal Entries Test* mediante un approccio semplificato di configurazione e gestione che ne rende semplice e intuitivo l'utilizzo anche da parte di revisori con minori competenze informatiche.
Per poter procedere al test, l'utente deve scaricare il modello di partenza da utilizzare per richiedere l'estrazione del libro giornale da parte della società cliente.
Una volta importato il libro giornale nel formato *excel* codificato da Revisya, il sistema estrapola tutti i dati dal file e consente all'utente di configurare i conti da utilizzare nei controlli distinguendo tra conti di cassa, conti di debito, conti relativi a Finanziamenti soci e Patrimonio netto, mastri clienti e mastri fornitori.
Dopo aver eseguito la configurazione dei conti, l'utente dovrà configurare i controlli da eseguire scegliendo tra quelli già codificati all'interno del sistema e/o eseguendo ulteriori controlli manuali personalizzati.
I controlli preconfigurati che consentono a Revisya di eseguire la ricerca automatica delle anomalie nelle registrazioni presenti nel libro giornale sono i seguenti:

- Scritture non bilanciate;
- Scrittura duplicata;
- Scritture composte fuori orario;
- Scritture di importo inconsueto;
- Insussistenze di cassa;
- Pagamenti in contanti oltre il limite consentito;
- Utilizzo di causali contabili generiche;
- Storni da un cliente all'altro;
- Storni da un cliente a un fornitore;
- Storni da un cliente ad altri conti di debito;
- Finanziamenti dei soci in contanti;
- Versamenti dei soci (Riserve) in contanti;
- Conto utilizzato raramente;
- Utente inusuale;
- Descrizione inadeguata;
- Test quadratura libro giornale e bilancio di verifica.

Per ognuno dei controlli appena evidenziati, il sistema riconosce le colonne da utilizzare e lancia una *query* che restituisce come risultato l'elencazione di tutte le righe che corrispondono alle caratteristiche ricercate. Di seguito la descrizione di dettaglio dei controlli eseguibili tramite il *software*.

Scritture non bilanciate

Questo tipo di controllo è finalizzato ad individuare possibili scritture in cui gli importi in dare e in avere della registrazione non risultano bilanciati. Per poter eseguire questo tipo di controllo, Revisya lavora sui dati relativi al numero della registrazione, alla data e agli importi in dare e in avere.

Ad esempio, la *query* utilizzata per questa tipologia di controllo è la seguente:

```
SELECT NumeroReg, DataReg FROM Giornale riga WHERE IdGiornale = {{IdGiornale}} GROUP BY IdGiornale, NumeroReg, DataReg HAVING SUM(riga.d) != SUM(riga.a)
```

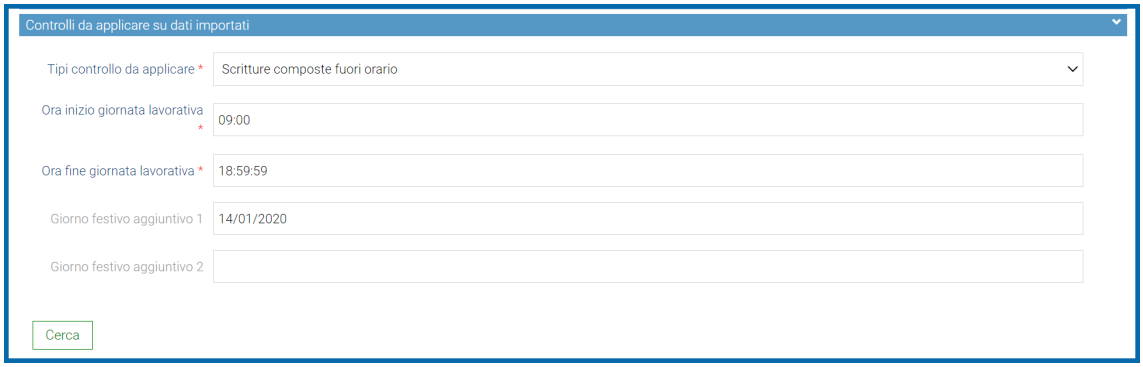
Scritture duplicate

Il controllo sulle scritture duplicate ha l'obiettivo di verificare la presenza di scritture eseguite più di una volta. La *query* utilizza i dati relativi al numero e alla data di registrazione e i valori registrati in dare e avere.

Scritture composte fuori orario

Il controllo è eseguito allo scopo di verificare se siano state eseguite scritture a libro giornale al di fuori del normale orario lavorativo. Revisya, in questo caso, richiede all'utente un'ulteriore attività di configurazione mediante la quale specificare l'orario di inizio e di fine dell'attività lavorativa e eventuali giorni di festa aggiuntivi rispetto a quelli ordinari.

Figura 38 - Configurazione scritture composte fuori orario



Il risultato ottenuto è l'elencazione di tutte le scritture eseguite al di fuori dell'orario lavorativo e/o nei giorni festivi.

Figura 39 - Risultato controllo scritture composte fuori orario

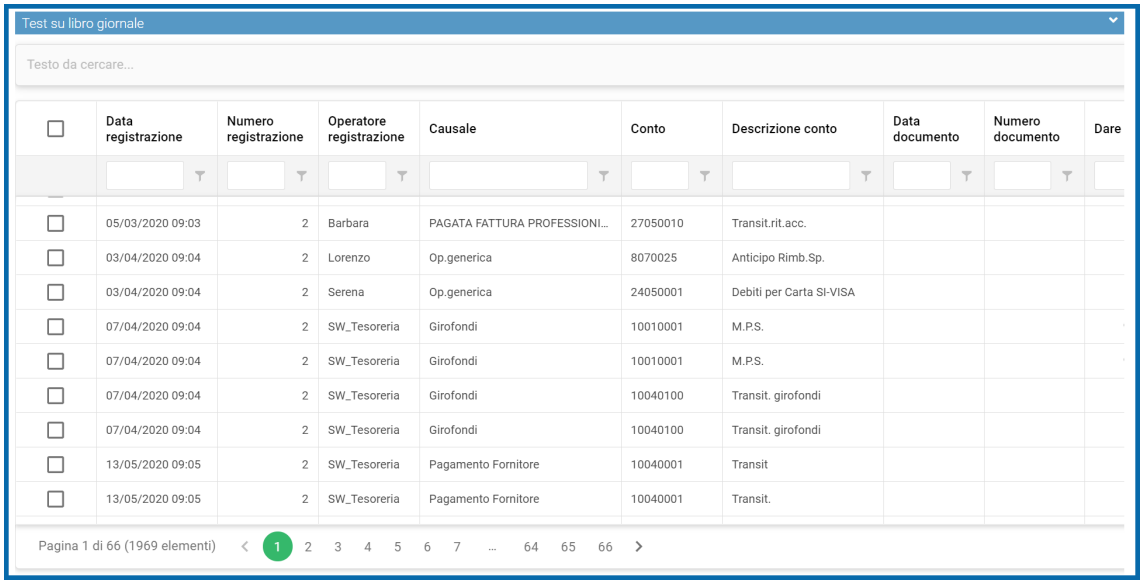
Scritture di importo inconsueto

Il test consente al revisore di identificare eventuali importi inusuali presenti a libro giornale verificando i valori in dare e avere contenuti nel documento. Il *software* propone 4 valori inconsueti che possono essere modificati dal revisore in base alle specifiche esigenze.

Figura 40 - Configurazione controllo

Il risultato ottenuto è visibile nell'immagine seguente:

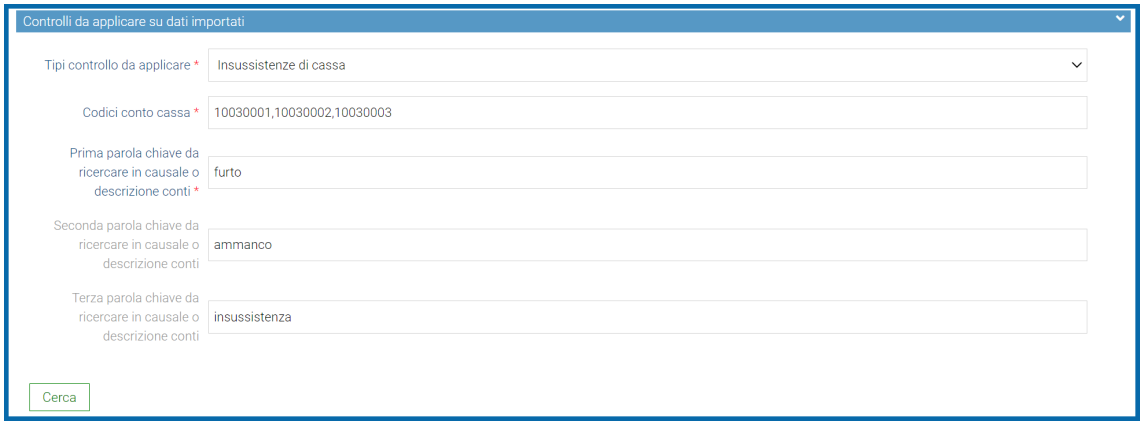
Figura 41 - Risultato controllo scritture di importo inconsueto



Insussistenze di cassa

Il controllo è finalizzato a verificare la presenza di insussistenze di cassa da identificare consultando le casuali e le descrizioni utilizzate all'interno delle registrazioni. Il test presuppone che siano identificati i conti di cassa mediante la propedeutica attività di configurazione conti e che l'utente specifichi le parole chiave da impiegare per poter individuare tali rilevazioni.

Figura 42 - Configurazione controllo su insussistenze di cassa



Pagamenti in contanti oltre il limite consentito

La verifica consente di rilevare eventuali pagamenti eseguiti dalla società in contanti oltre al limite consentito dalla normativa antiriciclaggio. Il *software* esegue il controllo considerando la lista dei conti cassa individuati e l'importo limite configurato dall'utente.

La query applicata in questo caso è la seguente:

```
SELECT * FROM Giornale  WHERE IdGiornale = {{IdGiornale}}    AND Con in
({{filter1}}) AND (D >= {{filter2}} or A >= {{filter2}})
```

Utilizzo causali contabili generiche

Il controllo è effettuato allo scopo di verificare la presenza di causali contabili generiche all'interno delle registrazioni eseguite. Revisya consente all'utente di inserire fino a 4 parole chiave da utilizzare per l'esecuzione della ricerca.

Storni da un cliente all'altro

La verifica è eseguita considerando il tipo di conto e il tipo di contropartita al fine di individuare eventuali storni eseguiti da un cliente all'altro.

Storni da un cliente ad altri conti di debito

Questo tipo di controllo è molto simile a quello descritto al punto precedente, ma con estensione della verifica a tutti i conti di debito identificati dall'utente in fase di configurazione.

Finanziamenti dei soci in contanti

La verifica è eseguita controllando simultaneamente i conti di cassa con la lista dei conti relativi ai finanziamenti soci.

```
SELECT * FROM Giornale
INNER JOIN
            (
                  SELECT  '%{{filter3}}%' Col
                  UNION SELECT '%{{filter4}}%'
            )caus ON r.Caus LIKE caus.Col
```

```
WHERE IdGiornale = {{IdGiornale}}  AND Con IN ({{filter1}}) AND CoContr IN ({{filter2}})
```

Versamenti dei soci in contanti

Il controllo prevede la verifica dei conti di cassa e dei conti di patrimonio netto per i quali verificare conto, contropartita e causale.

Conto utilizzato raramente

Il controllo viene eseguito allo scopo di identificare eventuali conti utilizzati raramente nel corso dell'esercizio in quanto caratterizzati da un numero limitato di rilevazioni. Per poter eseguire tale verifica il *software* richiede all'utente l'inserimento del numero massimo di scritture eseguite su un conto affinché si possa considerare che lo stesso sia utilizzato raramente.

Utente inusuale

Il controllo identifica tutti gli utenti che abbiano eseguito un numero limitato di rilevazioni la cui quantità massima viene definita dallo stesso revisore. Tutti gli operatori che hanno eseguito un numero pari o inferiore al livello prestabilito di rilevazioni, saranno presentati al revisore come utenti inusuali.

Descrizione inadeguata

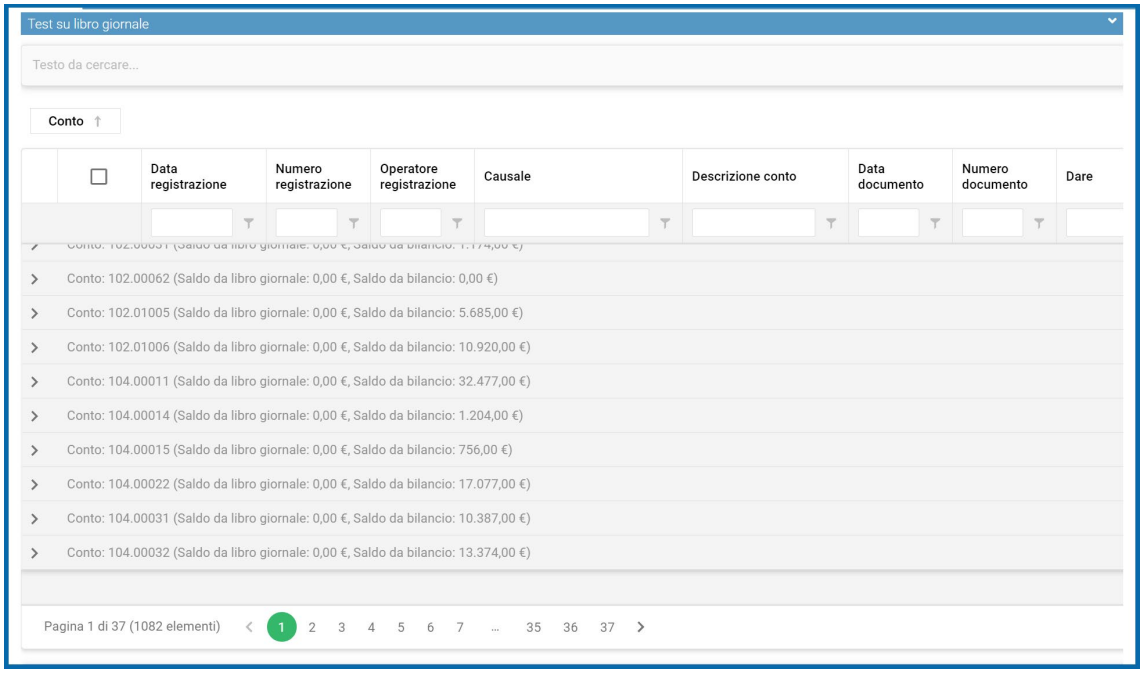
Scopo della verifica è quello di identificare tutte le descrizioni contenute nelle registrazioni contabili che presentano un numero limitato di caratteri, tale da far ritenere che la descrizione non possa essere considerata sufficiente e adeguata.
La *query* lanciata dal *software* è, quindi, finalizzata a confrontare le note con la lunghezza minima della descrizione configurata dall'utente.

Test di quadratura del libro giornale e del bilancio di verifica

Quest'ultima tipologia di controllo parte dall'assunto che il saldo dei conti esaminati tramite libro giornale coincida con quello derivante dal bilancio di verifica importato nell'apposita funzione di Revisya.
Partendo da tale presupposto, il controllo effettua una ricerca finalizzata ad individuare tutti i conti per i quali la considerazione di partenza non risulta verificata e che, quindi, presentano una squadratura rispetto al saldo contenuto nel bilancio di verifica.

Il risultato del controllo presentato all'utente è costituito dall'elencazione di tutti i conti per i quali è presente una squadratura con indicazione dei due saldi rilevati posti a confronto.

Figura 43 - Risultato quadratura del libro giornale con il bilancio di verifica



3.3.2 La circolarizzazione digitale

Le richieste di conferme esterne, comunemente denominate dal revisore "circolarizzazioni", sono procedure disciplinate dall'ISA Italia 505 che le definisce come *«elemento probativo acquisito come una risposta diretta in forma scritta al revisore da parte di un soggetto terzo (il soggetto circolarizzato), in formato cartaceo, elettronico ovvero in altro formato».*

Mediante tale tipologia di raccolta degli elementi probativi, il revisore può richiedere al soggetto terzo destinatario della richiesta, informazioni sui saldi contabili o su altri elementi specificamente individuati.

L'importanza di questa procedura risiede nella constatazione che le informazioni ottenute direttamente dal revisore e provenienti da soggetti terzi possono essere più attendibili rispetto a quelle fornite direttamente dalla società sottoposta a revisione[217]. Tale considerazione deriva dalla lettura dell'ISA Italia 500 che, al paragrafo A5, stabilisce che l'attendibilità degli elementi

[217] ISA Italia 505.

provativi raccolti dal revisore è influenzata dalla loro fonte di provenienza e dalla loro natura, inoltre dipende dalle circostanze specifiche in cui tali elementi sono acquisiti. Il paragrafo A31, inoltre, aggiunge che:

- Gli elementi probativi sono più attendibili quando sono acquisiti da fonti indipendenti esterne all'impresa;
- Gli elementi probativi acquisiti direttamente dal revisore sono più attendibili di quelli acquisiti indirettamente o per deduzione;
- Gli elementi probativi sono più attendibili ove esistano in forma documentale, sia essa cartacea, elettronica od in altro formato.

Per tutte le considerazioni contenute all'interno dell'ISA Italia 500, quindi, la procedura di richiesta di conferma esterna si configura come una delle procedure più importanti all'interno del processo di revisione proprio in quanto in grado di rispondere simultaneamente a tutti e tre gli elementi appena descritti.

La richiesta di comunicare o di confermare un saldo contabile si riferisce alla procedura di circolarizzazione eseguita nei confronti di soggetti quali clienti o fornitori per i quali è necessario verificare che vi sia corrispondenza tra quanto presente nella contabilità aziendale e quanto risulta dalla contabilità dei soggetti terzi coinvolti.

La richiesta di conferma esterna non viene inviata esclusivamente nei confronti di clienti e fornitori ma anche di soggetti quali banche, legali, consulenti fiscali, consulenti del lavoro, depositari di titoli e di merci, agenti, banche, società di leasing e di factoring, agenzie di assicurazione. L'elencazione, seppur non esaustiva di tutte le possibili richieste che possono essere inoltrate ai molteplici soggetti con cui la società opera, è esemplificativa dell'eterogeneità delle informazioni che possono essere acquisite tramite questa procedura.

Ai soggetti diversi dai clienti o fornitori possono essere richieste, infatti, informazioni su accordi, contratti, operazioni che l'impresa ha eseguito con altre parti, rapporti in essere con banche e altri intermediari finanziari.

La selezione dei soggetti nei confronti dei quali eseguire l'invio delle richieste è effettuata dal revisore sulla base di tre criteri di scelta:

- Intera popolazione: questo criterio viene utilizzato per tutte le categorie di soggetti da circolarizzare che non siano caratterizzati da una popolazione numerosa.
- Selezione campionaria: per le popolazioni numerose (normalmente dei clienti e dei fornitori) il revisore estrae un campione di soggetti a cui inviare la richiesta. Il revisore può utilizzare molteplici metodi di selezione di tipo statistico e non statistico in base ai

quali operare la successiva proiezione dei risultati ottenuti all'intera popolazione di riferimento.

- Selezione in base ad elementi specifici: la scelta dei soggetti da circolarizzare avviene sulla base di un criterio oggettivo (legato al piano di revisione), soggettivo (in base alla valutazione delle informazioni che il revisore intende ottenere dalla procedura) o in base alla presenza di elementi di anomalia riscontrati.

Le richieste di conferma possono essere di due tipologie:

- Richiesta di conferma positiva;
- Richiesta di conferma negativa.

La richiesta di conferma positiva presuppone che il soggetto circolarizzato risponda in ogni caso fornendo le informazioni contenute nella lettera o esprimendo di essere in accordo o in disaccordo con quanto comunicato.

La richiesta di conferma negativa, al contrario, richiede che la risposta sia fornita solo in caso di disaccordo con quanto comunicato. Tale seconda forma di richiesta di conferma, in realtà, non è utilizzata in modo frequente in quanto non rende possibile effettuare una distinzione tra le risposte non pervenute per inerzia del destinatario e le risposte effettivamente in accordo con quanto comunicato. Ciò costituisce un importante elemento di debolezza di questa tipologia di conferma se si considera che, in caso di mancata risposta o di risposta non attendibile, il revisore è tenuto a svolgere procedure alternative che gli consentano di ottenere elementi probativi sufficienti e appropriati mediante verifiche differenti.

Come stabilito dall'ISA Italia 505, la risposta ottenuta dalle controparti circolarizzate può presentarsi in formato cartaceo, in formato elettronico o in altro formato.

La richiesta di conferma esterna in formato cartaceo è sempre meno utilizzata, ma rappresenta la forma di circolarizzazione originaria su cui è stata costruita l'intera procedura. L'invio cartaceo presuppone la preparazione di una lettera per ciascuno dei soggetti selezionati come destinatari della richiesta. La lettera deve essere predisposta su carta intestata della società revisionata e sottoscritta dal legale rappresentante al fine di autorizzare il soggetto terzo coinvolto nella procedura a rilasciare le informazioni e i dati richiesti. Le lettere così ottenute sono, per prassi, inviate dal revisore ai destinatari tramite il servizio di posta ordinaria.

Le risposte, che il soggetto circolarizzato deve inviare presso la sede del revisore, sono raccolte e analizzate ai fini dei controlli e delle verifiche da eseguire in fase di risposta al rischio di revisione.

In caso di mancata risposta al primo invio, il revisore è tenuto ad eseguire un secondo invio: in

questo modo si è certi dell'avvenuta ricezione della richiesta che potrebbe essere andata persa e mai ricevuta dal destinatario nell'invio precedentemente effettuato.
In caso di mancata risposta anche al secondo invio eseguito dal revisore, egli può procedere a un sollecito prima di implementare procedure di revisione alternative che gli consentano di verificare le medesime informazioni in modalità differente.
Lo stesso iter procedurale è eseguito nel caso di invio tramite posta elettronica certificata. La circolarizzazione tramite *pec* richiede che la lettera, avente le medesime caratteristiche già analizzate per la tipologia cartacea, sia predisposta in formato *pdf/A* o in altro formato elettronico non modificabile. Il *file* così predisposto deve essere inviato come allegato al messaggio *pec* a tutti i soggetti selezionati dal revisore. Prima di eseguire l'invio è molto importante che il revisore verifichi l'autenticità degli indirizzi *pec* dei destinatari, per accertarsi della loro identità ed esistenza e gestire i probabili rischi correlati all'attendibilità delle risposte.
La procedura di circolarizzazione inserita all'interno di Revisya è stata completamente rivista e riprogettata in chiave digitale mediante la costruzione di una funzione dedicata esclusivamente all'esecuzione di questa attività. La funzione consente al revisore di gestire la procedura tramite una *dashboard* mediante la quale è possibile configurare e eseguire l'invio delle richieste nei confronti di tutte le possibili controparti.
La funzione dedicata alla circolarizzazione è, inoltre, direttamente collegata al *tool* del campionamento al fine di gestire l'intero processo mediante un unico flusso logico. Per eseguire il campionamento di una popolazione al revisore basterà, infatti, selezionare l'apposita opzione in fase di configurazione della procedura di circolarizzazione per ottenere il collegamento e il caricamento della popolazione importata all'interno della *dashboard* di gestione del campionamento. Le due funzioni risultano, in questo modo, completamente collegate: la popolazione importata tramite la funzione dedicata alla procedura di circolarizzazione viene trasferita alla funzione relativa al campionamento e, a sua volta, al termine dell'estrazione degli *item*, il campione sarà trasferito alla procedura di circolarizzazione per proseguire con le attività finali di configurazione e invio delle richieste.
La circolarizzazione all'interno di Revisya prevede, inoltre, due differenti modalità di invio delle richieste: una modalità manuale e una modalità automatica.
La modalità manuale è così definita in quanto presuppone che l'effettivo invio delle richieste venga gestito dal revisore al di fuori del *software*. In questo caso Revisya è utilizzato per:

- caricare i dati relativi alla popolazione di riferimento tramite *import* di un *file* in formato *excel*;

- configurare la procedura;
- selezionare tramite campionamento le controparti da circolarizzare (fase eventuale);
- tracciare i dati del soggetto che ha eseguito l'invio e della data di esecuzione;
- annotare le risposte ricevute e i risultati della procedura.

La procedura manuale prevede, quindi, che l'invio effettivo delle richieste venga gestito dal revisore al di fuori del *software* tramite posta ordinaria o mediante posta elettronica certificata seguendo le modalità "classiche" di esecuzione.

La vera rivoluzione nella modalità di gestione della procedura è rappresentata dalla tipologia di circolarizzazione automatica in base alla quale anche l'effettivo invio delle richieste è eseguito direttamente dal *software*. Utilizzando l'indirizzo di posta elettronica del revisore, indicato all'interno dei dati di configurazione, Revisya è in grado di inviare una *pec* all'indirizzo delle controparti circolarizzate. La *pec* contiene una breve spiegazione della procedura e un *link* cliccabile mediante il quale il destinatario può attivare un portale riservato grazie al quale poter:

- acquisire tutti gli elementi di dettaglio relativi alla richiesta;
- rispondere alle richieste del revisore utilizzando le funzioni messe a disposizione nel portale.

La modalità automatica rende la procedura particolarmente efficiente ed efficace in quanto consente di ridurre notevolmente i tempi di esecuzione del processo evitando l'*iter* di predisposizione delle lettere è l'invio singolo di ciascuna richiesta tramite posta ordinaria o *pec*. Contestualmente, questa modalità di gestione assicura un notevole aumento del tasso di risposta in quanto rende la procedura molto più snella e facile da gestire anche per i destinatari della richiesta.

Le risposte ricevute sono, inoltre, raccolte direttamente da Revisya e riepilogate all'interno dell'apposita *form* dedicata agli esiti della procedura. In questo modo, le attività di raccolta e di formalizzazione delle risposte sono gestite completamente in modo automatico azzerando il tasso di errore che può essere correlato all'esecuzione manuale di tali operazioni.

La procedura è, quindi, snellita e il revisore liberato da tutte le attività strettamente ripetitive e operative che la procedura tradizionale prevede. Il revisore può, in questo modo, dedicarsi alla valutazione e all'analisi delle risposte utilizzando il tempo risparmiato per attività caratterizzate da un più alto valore aggiunto per lo svolgimento dell'incarico.

3.3.3 I test sulle fatture elettroniche

La fatturazione elettronica è stata introdotta in Italia con la Legge Finanziaria del 2008 che ha obbligato, a partire dal 6 giugno del 2014, le pubbliche amministrazioni interessate all'emissione e alla ricezione di fatture in formato elettronico.

Con la Legge di bilancio 2018, l'obbligo di utilizzare la fatturazione elettronica è stato esteso anche ai soggetti privati per tutte le cessioni di beni e le prestazioni di servizi effettuate tra soggetti residenti o stabiliti nel territorio dello Stato. L'introduzione della fatturazione elettronica è avvenuto in più fasi che hanno coinvolto gradualmente più soggetti fino all'estensione dell'obbligo a tutte le operazioni B2B – *Business to Business*, quindi effettuate tra due operatori IVA, e alle operazioni B2C – *Business to Consumer* eseguite nei confronti di un consumatore finale.

Le fatture elettroniche sono trasmesse mediante il Sistema di Interscambio (SdI) che effettua un controllo automatico finalizzato alla verifica della presenza di tutte le informazioni obbligatorie previste dagli artt. 20 e 21-bis del D.P.R. 633/1972 e al controllo della partita iva o del codice fiscale di fornitori e clienti. Il Sistema di Interscambio, inoltre, certifica l'avvenuto invio o la ricezione della fattura tramite una ricevuta di recapito che attesta l'avvenuta trasmissione in modo sicuro al destinatario.

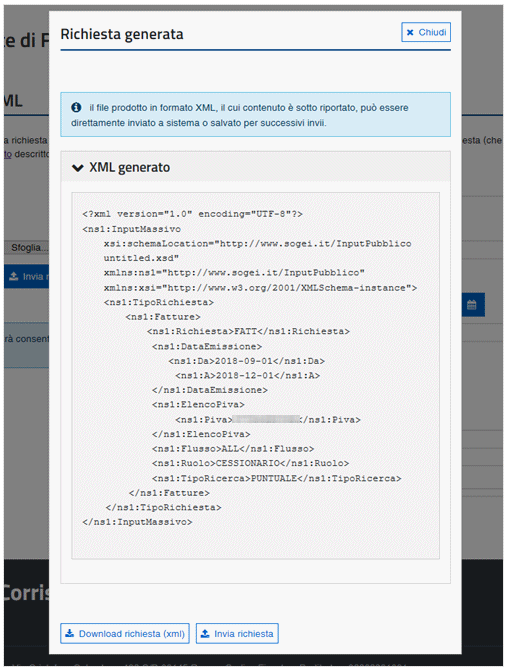
Il file deve essere predisposto in formato XML (*eXtensible Markup Language*) come previsto dal provvedimento dell'Agenzia delle Entrate del 30 aprile 2018 e viene archiviato all'interno del cassetto fiscale tra le fatture emesse o ricevute.

Le fatture possono essere successivamente estratte nel formato originale elaborato e utilizzato dal Sistema di Interscambio secondo la procedura prevista dall'Agenzia delle Entrate che prevede l'estrazione in seguito all'invio di apposita richiesta. Al termine dell'elaborazione, il richiedente ha la possibilità di procedere all'estrazione delle fatture ottenendo per ciascuna di esse il file XML della fattura e il file XML contenente i Metadati correlati che certificano l'autenticità del documento.

Il revisore può estrarre direttamente le fatture elettroniche della società sottoposta a revisione ottenendo le credenziali di accesso al cassetto fiscale ed eseguendo in autonomia la procedura prevista. In questo modo, il revisore ha la certezza di aver raccolto tutte le fatture inviate e ricevute tramite il sistema di interscambio evitando qualsiasi possibile alterazione o omissione da parte del cliente revisionato. Rispetto al precedente utilizzo delle fatture in formato cartaceo,

quindi, l'analisi delle fatture elettroniche conferisce un maggior grado di autorevolezza e di attendibilità alle procedure di revisione svolte.

Figura 44 - Tracciato XML fattura elettronica



Fonte: istruzioni al download massivo fornite dall'Agenzia delle Entrate sul sito https://www.agenziaentrate.gov.it/

Unica difficolta insita nell'utilizzo della fatturazione elettronica risulta essere costituito dalla necessità di convertire le informazioni contenute nel tracciato XML in un formato che ne agevoli la lettura e l'utilizzo da parte del revisore.

Per poter far fronte e gestire tale ultima esigenza, Revisya mette a disposizione degli utenti una funzione di conversione dei file zip generati dall'estrazione massiva delle fatture elettroniche dal cassetto fiscale. La funzione consente di caricare il file contenente tutti gli XML relativi alle fatture estratte e convertire in dati in forma tabellare tramite l'utilizzo di apposite *query.*

In pochi secondi il *software* rielabora le informazioni e le rende disponibili all'utente che potrà scegliere di scaricare la griglia generata in formato *pdf*, *xlsx* o *csv* per l'utilizzo nelle successive attività di revisione.

CONCLUSIONI

Il mio progetto di ricerca è nato con l'obiettivo di individuare e progettare strumenti e tecniche innovative da impiegare nell'attività di audit e revisione contabile al fine di migliorare l'efficienza e l'efficacia delle procedure e delle attività di revisione. Punti fondamentali di indagine sono stati l'analisi delle frodi e l'attività di individuazione delle stesse svolta da parte del revisore sulla base dei principi di revisione che ne guidano e ne disciplinano l'attività.

L'analisi delle frodi aziendali e dei principali schemi fraudolenti, così come dei modelli e delle principali teorie poste a supporto dello studio del fenomeno in esame sono stati oggetto del primo capitolo del presente lavoro. Tali studi sono stati fondamentali per poter definire il contesto di riferimento e il campo di indagine dell'attività di ricerca svolta.

Nel secondo capitolo sono stati, invece, indagati i confini della materia e l'ambito disciplinare di riferimento costituito dal *forensic accounting* e da tutte le discipline che, a vario titolo, rientrano nella medesima categoria, evidenziando le differenze e i punti di congiunzione con la materia della revisione contabile.

Il *background* teorico di riferimento ha costituito il punto di partenza per lo sviluppo degli approfondimenti relativi all'utilizzo dei sistemi esperti, dei *big data* e delle nuove tecnologie nell'ambito dell'attività di revisione contabile.

Come illustrato nel terzo capitolo dell'elaborato, gli studi e la ricerca teorica sono stati supportati e accompagnati da un'attività empirica svolta in forma di collaborazione alla realizzazione di un innovativo *software* di revisione. Il *software* è nato dalla riprogettazione delle procedure di revisione in chiave digitale e dall'utilizzo di tecniche avanzate di intelligenza artificiale e aumentata finalizzate a fornire al revisore strumenti sempre più efficienti ed efficaci. L'automatizzazione dei processi e l'utilizzo di procedure digitali non devono essere interpretati in un'ottica di sostituzione del lavoro umano con quello robotico ma di potenziamento delle attività. Le analisi e le procedure automatizzate rappresentano degli strumenti posti a supporto dell'attività del revisore che, partendo dai risultati o dalle previsioni elaborate dal software, è in grado di eseguire valutazioni più accurate e approfondite delle caratteristiche aziendali e degli eventuali segnali di anomalia presenti.

Il software è in grado, quindi, di guidare il revisore durante tutte le fasi di lavoro migliorando la qualità dell'attività di revisione, riducendo il livello di rischio e innalzando il livello di efficienza ed efficacia dell'attività.

La componente di intelligenza aumentata del software è posta a supporto delle decisioni dell'utente in quanto elabora i dati a disposizione confrontandoli con le variabili di riferimento e valutando le caratteristiche aziendali e del settore di riferimento proponendo un valore o una soluzione al revisore. Il software è in grado, inoltre, di valutare i rischi e la significatività delle poste ai fini della predisposizione di programmi di lavoro personalizzati e adatti a coprire tutte le asserzioni pertinenti. A ciò si aggiungono i molteplici strumenti di *Intelligent Data Analytics* quali l'elaborazione della centrale rischi, il campionamento, le analisi delle fatture elettroniche oltre alle funzioni dedicate ai test sul libro giornale e all'analisi di bilancio.

I risultati ottenuti grazie all'utilizzo del software hanno avuto importanti impatti nell'organizzazione del lavoro e nello svolgimento delle procedure aziendali. Innanzitutto, grazie all'utilizzo del software, è stato possibile riscontrare un forte miglioramento del lavoro in team e nella conseguente facilitazione della pianificazione del lavoro, della suddivisione delle attività, del monitoraggio della tempistica inserita a *budget* e nella conseguente *review* delle attività. Il miglioramento delle attività è stato ottenuto anche grazie al ruolo di guida svolto dal software, in particolare nei confronti degli utenti meno esperti che possono beneficiare di un sistema di *training on the job* che favorisce la formazione del personale e riduce l'incidenza degli errori commessi nell'esecuzione delle procedure e nella conseguente valutazione dei risultati.

L'estensione delle verifiche alle intere popolazioni oggetto di analisi ha fortemente migliorato le attività di revisione e l'efficacia dei controlli svolti. In particolare, le tecniche e gli strumenti finalizzati all'individuazione delle frodi e delle possibili manipolazioni di bilancio hanno dimostrato di essere pienamente efficaci nel distinguere casi effettivi di frode con un basso tasso di errore.

BIBLIOGRAFIA

- ACCOUNTANCY FUTURES ACADEMY, *Big Data: its power and perils*, The Association of Chartered Certified Accountants, Novembre 2013
- ACFE, Report to the Nations. 2020 Global Study on occupational fraud and abuse.
- AGNEW H., *Revisioni contabili, battaglia campale per le Big Four della consulenza*, Il Sole 24 ore, 23 maggio 2016.
- AICPA, Litigation Services and Applicable Professional Standards, Consulting Services, Special Report 03-1.
- ALBRECHT W.S., ALBRECHT C.O., ALBRECHT C.C., ZIMBELMAN M.F., *Fraud Examination*, Fourth edition, South-Western Cengage Learning, 2011.
- ALLEGRINI M., D'ONZA G., MANCINI D., GARZELLA S., *Le frodi aziendali*. *Frodi amministrative, alterazioni di bilancio e computer crime*, Franco Angeli, Milano, 2003
- ALLES M., GRAY G. L., The pros and cons of using big data in auditing: a synthesis of the literature and a research agenda, Settembre 2015.
- ANASTASI J., *The new forensics. Investigating Corporate Fraud and the Theft of Intellectual Property*, John Wiley & Sons, Inc., Hoboken, New Jersey, 2003.
- ASK U., MAGNUSSON J., BREDMAR K., *Big Data Use in Performance Measurement and Management: A Call for Action*, Journal of Business and Economics, Marzo 2016, Volume 7, No. 3.
- ASSOCIATION OF CERTIFIED FRAUD EXAMINERS, *Fraud Examiners Manual (International)*, 2011
- ASSOCIATION OF CERTIFIED FRAUD EXAMINERS, *Fraud Examiners Manual*, 2011.
- ATACK J., NEAL L., *The Origins and Development of Financial Markets and Institutions*, *The Mississippi Bubble revisited*, Cambridge University Press, 2009.
- BORSA ITALIA*, Il caso Madoff. Il truffatore, lo schema Ponzi e la condanna*, FTA Online News, Milano, 10 Lug 2009.
- COENEN T.L., Expert Fraud Investigation. A step by step guide, John Wiley & Sons, Inc, 2009.
- D'ALESSIO R., ANTONELLI V., BOZZA E., *Principi di Auditing. Concetti, modelli, metodologie, applicazioni*, Volume I, Edises, 2017.
- D'ALESSIO R., ANTONELLI V., Principi di Auditing. Concetti, modelli, metodologie, applicazioni, Volume I, Edises, 2021.

- DRAKE P.D., NIGRINI M.J., Computer assisted analytical procedures using Benford's Law, Journal of Accounting Education, Ed. 18 (2000) 127-146.
- EY, *Big Data and analytics in the audit process: mitigating risk and unlocking value*, EY Center for Board Matters, Settembre 2015
- GARBER P.M., *Famous First Bubbles: the fundamentals of early manias*, Cambridge, Mass MIT Press, 2000.
- GIANNOTTI F., *Big Data e Social Mining*, KDDLAB
- GIUNTA F., BINI L., DAINELLI F., *Verifica della base informativa per l'analisi di bilancio: le azioni di manipolazione contabile*, Controllo di gestione, n.2: 5-17, 2014.
- GIUSTI G., NOUSSAIR C., VOTH H-J, *Recreating the South Sea Bubble: Lessons from an Experiment in Financial History*, University of Zurich, 2014
- Global Economic Crime and Fraud Survey 2018 – Summary Italia (PWC)
- GOLDEN T.W., SKALAK S. L., CLAYTON M.M., *A guide to forensic accounting investigation*, John Wiley & Sons, Inc., Hoboken, New Jersey, 2006
- KRANACHER M.J., RILEY R., Forensic Accounting and Fraud Examination, Wiley, 2020.
- LIBRO VERDE, La politica in materia di revisione contabile: gli insegnamenti della crisi, 13 ottobre 2010.
- MCKINSEY, Big data: The next frontier for innovation, competition, and productivity, McKinsey Global Institute, Giugno 2011.
- MOEN J., *John Law and the Mississippi Bubble: 1718-1720*, Mississippi Historical Society, 2001.
- Nigrini M.J. A taxpayer compliance application of Benford's Law. The Journal of the American Taxation Association, 1996.
- NIGRINI M.J., Forensic Analytics. Methods and Techniques for Forensic Accounting Investigations, Wiley, First Edition.
- NUNES T., LEITE J., PEDROSA I., *Intelligent Process Automation: An Overview over the Future of Auditing*, 2020 15th Iberian Conference on Information Systems and Technologies (CISTI), 24 – 27 June 2020, Seville, Spain
- PASINI P., PEREGO A., Big Data: nuove fonti di conoscenza aziendale e nuovi modelli di management, Rapporto di ricerca per IBM, SDA Bocconi, 2012.
- PASQUINI M., *Bernie Madoff. Il grande illusionista di Wall Street*, Area51 Publishing s.r.l., San Lazzaro di Savena (Bologna), 2018

- POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali. Forensic accounting, fraud auditing e litigation*, Egea, 2012.
- PORTER B., *An Empirical Study of the Audit Expectation – Performance Gap*, Accounting and Business Research, Vol. 24, N. 93, 1993.
- PwC's Global Economic Crime e Fraud Survey, *Fighting fraud: A never-ending battle*, PWC, 2020
- S. AGHILI, *Fraud Auditing Using CAATT. A Manual for Auditors and Forensic Accountants to Detect Organizational Fraud*, CRC Press, 2019
- SCHUCHTER A., LEVI M., *The Fraud Triangle revisited*, Macmillan Publishers Ltd, 0955–1662 Security Journal, 2013.
- SICIGNANO G.J., *Bitcoin e riciclaggio,* G Giappichelli Editore, 2019
- SINGLETON T., SINGLETON A., BOLOGNA J., LINDQUIST R., Fraud Auditing and Forensic Accounting, Third Edition, John Wiley & Sons, Inc, 2006
- SINGLETON T., SINGLETON A., Fraud Auditing and Forensic Accounting, Four Edition, John Wiley & Sons, Inc, 2010.
- VONA L.W., *Fraud Risk Assessment. Building a Fraud Audit Program*, John Wiley & Sons, Inc., 2008
- VONA L.W., The Fraud Audit. Responding to the Risk of Fraud in Core Business Systems, John Wiley & Sons, Inc, 2011
- WELLS T. G., *International Fraud Handbook*, Wiley, 2018.
- WHITHOUSE T., *Auditing in the Era of Big Data*, Compliance Week, Aprile 2014.
- YUE D., WU X., WANG Y., LI Y., CHU C., A Review of Data Mining-Based Financial Fraud Detection Research, International Conference on Wireless Communications, Networking and Mobile Computing, Shanghai, 2007.

SITOGRAFIA

- https://inflosoftware.com.
- https://www.agenziaentrate.gov.it