LUISS Guido Carli
LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI

Facoltà di Impresa e Management

Corso di laurea in Amministrazione, Finanza e Controllo
Cattedra di Corporate Governance and Internal Auditing

LE FRODI ED IL SISTEMA DI INTERNAL AUDITING

RELATORE
Chiar.mo Prof. Scettri Simone

CANDIDATO
Viktor Tarroni
Matr. 708601

CORRELATORE
Chiar.mo Prof. Musaio Alessandro

ANNO ACCADEMICO 2019-2020

Prima di procedere con la trattazione, vorrei dedicare qualche riga a tutti coloro che mi sono stati vicini in questo percorso di crescita personale e professionale.

Ringrazio i miei genitori che mi hanno sempre sostenuto, appoggiando ogni mia decisione.

Un ringraziamento speciale va a Stefano Mango che mi ha aiutato a condurre le ricerche, oggetto dell'elaborato.

Infine, vorrei dedicare questo piccolo traguardo a me stesso, che possa essere l'inizio di un nuovo percorso.

INTRODUZIONE

'Gallici hostes tempus atque occasionem fraudis ac doli quarebant'.[1]

Sono queste le parole usate da Giulio Cesare nel Debello Gallico nel definire il tentativo da parte dei Galli di trovare il '*momento favorevole per un atto di inganno e di tradimento*', e sono queste le parole che ho intenzione di usare per introdurre il mio elaborato. Fin dall'antichità la frode ha sempre rappresentato un male innegabile della società. Già Petronio, nel I secolo D.C., in una delle sue opere maggiori il '*Satyricon*' descrive come l'alta società dell'Impero romano fosse caratterizzata da individui dediti alla corruzione ed ad altri comportamenti riprovevoli nella gestione del denaro pubblico.

Il tema delle frodi è qualcosa di intrinseco nell'indole umana come tentativo losco di prevalere scorrettamente nei confronti del prossimo, prossimo che si può identificare in un esercito nemico, o prossimo inteso come diretto concorrente all'interno dello stesso mercato. La frode intesa come inganno, si è evoluta notevolmente nel tempo, sfruttando al meglio quali fossero gli strumenti offerti dalla contemporaneità del periodo di appartenenza, e con il boom tecnologico, il concetto di frode ha raggiunto evoluzioni e mutazioni così rapide e sofisticate quasi da non poter esser più identificate e classificate.

Nel Primo capitolo analizzeremo le fattispecie caratterizzanti del sistema fraudolento nella sua generalità, successivamente andremo ad identificare gli strumenti necessari nella gestione delle frodi. Nel terzo e quarto capitolo seguiremo quella che è l'evoluzione normativa in tema di *Sistema di Controllo Interno.* In fine negli ultimi capitolo andremo a vedere del sistema fraudolento nel sistema bancario, assicurativo ed informatico.

[1] *De Bello Gallico. B.C.2,14,1*

L'obiettivo del presente elaborato risiede nel tentativo di ripercorrere e ricostruire quelli che sono gli schemi tipici e non di generali schemi di frode ed in parallelo considerare ed argomentare quelli che sono gli strumenti principali nati ed in continua evoluzione che mirano a contrastare la diffusione delle frodi societarie in diversi settori e canali del panorama moderno.

È fondamentale quindi assicurarsi l'esistenza e l'effettiva efficacia di strumenti di prevenzione, misurazione e ponderazione dei rischi che possono avere origine da operazioni fraudolente con il tentativo ultimo di fermare al nascere il susseguirsi di manovre illecite tra le righe della vita societaria. All'interno di questo elaborato, inizieremo con il definire gli elementi chiave che ruotano attorno al concetto di frode tenendo conto delle variabili esogene ed endogene che la influenzano.

Successivamente andremo ad analizzare i principali strumenti di identificazione e gestione del rischio di frode esistenti a livello nazionale ed internazionale, partendo dal d.lgs. n° 231/2001 per arrivare alla Fraud investigation e forensic accounting approach. Nel terzo capitolo invece ci soffermeremo sul Sistema di Controllo Interno come strumento di prevenzione, definendo quelle che sono tutte le sue sfaccettature; partiremo quindi dalla sua definizione fino ad arrivare all'analisi del Coso Report e della sua evoluzione.

Particolare attenzione verrà data al mondo delle frodi informatiche, assicurative e bancarie, che rappresentano un tema topico del sistema fraudolento moderno. Il lavoro mira ad analizzare e valutare se, gli strumenti preposti ad evitare azioni fraudolente, siano sufficientemente efficaci nel perseguire questo compito ed inoltre ad evidenziare i punti di rottura o di collasso degli stessi, con il fine ultimo di incrementare l'efficacia della prevenzione alle frodi.

CAPITOLO 1

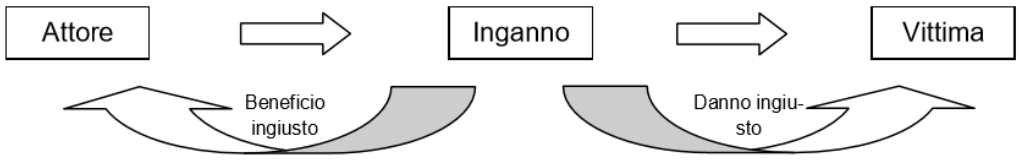
LA FRODE: FATTISPECIE, FATTORI CHE NE FAVORISCONO IL REALIZZO

1.1 Il concetto di frode

Punto centrale e fondamentale di questo elaborato ruota nel percorrere l'evoluzione in corso delle tecniche fraudolente moderne e non; nasce quindi l'esigenza di fornirne una definizione completa e tonda. Data la complessità della tematica e la sua continua evoluzione nel tempo e le numerose sfaccettature che può assumere; la definizione di frode muta e varia a seconda del contesto di riferimento. Tenendo conto di quello che viene riportato dal Treccani si definisce come frode:' *Atto o comportamento diretto a ledere con l'inganno un diritto altrui'*[2].

In entrambi i casi gli elementi essenziali per il compiersi di una frode si identificano; nell'attore e la vittima (elementi soggettivi) e nell'inganno, l'ingiusto guadagno e/o il danno (elementi oggettivi).

Tab.1.1.1 Lo schema fraudolento [3]



[4]

[2] *Treccani*

[3] *Allegrini M., et al., 2003*

[4] In particolare, la frode può essere commessa: dalla società (tramite i propri amministratori e rappresentanti) per ottenere un ingiusto vantaggio societario a danno di terzi soggetti o di dipendenti interni; da amministratori e dipendenti per ottenere vantaggi personali; da soggetti terzi che attuano comportamenti fraudolenti a danno della società, dei suoi amministratori o dei suoi dipendenti. Altro caso prevede la complicità tra soggetti terzi e amministratori per porre in essere comportamenti atti a frodare la società e gli azionisti. La distinzione tra frodi compiute a favore e a danno della società risulta assai sottile. La reale possibilità, infatti, di incorrere in danni di natura indiretta (deterioramento dell'immagine, crisi culturale, demotivazione personale, aumento dei costi, comportamenti imitativi, stato di conflitto interno) fa venire meno tale distinzione e quindi, gli atteggiamenti fraudolenti commessi in ambito societario si risolvono in effetti negativi e rischi per la stessa società, anche quando l'intento di partenza era diverso.

Elementi soggettivi

- Attore: colui o coloro che fattivamente, attraverso condotte commissive od omissive, pianificano ed eseguono con dolo lo schema fraudolento.
- Vittima: soggetti che subiscono direttamente o indirettamente le condotte illecite perpetrate dai frodatori.

Nel proseguire nel nostro lavoro dobbiamo identificare prioritariamente due tipologie diverse di errore:

- *errore intenzionale*
- *errore non intenzionale*

Nel primo caso, ci si riferisce ad un atto intenzionalmente e dolosamente posto in essere al fine di ottenere un vantaggio ingiusto o illecito.

Per errore non intenzionale, intendiamo sia l'errore materiale sia l'errore interpretativo sia quello consistente nell'impropria o mancata applicazione di un principio contabile o quello consistente nella disattenzione nel raccogliere informazioni e dati per un corretto trattamento contabile.

Inganno

L'inganno può essere indotto da:

1. *Raggiro*: imbroglio, inganno fatto per mezzo di parole tortuose e promesse allettanti o di altri mezzi idonei a sorprendere l'altrui buonafede.

2. *Artificio* presuppone una violazione della realtà esterna o della sua percezione volta a simulare circostanze inesistenti, a dissimulare o nascondere circostanze esistenti, a falsare la realtà fornendone una rappresentazione diversa e non vera.

3. *Silenzio malizioso*: l'attore per indurre la vittima in errore approfitta di una situazione di errore persistente 'serbando maliziosamente silenziò. Perciò sono i concetti di buona fede, correttezza e lealtà nei rapporti di lavoro e nelle dinamiche contrattuali di tipo commerciale che tracciano i confini del comportamento fraudolento.

Inoltre, nel determinare la condotta fraudolenta non si prende in considerazione la valutazione del grado d'ingenuità del soggetto truffato e non rileva neppure il grado di sofisticazione raggiunta per mettere in atto l'intento. Da una analisi svolta dall'Acfe [5]nel corso del 2020, riguardante il 2019 è emero come nell'opinione comune, le società targhettizzate come raggirabili riguardavano servizi bancari e finanziari, il governo e la pubblica amministrazione e l'industria manifatturiera. Sulla base dei questionari somministrati da ACFE le perdite economiche imputabili a frodi assumono valori maggiori nel settore minerario ed energetico (l'industria mineraria ha subito la più alta perdita di 475.000 USD, mentre le frodi nel settore dell'energia hanno avuto la perdita mediana più alta di 275.000 USD.)

[5] L'Associazione degli esaminatori di frodi certificati è un'organizzazione professionale di esaminatori di frodi. Le sue attività comprendono la produzione di informazioni, strumenti e formazione sulle frodi. Con sede ad Austin, in Texas, l'ACFE è stata fondata nel 1988 da Joseph T. Wells

Tab.1.1.2 Tipologia di frodi dichiarate dalle organizzazioni nel 2019[6]

[6] *Report of the Nation*

Da una semplice analisi dei dati forniti dall'Acfe possiamo al meglio analizzare la correlazione Median Loss e Cases. Possiamo intuitivamente notare come non vi sia una costante relazionale tra perdita in valore economico e casi per settore. Il settore infatti più colpito come numero di casistiche è il settore bancario, pur non avendo avuto il danno economico più alto tra i settori presi in analisi dall'Acfe.

1.2 'Il triangolo della frode'

I primi studi tracciati sulla prevenzione della criminalità à risalgono già al XIX secolo da parte di studioso quale Cesare Beccaria [7]e Jeremy Bentham[8], i quali sostenevano che i criminali sono esseri razionali che agiscono con lo scopo di massimizzare il soddisfacimento dei propri bisogni e il proprio benessere. Altri studiosi come N. Shover [9]e K.M. Bryant[10], sostenevano che la valutazione dei vantaggi dell'azione criminale da parte di un individuo fosse condizionata da tre precisi fattori: la *pressione* per il raggiungimento degli obiettivi, la *certezza* e la *severità* delle sanzioni percepite come possibili conseguenze negative in caso di scoperte e, da ultimo, la *cultura*, propria della situazione di appartenenza, volta all'accettazione e agevolazioni di condotte criminali.

Queste variabili sono state poi prese e sviluppate dal ricercatore americano Donald R. Cressey [11]che, a seguito di un'indagine empirica sulle frodi svolta negli anni Cinquanta, ha elaborato una teoria che, ad oggi, è la più adatta per comprendere il perché vengano attuate azioni fraudolente.

[7] Cesare Beccaria è stato un giurista, filosofo, economista e letterato italiano, del XVII secolo.
[8] Jeremy Bentham è stato un filosofo e giurista inglese. Fu un politico radicale e un teorico influente nella ù filosofia del diritto anglo-americana.
[9] Neal Shover è un accademico americano specializzato in white collar crime.
[10] K.M. Bryant è un esperto americano in forensic account e fraud auditing.
[11] Donald R. Cressey era un penologo, sociologo e criminologo americano che ha dato contributi innovativi allo studio della criminalità.

Tale teoria, meglio nota come the *fraud triangle*, sancisce che ogni frode presenta tre elementi caratterizzanti:

1) *Incentivi e pressioni*; fattori esterni quali ad esempio un target aziendale ritenuto non raggiungibile o la necessità di denaro, possono indurre il frodatore a compiere illeciti.

2) *Opportunità*; l'attore della frode prefigura la possibilità di commettere l'atto fraudolento grazie all'identificazione, dettata dall'esperienza, di punti deboli nel sistema dei controlli interni o di c. collaborazioni interne/esterne

Sul punto si precisa che l'assenza o la superficialità dei controlli è imputabile all'esistenza di rapporti fiduciari fra i preposti alle attività di controllo e i responsabili dei reati, tali da aumentare la probabilità di accadimento degli stessi.

Va rilevato come generalmente l'opportunità di commettere una frode sia direttamente proporzionale alla durata del rapporto di lavoro con quella particolare società, per il semplice fatto che una collaborazione pluriennale consente ai singoli soggetti di venire a conoscenza delle debolezze e delle lacune del sistema di controllo interno, fornendo loro una potenziale occasione per mettere in atto la frode.

Il meccanismo della razionalizzazione consiste nell'abilità dell'attore di riuscire a giustificare a sé stesso e, qualora fosse scoperta, anche agli altri membri dell'organizzazione, la frode realizzata.

Questo accade perché il frodatore non si identifica in un criminale. Sfruttando questa catena irrazionale anche i dipendenti più onesti sono potenzialmente capaci commettere reati fraudolenti.

La forma di razionalizzazione più frequente consiste nel trasformare il reato (ad es. un furto di cassa) in un 'altra azione (ad es. un prestito temporaneo ottenuto dall'azienda), trovando così una giustificazione al comportamento criminale.[12]

Sebbene la razionalizzazione sia un processo di natura soggettiva, alcune variabili connesse all'ambiente societario, come il comportamento del management e la gestione del personale, possono inconsapevolmente innescare il suddetto meccanismo psicologico.

Tenendo fede a quello che è lo scenario mondiale nel corso di questo 2020 non possiamo non riportare di seguito alcune considerazioni che enucleano tali aspetti con riferimento specifico al rischio di frode correlato alla vicenda COVID-19.

Nel corso di questa fase dell'emergenza da COVID-19 si riscontrano perlomeno due fattori standard che fisiologicamente aumentano il rischio di frode all'interno di una società; l'obiettivo immediato del management riguarda il contenimento dell'impatto economico-patrimoniale degli effetti dell'emergenza sul business per salvaguardare la continuità della propria impresa nel breve periodo ed lo scenario in cui l'impresa opera è costantemente mutevole e si adatta agli sviluppi dell'emergenza, dettati ad esempio da provvedimenti d'urgenza emanati dal Legislatore per contenere gli impatti negativi legati alla vicenda.

In questo contesto uno dei principali esempi di opportunità legata alla commissione o tentata commissione di frodi è rappresentato dal ricorso allo smartworking nelle realtà in cui il processo non era normato prima dell'emanazione dei recenti DPCM che ne prevedono l'adozione.

[12] "Le Frodi Aziendali: frodi amministrative, alterazione di bilancio e computer crime. Marco Allegrini, Giuseppe D'Onza, Daniele Mancini, Stefano Garzella- Franco Angeli, 2003.

I principiali rischi sono dettati da:

- La mancanza di un framework di controllo che garantisca livelli di performance dei dipendenti assimilabili alla situazione pre-COVID-19 e prevenga comportamenti non etici messi in atto dagli stessi;
- L'impossibilità di svolgere alcuni controlli da remoto in quanto non è prevista la versione, ove possibile, automatizzata degli stessi;
- Il proliferare di schemi di frode che basano la propria riuscita sulla difficoltà di comunicazione tra soggetti fisicamente distanti. Si pensi ad esempio alla cd. "CEO Fraud", in cui il frodatore inoltra ad un dipendente del dipartimento amministrativo una e-mail fake in cui, spacciandosi per l'AD, richiede, in deroga alle procedure in vigore, la disposizione urgente di un pagamento a favore di un beneficiario a lui riconducibile.

  In questo contesto il soggetto interno incline a comportamenti fraudolenti, se a conoscenza del funzionamento del sistema di controllo interno e dei relativi punti di debolezza causati dalla situazione di emergenza attuale, ha l'opportunità di compiere o tentare di compiere azioni illecite volte ad ottenere un beneficio personale a danno dell'azienda o terzi. In un contesto di crisi ed incertezza come quello provocato dal COVID-19, comportamenti comunque giudicati fraudolenti tendono ad essere giustificati più facilmente dal soggetto che commette o tenta di commettere l'illecito perché messi in atto al fine salvaguardare un interesse reputato più meritevole di tutela.

  I soggetti apicali in questa fase, ad esempio, potrebbero tollerare maggiormente condotte non lecite perché risulterebbero in linea di principio finalizzate al contenimento degli impatti della crisi e permetterebbero di continuare a pagare gli stipendi dei propri dipendenti.[13]

[13] "Il rischio di frode ai tempi del COVID-19", Fabrizio Santaloia e Stefano Mango, LinkedIn (https://www.linkedin.com/pulse/il-rischio-di-frode-ai-tempi-del-covid-19-fraud-risk-santaloia/?trackingId=BEKqPYcqI5546BY98x7%2FxA%3D%3D), Marzo 2020

1.3 Fattori che agevolano la diffusione delle frodi

Schematizzare gli elementi che portano un soggetto a compiere atti fraudolenti, tenendo conto del fatto che le fonti delle frodi sono differenti anche a seconda del ruolo ricoperto dal perpetratore; rende quasi impossibile riscostruire un modello unico in grado di delineare un meccanismo univoco.

Se prendiamo come esempio i *white collar crime* e li mettiamo a confronto con le *corporate fraud* possiamo con semplicità identificare leve e ragioni diverse pur avendo come risultato il compiersi di una frode. Secondo Bologna gli elementi che danno luogo a queste reazioni fraudolente sono le seguenti:

- Ideologico, quali la consapevolezza di vivere in un sistema dove gli stessi supervisori commettono delle azioni scorrette senza subire delle conseguenze o con la più diffusa idea che la frode possa essere un guanto di sfido verso la società presso cui si presta la propria attività.
-
- Economico, quali la volontà o esigenza di arricchirsi velocemente, per sopperire a posizioni finanziarie personali negative o semplicemente per il raggiungersi di un posizionamento economico non altrimenti perseguibile dalla propria posizione lavorativa.
- psicologico, quali la perdita dei propri freni inibitori o il verificarsi di una serie di fatti personali che mettono in discussione la propria integrità morale.

Nel valutare questi elementi bisogna tenere costo che oltre a fattori di natura personale, esistono un insieme di fattispecie esterne collegate all'ambiente di lavoro ed al collocamento dell'impresa che influenzano le scelte decisionali fraudolente del soggetto. Quando si parla di frodi derivanti da fattori interni bisogna tenere conto di quelle che nascono e si sviluppano a causa di carenze nel sistema di con trollo interno della società. In questi casi, in sostanza, è la stessa società è carente di misure di prevenzione efficaci.

Possiamo riconoscere qua sotto alcuni degli elementi interni che possono influire sul livello di qualità del sistema di controllo interno;

- il grado di separazione dei compiti;
- -le modalità di effettuazione delle pianificazioni e dei controlli su di esse; ù
- le vie intraprese per la gestione dei rapporti con il personale;
- lo stile di direzione e le deleghe di responsabilità;
- l'assenza di codici etici realmente attuati nella società e non riconosciuti dai dipendenti.

Considerando invece quelle che sono le fattispecie esterne, rilevanti nell'effettuazione o meno di frodi nella società identifichiamo come elementi ambientali:

- il livello generale dell'economia in cui la società opera;
- il livello di competitività del settore di appartenenza;
- l'efficacia e l'efficienza del sistema giudiziario del paese;
- il livello e la qualità degli organi preposti alla prevenzione ed individuazione delle frodi;
- la presenza di legislazioni a carattere specifico (ad esempio leggi antiriciclaggio).

Non essendo verosimile stendere un qualsivoglia elenco in grado di racchiudere al suo interno gli elementi interni ed esterni in grado di delineare i presupposti di una frode, l'attività di analisi e valuta zione dei fattori esterni che possono in una società costituire il motivo scatenante di frodi societarie è estremamente complessa è, per tale ragione, spesso delegata ad esperti esterni [14].

[14] *Laganà G., Gallo Riva P., Mastromarchi D., 1995*

1.4 Tassonomia ed i soggetti coinvolti

Un'altra distinzione in merito alla generale distinzione delle frodi riguarda le frodi interne e quelle esterne.

Le prime sono attuate da soggetti che hanno legittimo accesso agli edifici, agli asset e ai documenti contabili aziendali (manager, impiegati e collaboratori a tutti i livelli). Le seconde invece sono commesse da soggetti esterni, oppure che entrano in contatto con l'azienda in virtù di relazioni legittime (clienti, fornitori, equiparati a soggetti interni). Esiste poi una categoria mista, nella quale possono essere quelli illeciti compiuti grazie alla collaborazione tra un membro dell'organizzazione e un soggetto esterno.[15]

Con l'obiettivo ultimo di combattere e limitare la diffusione delle frodi, il primo Passo che deve essere fatto è quello di classificare e riconoscere gli schemi di frode potenzialmente attuabili dentro l'impresa; a tale scopo interviene l'*Association of Certified Fraud Examiners* (AFCE)[16]. La mission di questa associazione risiede nel tentativo '*to reduce the incidence of fraud and white-collar crime and to assist the membership in fraud detection and deterrence.'*[17]

L'ACFE istituisce poi un'ulteriore classificazione, considerata universalmente come la più autorevole, relativamente alle occupational fraud [18]. In tale ambito, secondo l'ente, i comportamenti fraudolenti possono essere suddivisi in:

- le frodi di bilancio informativa finanziaria (financial statement fraud);
- l'appropriazione indebita di beni (asset misappropriation);
- la corruzione (corruption).

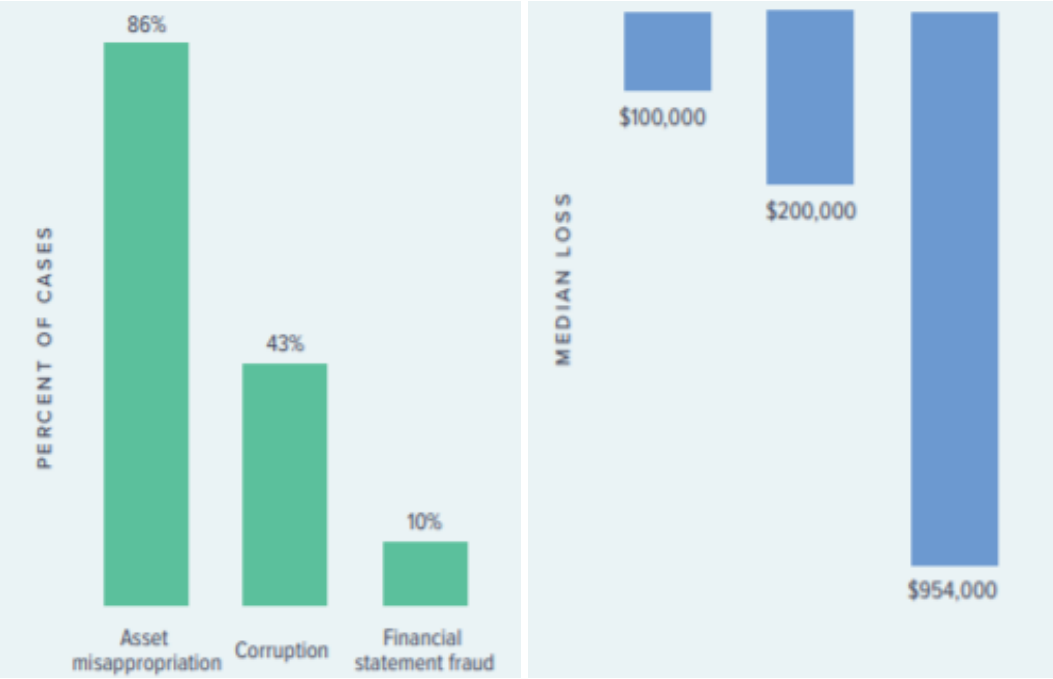
[15] Tratto da: "Frodi aziendali" Ed. Egea (2012) - Giuseppe Pogliani, Nicola Pecchiari, Marco Mariani

[16] *L'ACFE è la più grande organizzazione antifrode del mondo e il principale fornitore di formazione e istruzione antifrode. Insieme a più di 85.000 membri, l'ACFE sta riducendo le frodi commerciali in tutto il mondo e sta ispirando la fiducia del pubblico nell'integrità e nell'obiettività all'interno della professione.*

[17] *AFCE Web Site_Mission*

[18] Le frodi professionali sono quelle in cui un dipendente, un manager, un funzionario o il proprietario di un'organizzazione commette una frode a danno di tale organizzazione.

Tab.1.4.1 ***Dati in merito a Percent of Class & Median Loss***[19]



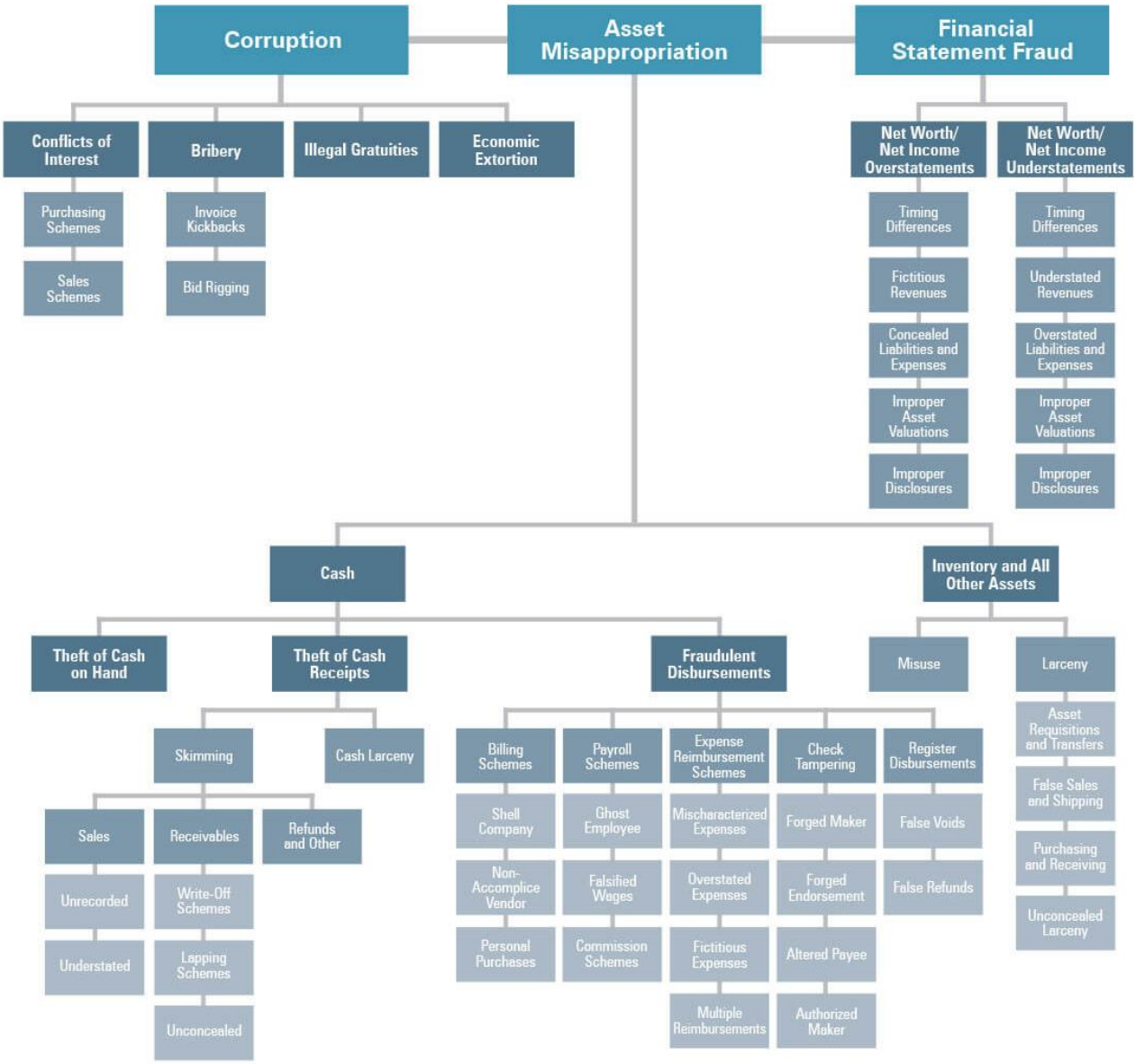
Al livello più alto del *Fraud Tree*, ci sono le tre categorie principali di frodi professionali. Malversazione di beni (*Asset Misappropriation*), riguardante un dipendente che ruba o utilizza in modo improprio le risorse dell'organizzazione che lo impiega, si verifica nella maggioranza delle casistiche (86% dei casi); tuttavia, anche questi schemi tendono a causare la perdita mediana più bassa a 100.000 USD per caso (vedere la tabella sopra riportata). Al contrario, la frode a livello di bilancio (*Financial Stament Fraud*), in cui l'autore del reato provoca intenzionalmente un'inesattezza o un'omissione materiale nella gestione finanziaria dell'organizzazione, sono i meno comuni (10% degli schemi), ma la categoria di frode professionale più costosa. La terza categoria, la corruzione - che comprende reati come la corruzione, i conflitti di interesse e l'estorsione - cade nel mezzo in termini di sia la frequenza che i danni finanziari. Questi schemi si verificano nel 43% dei casi e causano una perdita mediana di 200.000 dollari.

[19] *I dati sono stati estrapolati dal sito dell'ACFSE "Report to the Nations" (2020).*

Di seguito è riportata la classificazione completa delle frodi professionali, spesso indicate come l'Albero delle Frodi.

Tab.1.4.2 *'The Fraud Tree, occupational fraud and abuse classification system'*

20



[20] *"The Fraud Tree, occupational fraud and abuse classification system"; ACF*

Le prime due sono a loro volta citate anche nel SAS 99[21] il quale, dopo aver definito le frodi come atti intenzionali che sfociano in errori materiali del bilancio, classifica tali inesattezze contabili in:

- rendiconto finanziario fraudolento (fraudolent financial reporting);
- appropriazione indebita di beni patrimoniali (misappropriation of assets).

Corruzione

Se ponessimo l'attenzione alla definizione di *"Corruption"* data dall'ACFE, ritroviamo una definizione coerente e contemporanea all'interno del report "*Contract and Procurement Fraud Bribery and Corruption",* presentato all'interno di un corso di formazione nel 2020[22]. Secondo quanto illustrato nel report si definisce come *corruzione*

L'uso illecito dell'influenza per procurarsi un beneficio per l'attore o per un'altra persona.

Definisce come corruzione l'offerta, il dare, il ricevere o la sollecitazione di qualsiasi cosa di valore per influenzare un atto ufficiale o decisione aziendale.

Due tipi:

- Corruzione commerciale: La corruzione di un privato individuo per acquisire un'attività commerciale o vantaggio commerciale.
- Corruzione ufficiale: La corruzione di un pubblico ufficiale per influenzare un atto ufficiale di governo.

[21] *SAS (Statement on Auditing Standards) 99 definisce la frode come un atto intenzionale che si traduce in un'inesattezza sostanziale del bilancio. Sono considerati due tipi di frode: le dichiarazioni errate derivanti da un rendiconto finanziario fraudolento (ad es. falsificazione di registrazioni contabili) e le dichiarazioni errate derivanti da un'appropriazione indebita di beni patrimoniali (ad es. furto di beni patrimoniali o spese fraudolente).*

[22] Si tratta di un corso mirato alla consapevolezza delle vulnerabilità e dei rischi associati agli schemi di frode che attaccano le funzioni di acquisto, approvvigionamento e appalto.

Per quello che concerne il Corrupt Payments, l'ACSE identifica in dieci fattispecie le forme di pagamento:

1. Inappropriate or excessive gifts or favors
2. "Loans"
3. Personal use of credit cards or payment of credit card bills
4. Sexual favors
5. Overpaying for purchases
6. Free use of or discounted rent for housing or vehicles
7. Outright payments via cash or check
8. Hidden ownership interests
9. Selling or leasing property at less than FMV
10. Promises of favorable treatment

Altra "voce" da considerare in tema di corruzione è quanto viene detto da *Transparancy Information*[23].

"We define corruption as the abuse of entrusted power for private gain."

Sono queste le parole utilizzate dal sito per definire al meglio in concetto di frode. Secondo Transarancy la corruzione erode la fiducia, indebolisce la democrazia, ostacola lo sviluppo economico e aggrava ulteriormente la disuguaglianza, la povertà, la divisione sociale e la crisi ambientale. Esporre la corruzione e chiedere conto ai corrotti può avvenire solo se comprendiamo il modo in cui la corruzione funziona e i sistemi che la rendono possibile.

[23] *Si tratta di un sito riguardante la condivisione di dati che rivelano come le norme e gli interventi del governo e delle società influiscano su privacy e sicurezza dei dati nonché sull'accesso agli stessi.*

Secondo ACFE, l'atto corruttivo è mascherato in contabilità attraverso l'esecuzione di transazioni con terze parti apparentemente legittime ma mosse esclusivamente da finalità corruttive:

- Selezione errata di prodotti/servizi da acquistare
- Un pagamento eccessivo per prodotti/servizi
- Accettare prodotti/servizi di bassa qualità
- Accettare merci o servizi tardivi, brevi o mai consegnati
- Accettazione di fatture per beni/servizi mai pervenuti

Falsa informativa finanziaria

Negli ultimi anni, complice anche la crisi economica, il rischio di alternazione dolosa della rappresentazione della situazione economico-patrimoniale-finanziaria nel bilancio delle società è aumentato. Le ragioni che portano ad una manipolazione di quanto rappresentato in bilancio può avvenire per diverse ragioni, tra queste riconosciamo:

• Incoraggiare gli investimenti attraverso la vendita di azioni

• Per dimostrare l'aumento dell'utile per azione o dell'interesse sui profitti della società, quindi permettendo di aumentare i pagamenti di dividendi/distribuzione

• Per coprire l'incapacità di generare flussi di cassa

• Per evitare percezioni negative del mercato

• Ottenere finanziamenti o condizioni più favorevoli sui finanziamenti esistenti

• Ricevere prezzi di acquisto più elevati per le acquisizioni

• Dimostrare il rispetto dei patti di finanziamento

• Per raggiungere gli obiettivi e le finalità aziendali

• Ricevere i bonus legati alle prestazioni

In questo contesto il legislatore con l'intento di sanzionare le condotte di falso in bilancio e ridurre il rischio di frode è intervenuta andando a modificare la fattispecie di reato di *'false comunicazioni sociali*, di cui agli articoli 2621[24] e 2622 [25]del Codice civile.

L'oggetto materiale del reato è individuabile nei bilanci, nelle relazioni, nelle altre comunicazioni sociali, che siano previste dalla legge e rivolte ai soci o al pubblico. Ciò che differenzia profondamente, e caratterizza, le due fattispecie, oltre alla natura, contravvenzionale nell'ipotesi di cui all'art. 2621, delittuosa in quella di cui all'art. 2622, è la previsione di un evento di danno all'art. 2622.

Si può così osservare che il falso si realizza quando si rappresenta ad altri una realtà in modo difforme da ciò che è e quando i terzi, di questa falsa rappresentazione, abbiano avuto effettivamente la percezione; siano restati, in altri termini, ingannati. Con la Legge n. 69/2015 è stato modificato l'impianto normativo del reato di 'false comunicazioni sociali' contenuto negli articoli 2621 e 2622 del Codice civile, con l'intento di sanzionare in modo più severo le condotte di falso in bilancio e di ostacolare la corruzione nella Pubblica Amministrazione.

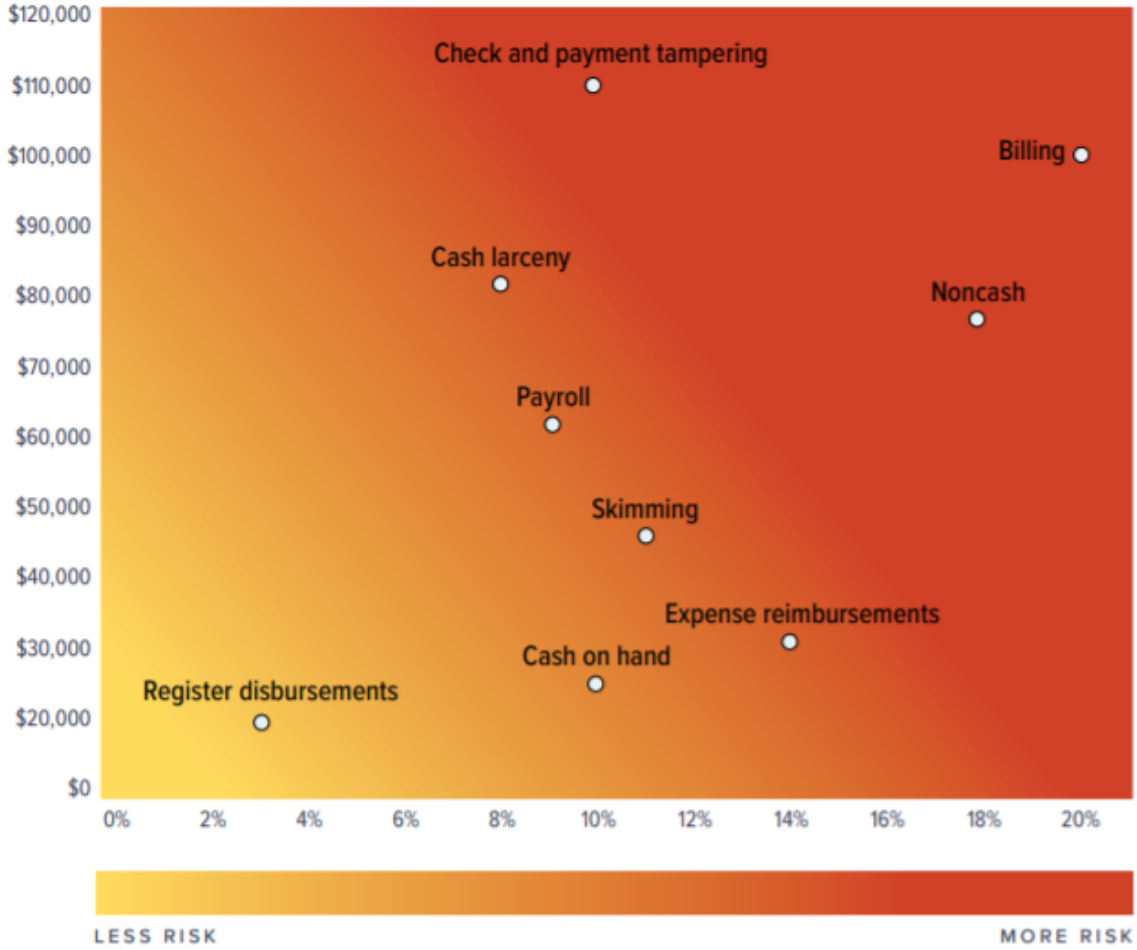
[24] ["Fuori dai casi previsti dall'art. 2622, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, i quali, al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali dirette ai soci o al pubblico, previste dalla legge, consapevolmente espongono fatti materiali rilevanti non rispondenti al vero ovvero omettono fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale la stessa appartiene, in modo concretamente idoneo ad indurre altri in errore, sono puniti con la pena della reclusione da uno a cinque anni….]"

[25] "[Gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società emittenti strumenti finanziari ammessi alla negoziazione in un mercato regolamentato italiano o di altro Paese dell'Unione europea, i quali, al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali dirette ai soci o al pubblico consapevolmente espongono fatti materiali non rispondenti al vero ovvero omettono fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale la stessa appartiene, in modo concretamente idoneo ad indurre altri in errore, sono puniti con la pena della reclusione da tre a otto anni..]

La Legge n. 69/2015 ha modificato il contenuto dei citati articoli introducendone altri due: gli articoli 2621-bis e 2621-ter riguardanti i fatti di lieve e particolare tenuità. Le principali modifiche apportate sono: l'illecito assume la natura di reato di mero 'pericolo' e non di 'danno' per cui può essere attivato a prescindere dalle querele di parte; eliminazione degli specifici indici di rilevanza della condotta delittuosa che precludevano la configurazione dell'illecito qualora non superati.

Al fine, quindi, di capire quando si configura il reato di falso in bilancio è opportuno analizzare la differenza riscontrabile tra: errore e frode, in quanto solo al verificarsi della frode si riscontra la fattispecie di reato. Ultimo aspetto da sottolineare sul reato di falso in bilancio è che lo stesso è stato rubricato tra i *'reati di pericolo* 'ed in pratica non è necessario dimostrare l'effettivo danno frutto di comportamenti contabili illeciti, per configurare il reato, ma è sufficiente una comunicazione motiva di frode aziendale, esperibile anche da parte dell'Agenzia delle Entrate o dalla Guardia di Finanzia, nel corso di una normale attività di accertamento.

Tab.1.4.3 ***Sub-Schema di appropriazione indebita di beni***[26]



Category	Number of Cases	Percent of All Cases	Median Loss
Billing	430	20%	$100,000
Noncash	395	18%	$78,000
Expense reimbursements	310	14%	$33,000
Skimming	230	11%	$47,000
Cash on hand	224	10%	$26,000
Check and payment tampering	206	10%	$110,000
Payroll	199	9%	$62,000
Cash larceny	169	8%	$83,000
Register disbursements	55	3%	$20,000

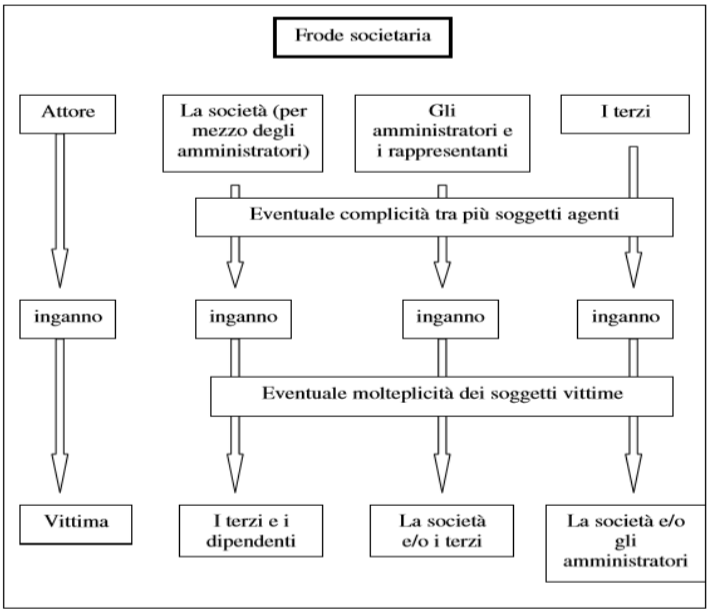
[27]

[26] *I dati sono stati estrapolati dal sito dell'ACFSE "Report to the Nations" (2020).*

[27] *Billing scheme: Schema in cui una persona induce il proprio datore di lavoro ad emettere un pagamento presentando fatture per beni o servizi fittizi.*
Noncash misappropriations: Qualsiasi schema in cui un dipendente ruba o abusa di beni non in contanti dell'organizzazione della vittima.
Expense reimbursements scheme: Uno schema di rimborso spese fraudolento.

All'interno dell'ampia categoria dell'appropriazione indebita di beni, i truffatori utilizzano diversi metodi per rubare fondi e altri risorse dai loro datori di lavoro. Il grafico soprariportato mostra la frequenza e la perdita di ogni categoria di appropriazione indebita di beni. I sistemi di fatturazione sono la forma più comune di appropriazione indebita di beni e causano anche un'elevata perdita, rendendo questo tipo di frode molto significativo. Altre frodi ad alto rischio, basate sulla combinazione di frequenza e impatto, sono la manomissione dei controlli e dei pagamenti, così come gli schemi che comportano il furto di beni non in contanti.

Tab.1.4.4. La Frode Societaria [28]



Skimming: Uno schema in cui un pagamento in entrata viene rubato da un'organizzazione prima di essere registrato nei libri e nei registri dell'organizzazione.
Cash-on-hand misappropriations: Uno schema in cui l'autore del reato si appropria indebitamente di denaro contante tenuto a portata di mano presso la sede dell'organizzazione della vittima.
Check or payment tampering scheme: Uno schema di erogazione fraudolenta in cui una persona ruba i fondi del proprio datore di lavoro intercettando, falsificando o alterando un assegno o pagamento elettronico.
Payroll scheme: Un sistema di erogazione fraudolenta in cui un dipendente fa sì che il suo datore di lavoro emetta un pagamento facendo richieste di risarcimento false.
Cash larceny: Uno schema in cui un pagamento in entrata viene rubato da un'organizzazione dopo che è stato registrato nei libri e nei registri dell'organizzazione .
Register disbursements scheme: Uno schema di esborso fraudolento in cui un dipendente effettua false registrazioni su un registratore di cassa per nascondere la rimozione fraudolenta di denaro contante

[28] *"Le Frodi Aziendali: frodi amministrative, alterazione di bilancio e computer crime". Marco Allegrini, Giuseppe D'Onza, Daniele Mancini, Stefano Garzella- Franco Angeli, 2003*

Spesso errori significativi di una falsa informativa economico-finanziaria riguardano la sopravvalutazione dei ricavi (ad esempio, attraverso la loro rilevazione anticipata o la registrazione di ricavi fittizi) o la loro sottovalutazione (per esempio, attraverso il loro non corretto rinvio ad un esercizio successivo). Se si presume che vi siano rischi di frode nella rilevazione dei ricavi, si deve valutare quali tipologie di ricavo, operazioni di vendita o asserzioni possono dar luogo a tale rischio. Una volta identificati e valutati tali rischi si devono svolgere le procedure di verifica giudicate più opportune nella fattispecie.

Le voci principalmente colpite sono;

- Attività o ricavi sopravvalutati, costi delle attività o ricavi artificiali
- Passività e spese sottovalutate

Questo attraverso una manipolazione di:

- Ricavi fittizi
- Differenze di tempistica
- Valutazione errata degli asset
- Passività e spese nascoste
- . Informativa impropria

Nella redazione del bilancio, la direzione ha la responsabilità di effettuare numerose valutazioni e assunzioni che riguardano le stime contabili significative ed ha la responsabilità di controllare la ragionevolezza di tali stime su base ricorrente. Una falsa informativa economico-finanziaria è spesso realizzata con stime contabili intenzionalmente non corrette. In caso di operazioni significative bisogna considerare se la motivazione economica sottostante alle operazioni (o la sua eventuale assenza) suggerisce che le operazioni siano state poste in essere per realizzare una falsa informativa economico-finanziaria o per nascondere appropriazioni illecite di beni e attività dell'impresa.

Tra le voci di bilancio sensibili ad azioni fraudolente riconosciamo anche i le consulenze e le intermediazioni fittizie; la tecnica, piuttosto semplice, è quella di utilizzare fatture per prestazioni di consulenza inesistenti o di valore nettamente inferiore allo scopo di creare indebite disponibilità per gli amministratori. Spesso tale tecnica è utilizzata anche dai gruppi societari per management *fees* addebitate da società in paesi a fiscalità privilegiata. Al fine di individuare e prevenire questo tipo di frode è opportuno andare a verificare tutti i costi per servizi più significativi, ed anche i costi legati alle intermediazioni, controllando che siano sottoposti a procedure rigide sia nella fase di creazione del rapporto, che nella fase di pagamento.

Non devono esserci deviazioni dalle ordinarie procedure (ad esempio, un agente che viene seguito direttamente dalla direzione e non dall'ufficio commerciale). In riferimento a caparre penitenziare fittizie[29], in questo caso la società stipula un contratto preliminare di vendita di un bene (solitamente immobili) ad un valore inferiore a quello di mercato con un soggetto compiacente prevedendo una caparra penitenziale in casi di mancato perfezionamento del contratto. Successivamente l'immobile viene venduto a un terzo soggetto al valore di mercato (il che giustifica il pagamento della penale) con creazione di riserva occulta presso il soggetto compiacente a danno della società. Poiché tali operazioni non sono usuali è facile individuarle.

È opportuno verificare le differenze di prezzo tra preliminare e atto definitivo e indagare sulle cause. Nei casi più dubbi deve essere chiesta una perizia esterna. Verificare anche la congruità della penale e l'operatività del soggetto promissorio acquirente. Riconosciamo inoltre il caso di operazioni di leasing fittizie dove; una società (A) vende ad una società compiacente (B) ad un prezzo irrisorio un bene. Il bene di fatto rimane nella disponibilità di (A). La società (B) vende al valore di mercato ad una società di leasing (C) che concede lo stesso bene in locazione finanziaria alla società (A).

[29] *https://fiscomania.com*

La società (B) ha acquistato la disponibilità di somme pari alla differenza tra il valore di acquisto da (A) e quello di vendita a (C) che provvede con altra operazione a stornare in parti sui conti dell'amministratore di (A). In questo caso, al fine di prevenire il rischio di frode, è opportuno verificare che l'inventario fisico dei beni strumentali sia costantemente e sistematicamente aggiornato. È opportuno verificare la conformità della procedura di decisione e conclusione del contratto di leasing. Altro caso riguarda le forniture stornate con note di credito[30].

Una società (A) effettua con altra società compiacente (B) la fornitura di beni o servizi. Dopo la fornitura l'acquirente (B) contesta fittiziamente i beni o servizi ricevuti da (A). Segue la transazione con emissione di nota di credito da parte di (A). La provvista creata presso (B) viene poi stornata su conti correnti intestati a soggetti legati all'amministrazione di (A). Le note di credito che scaturiscono da transazioni o arbitrati devono essere assoggettate ad una rigorosa procedura operativa.

È opportuno acquisire tutta la documentazione sottostante l'operazione oggetto di transazione e analizzare le cause di non conformità della merce o prestazione; la persona (e il correlato grado di indipendenza) che ha accertato la non conformità; l'intervento di legali nella transazione che vanno circolarizzati; l'operatività della società acquirente. Situazione diversa è quello delle emissioni multiple di Ri.BA[31]. a fronte di uno stesso credito. Le società in difficoltà finanziaria per ottenere liquidità immediate emette più Ri.BA. a fronte di uno stesso credito portando all'anticipo le stesse presso diversi istituti bancari.

[30] *https://fiscomania.com*
[31] *https://fiscomania.com*

All'atto dell'emissione della prima Ri.BA., chiude il conto cliente contro un conto Ri.BA. in portafoglio, poi chiude anche tale conto in contropartita del conto banche c/c o banche c/anticipi. Le successive anticipazioni vengono gestite con accredito del conto corrente o c/anticipi e addebito di un altro cliente o con utilizzo di un conto transitorio nel passivo banche c/RB, anticipi e similari. È opportuno verificare gli addebiti bancari per Ri.BA. insolute e le note di credito emesse.

Verificare in dettaglio il conto Ri.BA. in portafoglio o all'anticipo ed effettuare riscontro con distinte di presentazione in banca delle stesse. I doppi pagamenti [32]rappresentano anche essi un caso critico e comune di azione fraudolenta. Il dipendente della società paga due volte il fornitore per la stessa prestazione. Tale frode può essere posta in essere, ad esempio, inserendo due volte nell'anagrafica fornitori il fornitore complice. Attribuendo due codici è possibile registrare la fattura due volte ed eseguire il doppio pagamento.

In questo caso occorre verificare periodicamente l'anagrafe dei fornitori ponendo attenzione alle denominazioni sociali simili. Effettuare periodicamente riconciliazioni contabili tra schede contabili e risultanze del fornitore verificando attentamente se esistono importi identici. Infine, è opportuno verificare la separatezza delle funzioni tra chi esegue gli ordini, chi registra le fatture e chi esegue i pagamenti.

Ultimo caso che propongo riguarda le frodi sulla cassa assegni [33].Nei periodi di crisi per migliorare i dati di bilancio gli amministratori ricorrono ad alcune 'politiche di bilancio' quali: finanziamenti di soci che aumentano le disponibilità liquide e il patrimonio netto ma senza ci sia la reale volontà di apportare in modo permanente i mezzi propri (es. versamenti c/futuri aumenti di capitale sociale condizionati); crediti inesigibili non diventano esigibili solo perché la società ha acquisito un assegno.

[32] *https://fiscomania.com*
[33] *https://fiscomania.com*

CAPITOLO 2

IDENTIFICAZIONE E GESTIONE DEL RISCHIO DI FRODE E LE PRINCIPALI NORMATIVE ITALIANE E STATUNITENSI

In questo capitolo, tramite l'analisi delle disposizioni normative in tema di crime prevention andremo ad analizzare quelle che sono le tecniche valutative per abbattere il rischio di frode tenendo conto delle disposizioni normative previste d.lgs. n° 231/2001.

2.1 Le tecniche valutative per abbattere il rischio di frode

La gestione del rischio di frode e di cattiva condotta è una preoccupazione crescente per il management e per le parti interessate nell'ambiente aziendale odierno sia da un punto di vista di danno reputazionale che di impatto negativo sul risultato di esercizio[34]. In questo contesto, l'implementazione di un modello efficace ed efficiente di fraud management riveste un ruolo cruciali. Tale framework, seppur tarato sulle specifiche realtà aziendali, prevede, tra gli altri, la compresenza dei seguenti elementi:

- *Commitment CdA e del top management:* andrebbe definito un sistema di attribuzioni di responsabilità sulle attività di fraud governance. Inoltre, il management, deve farsi parte attiva nel comunicare e rendere noto il suo impegno nella gestione efficace del rischio di frode (cd. "tone of the top"). Uno dei metodi più utilizzati è lo sviluppo di policy antifrode e codici etici o di condotta rivolti al personale interno, ai clienti, ai fornitori e a tutte le terze parti che a diverso titolo si relazionano con l'azienda.

[34] Secondo un recente studio dell'Association of Certified Fraud Examiners, una tipica organizzazione perde circa il 7% dei suoi ricavi annuali a causa delle frodi.

- - *Comunicazione capillare su tematiche antifrode:* diffusione in tutta la gerarchia dove di codici etici, modelli 231 e policy antifrode (obiettivi, perimetro di applicabilità, ruoli e responsabilità, attività da svolgere, azioni disciplinari) e svolgimento periodico di training. Allo stesso modo dovrebbero essere previsti strumenti di whistleblowing che favoriscano la segnalazioni di possibili malpractice da parte di soggetti interni tutelando l'anonimato e la protezioni ritorsioni verso questi ultimi

- *Conflitto d'interessi*: dovrebbe essere sviluppato un processo aziendale, che mappi in maniera efficace ed efficienti le cariche e partecipazioni detenute perlomeno dai soggetti apicali dell'azienda; l'obiettivo consiste nel prevenire eventuali conflitti di interesse che si manifestano attraverso business relationship tra l'azienda e terze parti in cui soggetti interni detengono interessi non disclosed

- *Valutazione del rischio di frode:* dovrebbe essere sviluppato un processo continuo di fraud risk assessment che identifichi i possibili eventi e schemi fraudolenti di interesse per l'organizzazione, con la relativa misura sulle probabilità di accadimento e di impatto (economico e reputazionale) sull'azienda e le relative misure poste in essere dall'azienda per evitarne l'accadimento. A fronte di eventuali gap individuati a fronte dei quali alcune aree/processi a rischio frode non risultino opportunamente presidiati da opportuni controlli interni, il sistema dovrebbe prevedere azioni rimediali che implementi ulteriori controlli interni tali da ridurre il rischio di commissione di eventi fraudolenti.

- *Processo di investigazione*: le organizzazioni dovrebbero sviluppare processi investigativi opportunamente proceduralizzati, in cui attività da svolgere, ruoli e responsabilità, struttura della reportistica e flussi comunicativi interni ed esterni siano chiaramente esplicitati.

- *Monitoraggio continuo*: il processo nel suo complesso e nei singoli sotto-processi dovrebbe essere documentato e continuamente monitorato, al fine di poter effettuare la valutazione e il miglioramento del sistema che tenga conto dell'evoluzione del rischio di frode all'interno dell'ambiente aziendale.

La prevenzione del rischio di frode riguarda le procedure, le politiche, la formazione e la comunicazione, la fraud detection invece riguarda sistemi e metodologie di rilevamento di comportamenti sospetti o atti fraudolenti una volta che sono stati compiuti. Naturalmente, l'implementazione di un sistema efficiente di fraud detection agirà come deterrente, operando, quindi, da fattore di prevenzione. Tra i principali strumenti di controllo per la prevenzione delle frodi i più efficaci si sono rivelati i seguenti:

- *Procedure HR*: effettuare controlli e investigazioni sul background di un candidato in fase di assunzione, richiedere certificati dei carichi pendenti e del casellario giudiziario, effettuare formazione in funzione antifrode, sviluppare valutazioni della performance e programmi di compensazione che premino la fedeltà e il comportamento corretto dei dipendenti e dei dirigenti.

- *Limiti all'autorità*: la predisposizione di livelli di autorità commisurati ai livelli di responsabilità aiuta a limitare il rischio di frode. In particolare, sistemi autorizzativi di controllo e segregazione di responsabilità sviluppano un ambiente meno soggetto ad attività fraudolente.

- *Controlli sulle transazioni con parti terze*: instaurazione di sistemi di controllo sulle transazioni con parti terze all'azienda, come a esempio fornitori.

- *Analisi del contesto normativo*: tutte le attività ricomprese in un programma di fraud governante: devono essere sviluppate in coerenza e nel rispetto delle vigenti normative, nazionali e internazionali, con particolare riferimento a normative giuslavoristiche, Privacy, norme internazionali sull'Anti Corruption e Anti Bribery, norme sul rispetto dei diritti umani, ecc.

2.2 Il fraud risk assessment

Il Fraud Risk Assessment è quel processo attraverso cui il management acquisisce contezza del rischio di frode complessivo subito dall'azienda. L'attività prevede:

- Identificazione di processi fraud sensitive e relativi potenziali rischi di frode inerenti, ivi inclusi possibili schemi di frode applicabili alla specifica realtà aziendale.

- Valutazione, all'interno dei processi identificati, della probabilità e della significatività (impatto) del verificarsi dei rischi di frode identificati.

- Mappatura dei presidi di controllo di tipo preventivo ed investigativo in uso per contrastare i rischi di frode identificati.

- Valutazione della tenuta del sistema di controllo interno in relazione ai rischi frode identificati ed individuazione di eventuali gap rispetto a best practices nazionali ed internazionali di settore.

- identificazione e valutazione dei rischi di frode residui derivanti da controlli inefficaci o inesistenti.

- Risposta ai rischi di frode residui e gap identificati

La Valutazione del Rischio di Frode può rivelare alcuni rischi residui di frode che non sono stati adeguatamente mitigati a causa della mancanza o della non conformità con gli appropriati controlli preventivi e investigativi. Il professionista della frode dovrebbe lavorare con il cliente per sviluppare strategie di mitigazione di eventuali rischi residui con una probabilità o una significatività di accadimento inaccettabilmente alta. Le risposte dovrebbero essere valutate in termini di costi e benefici e alla luce del livello di tolleranza al rischio dell'organizzazione.

Siate consapevoli, tuttavia, che questa valutazione fornisce solo un'istantanea di un particolare momento. La natura dinamica delle organizzazioni richiede un monitoraggio e un aggiornamento di routine dei processi di valutazione dei rischi finanziari per poter rimanere efficaci.

2.3 Le disposizioni normative in tema di crime prevention

La prevenzione delle frodi aziendali è diventato un tema importante da quando l'approvazione negli USA del Sarbanes-Oxley Act del 2012 ha imposto nuovi obblighi alle aziende. Lo scopo della normativa era quello di ristabilire la fiducia dell'opinione pubblica dopo che gravi scandali aziendali come quello di Enron l'avevano compromessa. La normativa contenuta nella Section 404 del Sarbanes-Oxley Act obbliga le società a dotarsi di un sistema di audit interno. Lo scopo è quello di garantire una sistematica azione preventiva delle frodi aziendali in modo da incrementare la fiducia degli investitori. Le metodologie di prevenzione delle frodi sono diventate molto importanti anche nelle aziende al di fuori degli Stati Uniti parallelamente all'affermarsi delle funzioni di audit interno.

Lo scopo del sistema di prevenzione è di minimizzare il manifestarsi di comportamenti illeciti. L'analisi degli obiettivi aziendali e il monitoraggio dei sistemi incentivanti intendono attenuare le situazioni di tensione da cui ha origine il processo fraudolento. Già da diversi anni si ritiene che la prevenzione delle frodi aziendali debba essere messa in atto tramite un'adeguata implementazione del sistema di controllo interno.

Tale consapevolezza è emersa negli Stati Uniti dalle ricerche della Treadway Commission [35]che hanno portato alla definizione di standard in materia di controllo interno come quello emanato dal C.o.S.O. (Committee of sponsoring Organizations).

[35] *Il "Comitato delle organizzazioni sponsor della Commissione Treadway" è un'iniziativa congiunta per combattere le frodi aziendali.*

Tali standard hanno di conseguenza influenzato i contenuti dei codici di corporate governance, nonché numerose emanazioni normative, partendo dal Sarbanes-Oxley Act (SOA) alle leggi per la prevenzioni dei crimini economici, tra le quali l'Italiano D.lgs. 231/2001 in tema di responsabilità amministrativa.

Quando si vuole dare una specifica finalità al sistema di controllo interno è necessario considerare che l'ottica antifrode impone:

1. L'applicazione di metodi informativi e organizzativi al fine di garantire elevati livelli di tracciabilità delle operazioni aziendali, mediante sistemi di documentazione delle attività svolte che siano il più possibile delegati ai sistemi informatici e richiedano pochi interventi manuali;

2. La necessità di orientare i controlli interni in modo rilevante verso un'attitudine di prevenzione al realizzo di frodi, così come previsto anche dalle normative di "crime prevention"; i controlli consuntivi devono essere ritenuti adeguati solo quando possiedono carattere di efficacia segnaletica e tempestività molto elevate;

3. Di utilizzare in modo massivo controlli automatizzati, poiché questi sono in grado di non fare eccezioni e garantiscono un'elevata adeguatezza dei controlli stessi; i controlli svolti dal personale o dal management dovrebbero essere minimi;

4. Di focalizzarsi sulle transazioni poiché queste possono essere verificate da meccanismi automatizzati dei sistemi informatici; ciò impone di definire meccanismi di autorizzazione preventiva e regole di controllo stringenti, in modo da "bloccare" ex-ante l'operatività aziendale entro parametri ritenuti accettabili, ed ex-post, consentire la tempestiva segnalazioni di operazioni anomale.

5. Di esprimere una valutazione della componente di "separazione dei compiti", che consideri le possibilità di collusione tra più soggetti. Le frodi collettive dovrebbero essere ridotte drasticamente da adeguati controlli interni, almeno in quelle aree di attività aziendale dove comportamenti fraudolenti potrebbero produrre un impatto rilevante, se non catastrofico in termini di appropriazione indebita, corruzione o frodi in bilancio.

6. Sulla base di quanto sopra citato è fondamentale per le imprese in crescita l'impostazione di un modello di sistema di controllo interno, che non solo focalizzi l'attenzione sugli obiettivi e sui rischi dell'impresa a cui questa è sottoposta, ma che possa essere utilizzato come strumento di lavoro del Fraud Auditor e del forensic accountant. Facendo riferimento alla normativa e regole di riferimento nazionale, oltre al D.Lgs231 bisogna segnalare:

- *D.lgs. N. 58 del 1998 («TUF»)* introduce l'espressione «Sistema di Controllo Interno» (art. 149, comma 1, p.to c, «Doveri del collegio sindacale»). Tale decreto affida al collegio sindacale delle quotate il compito di vigilare "sull'adeguatezza della struttura organizzativa della società per gli aspetti di competenza, del sistema di controllo interno e del sistema amministrativo-contabile, nonché sull'affidabilità di quest'ultimo a rappresentare i fatti di gestione.

- *Codice di Autodisciplina per le Società Quotate* (Codice Preda) redatto dal Comitato per la Corporate Governance presso Borsa Italiana nel 1999 e successivi aggiornamenti. Il Codice Preda fornisce una definizione di controllo interno mutuata dai framework internazionali; ripartisce tra c.d.A. e organi delegati le competenze relative al sistema dei controlli interni (concreta configurazione del sistema vs verifica periodica).

- *D.lgs. N. 262 del 2005 «Tutela del Risparmio».* Impone alle società quotate l'obbligo di nominare un nuovo soggetto, il dirigente preposto alla redazione dei documenti contabili societari (art. 154-bis tuf), chiamato a predisporre adeguate procedure amministrative e contabili per la redazione dei bilanci d'esercizio e consolidato, nonché ad attestare la loro adeguatezza ed effettiva applicazione congiuntamente all'amministratore delegato; 1) pone uno specifico obbligo di vigilanza sul "rispetto effettivo" delle procedure a carico del consiglio di amministrazione; 2) interviene sulla composizione del consiglio di amministrazione e del collegio sindacale per

garantire la presenza di rappresentanti della minoranza nonché, significativamente, sui poteri dei sindaci.

- Principi di revisione internazionali (ISA Italia). I principi di revisione sono i riferimenti che regolano la revisione contabile. Quest'ultima non è altro che l'attività svolta dai revisori contabili, i quali applicando delle procedure campionarie hanno la possibilità di accertare la correttezza e la veridicità delle poste di un bilancio consolidato o di un bilancio di esercizio. La revisione contabile, infatti, tipicamente ha lo scopo di ottenere la certificazione del bilancio consolidato o del bilancio di esercizio da parte dei revisori contabili.

- Norme e Linee Guida emanate da CNDCEC e IFAC. L'International Federation of Accountants (IFAC) è un'organizzazione globale che rappresenta la professione contabile. L'IFAC stabilisce e promuove gli standard internazionali e parla a nome della professione su questioni di politica pubblica.

2.4 Il d.lgs. n° 231/2001

In Italia lo sviluppo di adeguati sistemi di controllo interno e di auditing è stato stimolato dall'adozione del Decreto Legislativo n. 231/2001 dell'8 giugno del 2001, intitolato "Disciplina della responsabilità amministrativa delle persone giuridiche", a norma dell'art. 11 della legge 29 settembre 2000, n.300, ha introdotto nel nostro ordinamento la responsabilità penale degli enti, aggiungendola a quella della persona che materialmente ha commesso il fatto.

Le società e le imprese sono responsabili per i reati commessi a proprio vantaggio o dalle persone che rivestono ruoli di rappresentanza, di amministrazione o direzione delle imprese stesse o dalle persone che ne esercitano di fatto la gestione e il controllo, ed ancora, dalle persone sottoposte alla direzione di queste ultime.[36]

Precedentemente la responsabilità amministrativa degli enti era già stata stabilita nella Convenzione OCSE del 1997 e più precisamente all'art. 2 che specificatamente riguardava la commissione di reati da parte dei pubblici ufficiali stranieri nelle operazioni internazionali.

Questo atto venne ratificato nel nostro Paese solo successivamente, nel 2000, con la legge n.300, per prevenire la corruzione nel commercio internazionale e le frodi ai danni della Comunità Europea[37]. Con il decreto del 2001 è stata ampliata la responsabilità dei soci i quali, fino all'entrata in vigore dello stesso, in definitiva non subivano conseguenze dalla realizzazione dei reati commessi a vantaggio della società.[38]

---

[36] Tratto da: "La responsabilità amministrativa per reati penali posta a carico di società ed associazioni secondo il D.Lgs.231/01", in "Revisione Contabile" n.42/2001.

[37] Tratto da: "La responsabilità amministrativa per reati penali posta a carico di società ed associazioni secondo il D.Lgs.231/01", in "Revisione Contabile" n.42/2001.

[38] "Valutazione dei rischi e controllo interno" - S. Beretta, Milano (2004), pag. 167

Una conseguenza fondamentale di una simile innovazione è stata, ovviamente, l'inserimento del controllo della legalità e della regolarità dell'operato sociale fra il novero degli interessi di tutti i soggetti che partecipano a vario titolo alle vicende patrimoniali dell'ente. Inizialmente gli studiosi hanno avuto delle perplessità, essi si sono domandati se la società potesse veramente compiere un reato, in realtà la risposta appare semplice: l'azienda non è solo un complesso di beni, ma è caratterizzata da un elemento umano.

La stessa nascita dell'ente deriva dalla volontà dell'imprenditore e anche successivamente le decisioni sono prese da individui ed essi possono compiere azioni illecite. La tipologia dei reati presenti nel D.Lgs.n.231 sottolinea la matrice penalistica della normativa in oggetto, nonostante il legislatore abbia qualificato la responsabilità delle società come amministrativa.

L'ambito di applicazione della norma è stabilito all'art.1, per ciò che concerne il lato oggettivo ci si riferisce alla "responsabilità degli enti per gli illeciti amministrativi dipendenti da reato", dal lato soggettivo è previsto che il decreto si applichi agli enti forniti di personalità giuridica e alle società e associazioni anche se prive di questo requisito, rimangono quindi esclusi lo Stato, gli enti pubblici territoriali ed infine quelli non economici che svolgono funzioni di rilievo costituzionale.

In base all'art.5 la responsabilità dell'ente si ha quando il reato è commesso o dai soggetti "apicali", (ovvero coloro che rivestono funzioni di rappresentanza o amministrazione o direzione dell'organizzazione), o da soggetti posti al vertice, ma non solo, risponde anche se il fatto è stato commesso da persone sottoposte alla direzione e alla vigilanza dei soggetti prima menzionati.

Le conseguenze per l'organizzazione cambiano a seconda del soggetto che ha commesso il reato: in caso di soggetti apicali, in base art.6, la società non è responsabile se dimostra che[39]:

a) L'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi; da segnalare che nel successivo art.7, relativo a reati commessi a soggetti sotto l'altrui direzione, il concetto risulta ampliato in modelli di organizzazione, gestione e controllo, dando così adito a possibili dubbi interpretativi.

b) Il compito di vigilare sul funzionamento e l'osservanza dei modelli e di curare il loro aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo;

c) Le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione; congiuntamente alla volontà di commettere un atto criminoso deve coesistere pertanto una condotta finalizzata ad aggirare tramite l'inganno i controlli preventivi preposti.

d) Non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla lettera b).

Al fine di beneficiare di questo esimente è opportuno che l'azienda si doti di un cd. *modello 231* periodicamente revisionato che identifichi aree sensibili e definisca meccanismi correttivi per prevenire le deviazione che potrebbero far scattare la responsabilità amministrativa e monitorino i risultati nel tempo. ll regime di responsabilità amministrativa a carico dell'impresa è configurabile per reati commessi da persone che rivestono funzioni di rappresentanza, amministrazione o direzione dell'ente, di unità organizzativa dotata di autonomia finanziaria e funzionale, da persone che esercitano, anche di fatto, la gestione e il controllo o che sono sottoposti alla direzione o alla vigilanza di uno di questi soggetti.

[39] *"Fondamenti aziendalistici della responsabilità degli enti ai sensi del D.lgs. n. 231 del 2001" - G.B. Alberti, in Le Società, Milano (2002), Fasc.5*

Il successivo articolo invece disciplina il caso in cui a compiere il reato siano stati soggetti sottoposti a vigilanza di altri, in tale ipotesi la responsabilità dell'ente si ha se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di vigilanza, in ogni caso questa inosservanza è esclusa a priori se l'ente ha adottato ed attuato in maniera efficace un modello di organizzazione, gestione e controllo idoneo a prevenire i reati della specie di quello commesso, ovviamente in un periodo precedente alla commissione dello stesso[40].

Per quanto concerne la tipologia di reati a cui si applica la disciplina in esame è opportuno segnalare come, al momento del decreto, il legislatore avesse optato per una scelta minima rispetto alle indicazioni contenute nella legge delega, prendendo in considerazione soltanto i seguenti reati: indebita percezione di erogazioni pubbliche, truffa in danno dello Stato o di altro ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico(art.24), concussione e corruzione(art.25).

Successivi interventi normativi hanno poi ampliato il campo d'applicazione del 231/01. La legge 23 novembre 2001, n. 409, ha inserito nel decreto i reati di falsità di monete, carte di credito e in valori di bollo (art 25 bis)123. Le sanzioni amministrative che possono essere inflitte dall'ente dal giudice penale sono di quattro tipi: sanzione pecuniaria, sanzioni interdittive, confisca, pubblicazione della sentenza di condanna.

La sanzione pecuniaria, sempre applicata, viene irrogata per quote, il cui numero, non inferiore a 100 e non superiore a 1000, è determinato dal giudice tenendo conto della gravità del fatto, del grado di responsabilità dell'ente, nonché dell'attività svolta per eliminare od attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti.

[40] "La responsabilità amministrativa per reati penali posta a carico di società ed associazioni secondo il D.Lgs.231/01", in "Revisione Contabile" n.42/2001.

Le sanzioni interdittive, espressamente elencate dal legislatore, consistono in: interdizione dell'esercizio dell'attività, sospensione e revoca delle autorizzazioni, licenze e concessioni funzionali alla commissione dell'illecito. Tali sanzioni sono applicate solo in relazione ai reati per i quali sono esplicitamente previste e quando ricorre almeno una delle seguenti condizioni: l'ente ha tratto un profitto di rilevante entità e il reato è stato commesso da soggetti in posizione apicale ovvero da soggetti posti all'altrui direzione quando, in questo caso, la commissione del reato è stata determinata o agevolata da gravi carenze organizzative; reiterazione degli illeciti.

Il tipo e la durata delle sanzioni interdittive è determinato dal giudice sulla base dei criteri validi per le sanzioni pecuniarie, tenendo presente che la sospensione dell'esercizio dell'attività, provvedimento che può comportare conseguenze economiche tali da poter pregiudicare la sopravvivenza stessa dell'ente, è applicabile solo quando l'irrogazione di altre sanzioni interdittive risulta inadeguata.

Tutte queste misure sono collegate all'apprezzamento della maggiore gravità delle violazioni che legittimano la privazione di un diritto o di una capacità dell'Ente secondo un meccanismo che non sembra solo punitivo, quanto piuttosto indirizzato a soddisfare esigenze esclusivamente preventive, sia di prevenzione sociale, poiché neutralizzano le attività criminose dell'Ente, per cui si procede sotto il profilo della dissuasione. Si tratta, infatti di misure che incidono sull'operatività e sulla funzionalità dell'Ente, non solo lo puniscono efficacemente rispetto alla sanzione pecuniaria, ma limitano per il futuro, quelle attività il cui abuso ha determinato la commissione del fatto-reato incriminato.

La confisca del prezzo o del profitto del reato è sempre disposta nei confronti dell'ente con la sentenza di condanna, tranne che per la parte che può essere restituita al danneggiato e fatti salvi i diritti acquisiti da terzi in buona fede. Ed infine la pubblicazione della sentenza di condanna può essere disposta in seguito all'applicazione di una sanzione interdittiva.

La sentenza è pubblicata una sola volta, a spese dell'ente, per estratto o per intero, in uno o più giornali indicati dal giudice, nonché mediante affissione nel comune ove l'ente ha la sede principale. Le suddette sanzioni amministrative si prescrivono nel termine di cinque anni dalla data di consumazione del reato. L'apparato sanzionatorio, previsto da tale decreto, risponde alle raccomandazioni comunitarie in tema di diritto punitivo di sanzioni effettive e proporzionali, dissuasive: sanzioni pecuniarie e interdittive si applicano in casi di particolare gravità.

CAPITOLO 3

STRUMENTO DI PREVENZIONE DELLE FRODI: IL SISTEMA DI CONTROLLO INTERNO

3.1 Il sistema di controllo interno

Il termine "sistema di controllo interno[41]" è già stato citato in diversi momenti nel presente lavoro, ogni volta riferendosi a questo come il migliore strumento di prevenzione delle frodi societarie, senza specificare tuttavia né in cosa consista effettivamente, né quale siano davvero la sua funzionalità e la sua potenzialità. L'obiettivo di questo capitolo è proprio quello di analizzare nello specifico le componenti di tale sistema, gli utilizzi che una società può farne e i benefici che ne trarrebbe, soprattutto in termini di efficienza nella prevenzione delle attività fraudolente.

L'espressione "controllo interno" assume, significati diversi a seconda dell'ambito a cui ci si riferisce. Nel settore pubblico il controllo interno consiste principalmente in attività di verifica effettuate da un soggetto che, nonostante non sia parte dell'ente monitorato, opera comunque nei confini dello stesso. In genere le best practices internazionali si rifanno al Coso Report ed in seguito le autorità di vigilanza nazionali operano per meglio amalgamare il Coso con il sistema di vigilanza per esistente.

Nel settore finanziario, al contrario, grazie alle richieste della Banca d'Italia, si va sempre più de lineando una definizione specifica di sistema di controllo interno. Le istruzioni di vigilanza per le banche prescrivono infatti agli enti creditizi non solo il rispetto di certi requisiti patrimoniali ma anche l'uso di procedure e sistemi di controllo finalizzati a garantire un "adeguata gestione dei rischi di mercato.

[41] Un sistema di controllo interno ha come obiettivo e priorità il governo dell'azienda attraverso l'individuazione, valutazione, monitoraggio, misurazione e mitigazione/gestione di tutti i rischi d'impresa, coerentemente con il livello di rischio scelto/accettato dal vertice aziendale

Non si può invece parlare di un "altrettanto chiara visione e definizione di controllo interno nel settore privato, dove, un po'" anche a causa di tale mancanza, molte società non si sono ancora poste il problema di adottare una struttura adeguata alle loro esigenze e non si sono nemmeno interrogate su quale possa essere la funzionalità di un tale sistema. Per molte infatti il termine controllo evoca ancora solo l'idea di verifica ispettiva o di mera rilevazione contabile.[42]

Quelle società che, al contrario, hanno cominciato ad interessarsi alla questione, si sono trovate di fronte al problema di non avere un adeguato supporto per quanto riguarda la costruzione vera e propria del sistema. In Italia, infatti, non esiste un modello di riferimento a cui rifarsi per la progettazione e l'implementazione della struttura di controllo ed è per tale ragione che risulta necessario fare dei rimandi alla letteratura e alla legislazione d'oltreoceano.

Negli Stati Uniti, infatti, il concetto di sistema di controllo interno è già stato trattato e definito da tempo dal Committee of Sponsoring Organizations of the Treadway Commission (CoSO) che nel 1992, dopo diversi significativi scandali avvenuti negli anni "80, ha pubblicato il CoSO Report: Internal Control – An Integrated Framework, un documento avente l'obiettivo di fornire sia una definizione comune di controllo interno, sia uno standard di riferimento attraverso il quale le società e ogni altra forma di organizzazione possano valutare ed implementare i loro sistemi di controllo.

Attraverso tale pubblicazione, la Commissione mirava proprio a migliorare la qualità dei report finanziari delle società mediante una maggiore focalizzazione sul corporate management, sugli standard etici e sul controllo interno.

[42] 1. AIIA, Il ruolo dell'internal auditor nella prevenzione ed il controllo delle frodi, Milano AIIA, 2000.

Il CoSO Report risulta essere di così grande importanza a livello mondiale non solo in quanto unico esempio di letteratura che ha cercato di fornire uno standard di sistema di controllo interno, ma soprattutto in quanto il modello da lui presentato è stato riconosciuto dalla Securities and Exchange Commission (SEC) come best practice di riferimento per costruire un "adeguata architettura dei sistemi di controllo interno e per conformarsi anche alle previsioni della Sarbanes-Oxley Act del 2002[43]. Tale riconoscimento ufficiale, al quale ne sono seguiti molti altri tra cui, a metà degli anni Novanta, quello dell'istituto Monetario Europeo (ora Banca Centrale Europea) che ha indicato il Report come esempio per i sistemi di controllo da inserire all'interno delle banche, ha reso pertanto questo Framework il punto di riferimento di ogni società, ivi comprese quelle italiane, impegnate nell'implementazione di una struttura interna di controllo. Prima di trattare però più nello specifico il modello presentato dal CoSO Report, è doveroso fornire una definizione avente valenza generale del concetto di sistema di controllo interno. Con tale espressione si intende un processo, implementato dal Consiglio di Amministrazione, dai dirigenti e da altri operatori della struttura aziendale, progettato per fornire una ragionevole certezza (in termini anglosassoni reasonable Assurance) in merito alla realizzazione degli obiettivi rientranti nelle seguenti categorie: [44]

I. efficacia ed efficienza delle attività operative, nella quale vengono inclusi gli obiettivi di base di un "azienda, compresi quelli di performance, di redditività e di protezione delle risorse;
II. attendibilità delle informazioni di bilancio, sia in termini di preparazione che di pubblicazione dello stesso;
III. conformità alle leggi e ai regolamenti in vigore a cui è sottoposta la società.

[43] *La Sarbanes-Oxley Act, conosciuta anche con il nome di Public Company Accounting Reform and Investor Protection Act of 2002 e comunemente chiamata Sarbanes-Oxley, Sarbox (o semplicemente SOX) è una legge federale emanata nel luglio 2002 dal governo degli Stati Uniti d'America a seguito di diversi scandali contabili che hanno coinvolto importanti aziende americane come Enron, la società di revisione Arthur Andersen, WorldCom e Tyco International. Suddetti scandali hanno causato grande sfiducia da parte degli investitori nei confronti dei mercati, sollevandone altresì diversi dubbi circa le loro politiche di sicurezza.*

[44] 17. AIIA - Associazione Italiana Internal Auditors, Corporate Governance Paper "Approccio integrato al Sistema di Controllo Interno ai fini di un'efficace ed efficiente governo d'impresa"

A partire da questa definizione è possibile effettuare alcune riflessioni: innanzitutto è importante sottolineare come il sistema di controllo interno sia un processo, un mezzo mirato ad un fine, non un fine di per sé stesso. Non è perciò un procedimento indipendente, una circostanza unica e irripetibile, ma comprende tutta una serie di atti che interessano l'intera attività aziendale e che si intrecciano nei processi fondamentali di pianificazione, esecuzione e monitoraggio.

Tale sistema infatti raggiunge l'apice della sua efficacia nel momento in cui è integrato nella struttura di un "organizzazione e fa parte della sua cultura aziendale. Esso inoltre non è costituito unicamente da manuali e da documenti, ma da persone che si collocano a tutti i livelli gerarchici di una società e non solo in posizione apicale. [45]

Tale definizione di sistema di controllo interno specifica inoltre come il management e il Consiglio di Amministrazione possano attendersi dalla struttura dei controlli solo una sicurezza ragionevole, non assoluta, riguardo alla realizzazione degli obiettivi; pertanto, per quanto un sistema di controllo interno sia adeguatamente strutturato e implementato, non garantirà mai la totale certezza, in quanto comunque viziato da limiti che sono insiti in ogni tipo di sistema, quali ad esempio disfunzioni dovute ad omissioni umane o elusione dei controlli da parte di uno o più soggetti.

Il sistema di controllo interno, in particolare il modello di riferimento delineato dal CoSO Report del 1992, è costituito da cinque componenti strettamente correlati tra di loro. Nonostante tali componenti siano attuabili sia in piccole, sia in medie che in grandi imprese, la loro realizzazione potrà essere diversa a seconda della dimensione della società, che impatterà pertanto sulla strutturazione delle singole parti del sistema. [46]

[45] .orporate Governance e qualità dell'informazione esterna d'impresa. G. Fiore. Giuffrè Editore. Milano. 2003
[46] "Sistemi di pianificazione e controllo" di Paolo bastia, Il mulino Manuali, 2008

Quest'ultimo, però, a prescindere dalla realtà aziendale che lo implementa, dovrebbe essere composto, secondo il modello presentato dal CoSO Report, dalle seguenti componenti (PricewaterhouseCoopers, 2006):

1. l'ambiente di controllo, i cui fattori costitutivi sono:

- l'integrità e i valori etici;
- il valore della competenza;
- il Consiglio di Amministrazione o l'audit committee;
- la filosofia e lo stile di direzione;
- la struttura organizzativa;
- l'attribuzione di poteri e responsabilità;
- le politiche e prassi riguardanti le risorse umane.

2. la valutazione del rischio, i cui elementi sono:

- gli obiettivi generali dell'impresa;
- gli obiettivi specifici per ciascuna attività;
- l'analisi e la valutazione dei rischi;
- la gestione dei cambiamenti.

3. le attività di controllo, costituite da:

- politiche e procedure, quali la separazione dei compiti, il controllo fisico dei beni, la corretta autorizzazione e registrazione delle operazioni;
- sicurezza;
- applicazione delle strategie elaborate in risposta ai cambiamenti;
- continuità aziendale;
- outsourcing.

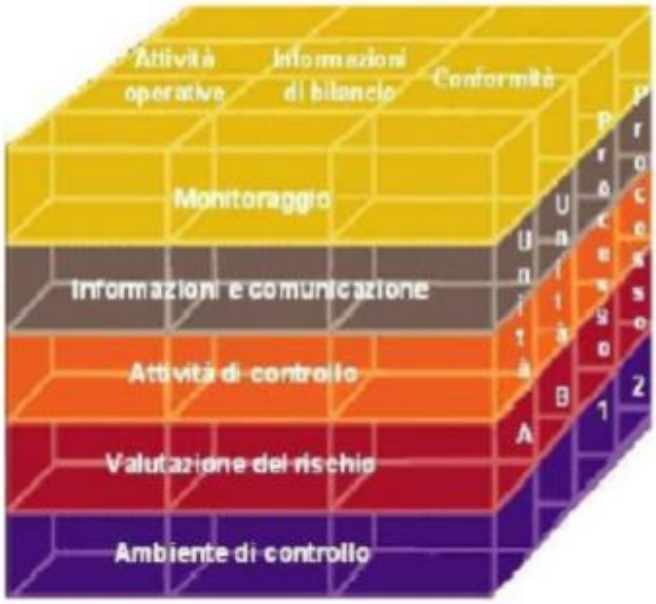
4. l'informazione e la comunicazione, focalizzate soprattutto:

- sulla qualità delle informazioni;
- sull'efficienza della comunicazione.

5. il monitoraggio, composto da:

- un monitoraggio continuo;
- valutazioni periodiche;
- segnalazioni delle disfunzioni.

Tab.3.1.1 Rappresentazione grafica del sistema di controllo interno esposto nel CoSO Report del 1992.



3.2L'implementazione del sistema di controllo interno

Sebbene il modello di sistema di controllo interno esposto nel CoSO Report del 1992 sia stato elaborato per essere applicato a ogni tipologia di impresa, a prescindere dalle sue dimensioni, è innegabile che le società di dimensioni più modeste hanno riscontrato delle difficoltà maggiori di applicazione della struttura. Realizzare infatti un controllo interno efficiente in imprese definibili smaller rappresenta sicuramente un "importante sfida, a maggior ragione se il vertice aziendale concepisce il controllo come un inutile obbligo in aggiunta ai sistemi operativi già esistenti nell'impresa e ritiene che il CoSO Framework sia in generale vago e privo di un "utilità per l'attività di revisione .[47]

[47] Olson D. L., Wu D. D., 2008

Le sfide che una smaller company si trova ad affrontare nella realizzazione di un sistema di controllo interno includono, tra le altre:

- una limitata disponibilità di risorse per creare una corretta e sufficiente separazione dei compiti
- la pervasività del management che domina le attività aziendali e, con i poteri a sua disposizione, può non solo non rispettare i controlli istituiti, ma anche eluderli per modificare i risultati aziendali;
- la difficoltà di assumere sia personale qualificato per lo svolgimento delle attività, sia soggetti con un "adeguata esperienza per ricoprire il ruolo di membri esterni nel Consiglio di Amministrazione o nei Comitati da questo costituiti;
- la complessità di creare, implementare e controllare sistemi informatici opportuni e adeguatamente costruiti per le esigenze della società.

Proprio per cercare di fornire un supporto alle imprese di piccole dimensioni per la realizzazione di appropriati sistemi di controllo interno, la Committee of Sponsoring Organizations of the Treadway Commission (CoSO) ha pubblicato nel 2005 una guida esplicitamente dedicata a questo tipo di società, basata sul Framework del 1992 e incentrata su una serie di tematiche che dovrebbero cercare di alleggerire i problemi affrontati dalle cosiddette smaller company. La guida, tuttavia, è adeguata e applicabile a ogni tipologia di società, di qualunque dimensione essa sia. La Guidance for Smaller Public Companies Reporting on Internal Controls over Financial Reporting adotta l'espressione smaller company con il significato di impresa non grande, senza avere alcuna pretesa di fornire una qualificazione della stessa in termini quantitativi.

Spesso, infatti, per tracciare una netta separazione tra le imprese di grandi dimensioni e quelle di piccole vengono individuati dei parametri di fatturato, di costi, di margine piuttosto che di dipendenti che assegnano in modo netto ed inequivocabile una determinata società a una categoria o all'altra.

La guida in questione, al contrario, non vuole limitare con dei parametri numerici il range di società a cui essa stessa è destinata e, per tale ragione, fornisce una definizione qualitativa di imprese di piccole dimensioni. all'interno di questa categoria rientrano quelle che:

- hanno poche linee di business o di prodotto;
- hanno un "attività di marketing articolata per canali di distribuzione o per area geografica;
- sono guidate da un management che detiene anche interessenze nel capitale di rischio;
- non hanno molti livelli gerarchici ma possono contare su un numero limitato di dirigenti a cui è sottoposto l'intero staff aziendale;
- hanno sistemi di protocollazione dei processi aziendali semplici ed elementari; hanno organici limitati con mansioni piuttosto varie.[48]

Proprio a causa di queste caratteristiche, le imprese di dimensioni limitate possono incorrere in maggiori costi nel momento in cui costruiscono un sistema di controllo interno. La guida, riconoscendo tale realtà, propone alcune soluzioni per cercare di ridurre tali esborsi di denaro e, a riguardo, fornisce alcune proposte. Innanzitutto, viene consigliato alle smaller company di ampliare il numero di membri dell'audit commettee che, avendo una visione più completa della società grazie alle loro conoscenze dell'attività e grazie al loro bagaglio di esperienze, possono davvero consigliare in modo proficuo in merito agli investimenti da effettuare nel sistema dei controlli. Un ulteriore consiglio che viene fornito dal CoSO, forse il più efficace per costruire un "efficiente struttura, riguarda l'integrazione nella cultura aziendale di principi legati alla responsabilità e al controllo: solo diffondendo questi valori all'interno nell" ambiente di lavoro è possibile fare in modo che essi vengano compresi ma soprattutto assimilati da tutti i dipendenti che saranno poi essi stessi

[48] 1G.M. MIRABELLI, Come affrontare la complessità normativa: l'esperienza Edison, in INTERNAL AUDIT -Corporate Governance, Risk Management e Controllo Interno, La Rivista dell'Associazione Italiana Internal Auditors, anno XVIII Pubblicazione quadrimestrale n. 60 Gennaio/Aprile 2008,

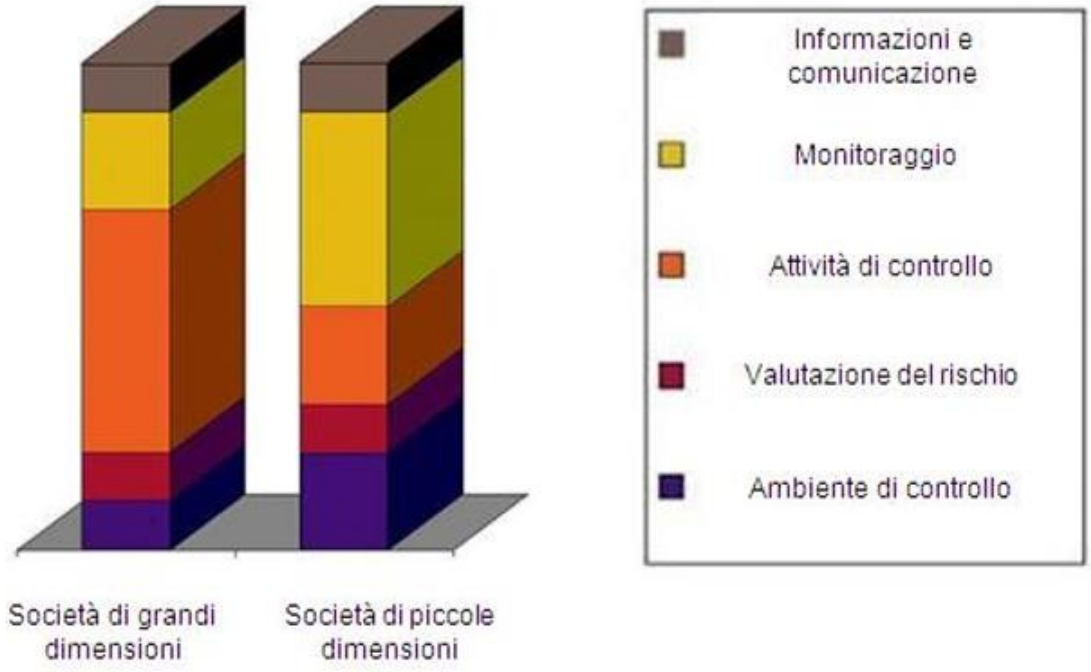
difensori di una politica fondata sul rispetto delle regole. Altri suggerimenti per tentare di abbassare il livello dei costi di implementazione di un sistema di controllo interno consistono in una visione maggiormente focalizzata sulle aree a più elevato rischio, nell'adozione di sistemi informatici facilmente disponibili, nell'ampliamento delle funzione del top management che dovrebbe occuparsi anche del monitoraggio delle attività non soggette alla sua diretta supervisione (The Committee of Sponsoring Organizations of the Treadway Commission, 2005). Nonostante la guida fornisca tutti questi spunti, essa tiene anche a precisare come questo non implichi che per le società di piccole dimensioni il CoSO Report debba essere applicato in modo diverso piuttosto che in modo più limitato: i concetti fondamentali del buon controllo sono sempre i medesimi, indipendentemente dal fatto che vengano presi in considerazione da una grande o da una piccola impresa. La differenza risiede semplicemente nel fatto che talvolta le società dimensionalmente più piccole tendono a formalizzare meno i procedimenti da loro compiuti, a dialogare in modo molto più diretto oltrepassando la burocrazia facilmente riscontrabile nelle grandi multinazionali. Queste minori formalità non sono necessariamente da vedere come un limite delle smaller company che, talvolta, sfruttando questi loro canali più diretti, riescono a trasferire in modo molto più trasparente i messaggi all'interno dell'intera azienda. [49]

La guida propone così alle smaller company di non rinunciare alla realizzazione di tutte e cinque le componenti del sistema di controllo interno, ma semplicemente di effettuare dei lievi cambiamenti per ciascuna di esse che consentano di adeguarle meglio alle esigenze, ma soprattutto alle risorse disponibili della società. Al termine di ognuno dei seguenti paragrafi verranno sintetizzate queste linee guida dedicate alle società di dimensioni limitate. Prima di intraprendere però l'analisi più specifica delle singole componenti del sistema, è utile mostrare, anche graficamente, l'effettiva differenza esistente tra il modo con cui i controlli vengono attuati dalle grandi società piuttosto che dalle piccole. Il seguente grafico, tratto proprio dalla Guidance for Smaller Public Companies

[49] "L'analisi e la gestione dei rischi aziendali: un'opportunità ad alto valore aggiunto per l'impres" di Paolo Bernardini e Maasimiliano Giacchè, Milano 10 giugno 2010

Reporting on Internal Controls over Financial Reporting, mostra un po'" la tendenza con cui le grandi e le piccole società applicano generalmente le cinque componenti del Framework.

Tab3.2.1 L'applicazione delle cinque componenti del sistema di controllo interno nelle realtà di piccole e grandi dimensioni.



Talvolta, le società di piccole dimensioni non si rendono conto di disporre effettivamente delle risorse necessarie per implementare a pieno i controlli, quali ad esempio la segregazione dei compiti, e pertanto tendono a concentrarsi maggiormente sulle attività di monitoraggio finalizzate ad evitare che un certo fatto possa ripetersi, o mirano a diffondere, attraverso messaggi del top management, una cultura aziendale del controllo.

Tutte queste attenzioni ad alcune delle aree del sistema non sono altro che dei tentativi di supplire alle mancanze in altre componenti dello stesso, in particolare, come si vede bene dal grafico, nell'attività di controllo.

Questa tendenza riscontrata in molte smaller company le contraddistingue dalle società di grandi dimensioni, anche se talvolta tale diversità potrebbe non essere così evidente, grazie alle risorse realmente disponibili all'interno delle società.

3.3 Le componenti del sistema di controllo interno

Il cd. "CoSO Report", ossia l'Internal Control Integrated Framework, cd. CoSO Report (ultima versione del maggio 2013) individua le seguenti cinque componenti del Sistema di controllo interno (S.C.I.), tutte interessate dai tre obiettivi di:

i) efficienza operativa (controllo di gestione);

ii) adeguatezza informativa (controllo amministrativo-contabile);

iii) conformità alla normativa(compliance), vale a dire:

- Ambiente di controllo (Control Environment): atmosfera di controllo e redazione dei report finanziari;
- Valutazione del rischio (Risk Assessment): processo per la gestione dei rischi, a sua volta suddiviso in Event identification, Risk assessment e Risk response;
- Attività di controllo (Control Activities): procedure e azioni intraprese per realizzare gli obiettivi aziendali;
- Informazione e comunicazione (Information & Communication): scambio di informazioni per il controllo dell'azienda (sistema informativo aziendale);
- Monitoring: monitoraggio del sistema di controllo[50].

[50] Report of the National Commission on Fraudulent Financial Information", obtained on March 23, 2011

3.3.1 L'ambiente di controllo

È l'identità di un'azienda, dipende dalla storia e dalla cultura aziendale ed è determinante perché costituisce le fondamenta su cui poggiano tutte le altre componenti dell'ERM. L'ambiente interno incide profondamente sulle modalità di determinazione di strategie e obiettivi, sulla progettazione delle attività e sull'identificazione e gestione del rischio.

Si possono identificare sei fattori che esercitano un'influenza importante su questo primo componente del modello ERM. Il primo è la filosofia della gestione del rischio, quell'insieme di valori e comportamenti che determinano l'atteggiamento della banca nei confronti del rischio: questo fattore ha un'influenza diretta sullo stile operativo della società e sulle modalità con cui gli altri componenti dell'ERM sono attivati.

È molto importante che la filosofia di gestione del rischio adottata da una banca sia capita e condivisa da tutto il personale: è una condizione necessaria affinché le attività delle diverse unità operative siano sempre orientate verso una visione complessiva del rischio d'impresa evitando in questo modo disallineamenti nell'assunzione dei rischi che potrebbero riflettersi negativamente sull'operatività della banca. [51]

Alla filosofia della gestione del rischio è collegato un altro importante fattore, quello dell'integrità e dei valori etici del management, prodotti della cultura aziendale essenziali per l'ambiente interno di una società che incidono sul disegno, sull'amministrazione e sul monitoraggio degli altri componenti dell'ERM. L'integrità e i valori etici si traducono in un codice di condotta che deve andare oltre il semplice rispetto della legge. Il CdA e il management hanno il compito di comunicare ma soprattutto formalizzare attraverso chiare indicazioni i valori etici e i comportamenti da seguire.

[51] Internal control - Integrated framework ", retrieved on March 23, 2011

La creazione e la comunicazione dei codici di comportamento al personale non costituisce però una garanzia sufficiente affinché questi vengano rispettati: è importante perciò che siano previste delle sanzioni per le violazioni del codice unitamente ad un sistema di comunicazione che incentivi i dipendenti a segnalare le irregolarità rilevate.

Inoltre, stabilire i valori etici può rivelarsi un procedimento problematico perché spesso gli interessi dei diversi attori aziendali risultano contrastanti. Proprio per questo al di là dei codici scritti e delle sanzioni, è l'atteggiamento del top management ad influire, con il suo esempio, sul comportamento del resto del personale: se l'alta direzione si comporta coerentemente ai principi e valori che va comunicando invierà un messaggio positivo a tutti i livelli dell'organizzazione. Il terzo fattore è il rischio accettabile che abbiamo già incontrato in sede di definizione del modello ERM: è l'ammontare di rischio che la banca è disposta ad assumere per perseguire le proprie finalità e a cui verrà allineata la formulazione delle strategie aziendali. È l'espressione concreta della filosofia di gestione del rischio.

Il Cda è un altro fattore dell'ambiente interno, ha un ruolo centrale in questa componente dell'ERM perché esercita un'influenza rilevante su tutti gli altri fattori. Infatti, la sua posizione di vertice fa sì che una società, e di conseguenza il modello di gestione adottato, funzionino bene solamente se a guidarla è un Cda composto da soggetti di alta levatura morale, indipendenti dal management e con un adeguato livello di competenze. [52]

Un consiglio di amministrazione così composto sarà in grado di adempiere ai suoi compiti di supervisione intervenendo, se necessario, nei confronti del management circa le strategie, la pianificazione adottate e i risultati ottenuti da quest'ultimo: tra i compiti del Cda c'è proprio quello di assicurarsi che il processo di gestione del rischio sia mantenuto efficace nel tempo.

[52] "The Trouble with COSO", March 15, 2006, accessed March 23, 2011.

La struttura organizzativa è il fattore che definisce le linee gerarchiche e la suddivisione di autorità e responsabilità all'interno di un'azienda, ma anche le modalità secondo cui le attività sono pianificate, attuate e verificate. La struttura organizzativa è concepita secondo le necessità dell'azienda e quindi dipenderà dalla natura dell'attività svolta e dalle sue dimensioni: la struttura adeguata sarà quella in grado di agevolare l'efficacia dell'ERM e l'esecuzione di attività dirette al conseguimento degli obiettivi.

L'attribuzione di poteri e delle responsabilità è un altro dei fattori dell'ambiente interno ed è strettamente collegato al precedente: consiste nella definizione delle linee gerarchiche, dei poteri concessi e dei limiti imposti sulle decisioni al personale dei vari livelli della struttura organizzativa.

Questo fattore comprende quindi la definizione di protocolli e politiche che descrivono le prassi aziendali appropriate: sarà l'alta direzione a decidere se delegare alcuni poteri verso i livelli più bassi dell'organizzazione per spostare il processo decisionale il più vicino possibile alle attività operative.

Questa delega può incentivare l'iniziativa del personale che per questo deve essere perfettamente conscio di quali siano gli obiettivi da realizzare: è essenziale che ogni soggetto operante nell'azienda sia consapevole dei legami intercorrenti tra le sue azioni. L'aumento dei livelli di delega necessita di un livello di competenza e di responsabilità più elevato: sarà importante accompagnare questa politica ad un sistema di monitoraggio che permetta al management di verificare i risultati e di intervenire se necessario sulle decisioni delegate.

Infine, abbiamo due fattori tra loro connessi: la competenza e le risorse umane. Infatti, le politiche di gestione delle risorse umane riguardano assunzioni e remunerazioni, gestione delle carriere, formazione e valutazione delle performance del personale: tutti aspetti che vengono valutati tenendo conto anche delle competenze necessarie allo svolgimento dei compiti di ogni singola posizione.

Ad esempio, in fase di assunzione, l'azienda selezionerà i soggetti con un livello di istruzione e un'esperienza professionale adeguati alle mansioni che andrebbero a svolgere.

Le politiche di gestione delle risorse umane rivestono inoltre un ruolo di comunicazione: servono a trasmettere al personale il livello di integrità, di comportamento etico e di competenza che l'azienda si aspetta. Merita un appunto il ruolo della formazione: è attraverso tali politiche che l'azienda si assicura un personale preparato e pronto a rispondere ai mutamenti dell'ambiente economico, all'evoluzione tecnologica e alla concorrenza

3.3.2 La valutazione dei rischi

Le considerazioni sulla valutazione dei rischi riportate nel CoSO Report sono riferite al tema del controllo interno in ambiente statunitense ma possono essere considera te attuali e condivisibili anche per il contesto italiano, rilevando tuttavia una differenza notevole nella concezione di rischio e nell'approccio ad esso nelle due realtà. La cultura del rischio altro non è che una cultura manageriale, che risulta essere partico larmente diffusa nell‟ambiente americano ma carente in molte organizzazioni italiane, non solo pubbliche ma anche private.

Nella nostra realtà economica, infatti, l'approccio al rischio è ancora embrionale e incompleto in quanto viene prestata attenzione solo ad alcune categorie di rischi, in particolare quelli di natura patrimoniale e finanziaria, trascurando al contrario tutti quelli che si possono incontrare nella semplice gestione operativa aziendale. [53]

[53] 8. Frodi in azienda, il ruolo dell'internal auditor, in Amministrazione e finanza, n.13/2000. M. Nobili.

La ragione della grande attenzione posta dalle nostre aziende ai rischi patrimoniali e finanziari risiede innanzitutto nel rapporto debito – patrimonio tipico della nostra cultura aziendale e di quella tedesca e giapponese, in contrapposizione con la realtà anglosassone e francese. "economia dei Paesi appartenenti a quest'ultimo gruppo vantano di fatti tradizionalmente un "esposizione debitoria verso le banche pari alla metà del capitale di rischio, rapporto che aumenta notevolmente nel caso di imprese italiane, tedesche e giapponesi (Pricewaterhouse Coopers, 2002).

Le considerazioni svolte dal CoSO Report in materia di valutazione dei rischi possono pertanto essere utili alle nostre imprese non solo per implementa re efficaci sistemi di controllo interno, ma anche per ampliare la nostra concezione di rischio.

Relativamente a questa seconda componente del sistema, il Framework mette subito in evidenza come, per poter effettivamente parlare di rischio, sia necessario effettuare un processo di identificazione e formulazione degli obiettivi aziendali. In altre parole, i rischi possono essere identificati e successivamente analizzati solo in termini di possibile mancato conseguimento degli obiettivi prefissati. La determinazione di questi ultimi, pur non essendo una delle componenti del sistema di controllo interno, ne è presupposto e supporto. Gli obiettivi possono essere indicati esplicitamente o implicitamente; a livello generale d'impresa, vengono spesso rappresentati sotto forma di missione aziendale e di valori. [54]

Essi, in associazione con una valutazione dei punti di forza e di debolezza, nonché a una valutazione delle opportunità e delle minacce, consentono di definire la strategia globale dell'azienda, da cui poi discendono gli obiettivi più specifici a livello di business unit, di divisione o di linea di prodotto.

[54] Liebenberg A., Hoyt R., 2003, "The determinants of Enterprise Risk Management: evidence from the appointment of Chief Risk Officer", Risk management and Insurance Review 6 (1), 37-52

Sebbene assai diversi, gli obiettivi si possono raggruppare in alcune grandi categorie:

- obiettivi operativi, che riguardano l'efficacia e l'efficienza delle attività operative aziendali; essi dipendono dalle scelte fatte dal management sulla struttura e sui livelli di performance;

- obiettivi relativi alle informazioni di bilancio, in particolare inerenti alla redazione di bilanci attendibili e veritieri. Tali obiettivi sono principalmente determinati da regole e norme stabilite da istituzioni esterne all'azienda;

- obiettivi di conformità, attinenti all'osservanza delle leggi e dei regolamenti applicabili all'azienda. Sono prefissati da fattori esterni quali, ad esempio, la normativa sulla protezione nell" ambiente e tendono perciò a coincidere per tutte le aziende operanti nel medesimo settore (PricewaterhouseCoopers, 2006). Una volta fissati gli obiettivi, sia a livello globale d'azienda che a livello più specifico di singole attività, è possibile passare all'identificazione, alla valutazione e all'analisi dei rischi, processo continuo ed interattivo, elemento chiave di un sistema di controllo interno. Per quanto concerne la fase di identificazione, è importante sottolineare come la performance di un "azienda possa essere a rischio sia a causa di fattori esterni (quali il progresso tecnologico, i cambiamenti dei bisogni o delle attese della cliente la, la concorrenza, le catastrofi naturali e i cambiamenti economici) che a causa di fattori interni (come la competenza del personale assunto, un cambiamento nell'attribuzione delle responsabilità, la natura dell'attività svolta e il livello dei sistemi informatici).

  Entrambi possono influire su ogni tipo di obiettivo, formulato o implicito. Sono state sviluppate numerose tecniche di identificazione dei rischi, in gran parte delle quali vengono applicati metodi quali –quantitativi che determinano le priorità e le attività ad alto rischio. Alcune tecniche normalmente utilizzate consistono nello svolgimento di esami periodici dei fattori economici ed industriali che interessano l'attività svolta, nell'esame di piani strategici ed analisi di settore.

La scelta di un metodo piuttosto che di un altro per il procedimento di identificazione non assume parti colare importanza. Ciò che risulta essere invece davvero rilevante è che i dirigenti tengano conto attentamente delle determinanti dei rischi e delle cause di un loro ed eventuale aggravamento. I fattori da prendere in considerazione sono in particolare:

- la mancata realizzazione in passato degli obiettivi;
- la competenza del personale;
- i cambiamenti che influenzano l'attività aziendale;
- la localizzazione geografica delle attività;
- l'importanza di una specifica attività per l'impresa nel suo complesso;
- la complessità di una certa attività (PricewaterhouseCoopers, 2006).

Una volta identificati i principali rischi, è possibile ponderarli ed eventualmente ricondurli alla specifica attività dell'impresa. Tale analisi può essere svolta in diversi modi, ma in ogni caso deve articolarsi comprendendo:

- una valutazione dell'importanza del rischio;
- una valutazione delle probabilità che si verifichi;
- delle considerazioni sul modo in cui il rischio dovrà essere gestito e quindi una valutazione delle misure che dovranno essere adottate.[55]

È da notare la differenza esistente tra la valutazione dei rischi, che è parte integrante del controllo interno, e i programmi individuati dal management per la gestione degli stessi. Gli interventi decisi, infatti, sono ovviamente un elemento rilevante del processo manageriale, ma non rappresentano una componente del sistema di controllo interno. Al fine di valutare adeguatamente i rischi a cui è esposta una determinata società è inoltre di fondamentale importanza implementare un processo di riconoscimento dei cambiamenti, che sia in grado, in modo più o meno formale, di

[55] "Enterprise Risk Management - Integrated Framework", accessed March 23, 2011

identificare gli eventi capaci di incidere sulla possibilità di realizzazione degli obiettivi fissati.

Un fattore indispensabile di questo processo è sicuramente un adeguato sistema informativo che riconosca ed elabori informazioni su eventi o attività che potranno richiedere una particolare reazione da parte della società per il perseguimento degli scopi già prefissati. Solo sulla base delle informazioni raccolte da tale sistema si potrà iniziare un processo di identificazione e reazione ai cambiamenti verificatisi, il quale potrà svilupparsi parallelamente a quello di valutazione dei rischi o potrà essere anche una parte dello stesso.

Il procedimento di valutazione dei rischi fin qui descritto può subire delle variazioni nel momento in cui viene implementato all'interno di società medio – piccole, tipiche della realtà italiana. In queste società, infatti, si ha da un lato una minore formalizzazione della definizione degli obiettivi, che spesso sono di tipo implicito piuttosto che esplicito, e dall'altro si assiste spesso a una struttura maggiormente centralizzata in cui il CEO e gli alti dirigenti impegnati nella valutazione dei rischi sono anche coinvolti nelle operazioni correnti.

Ciò sicuramente ha un impatto positivo sull'intero processo in quanto i rischi sono valutati dalle persone che non solo hanno accesso alle informazioni opportune, ma hanno anche una buona cognizione del lato pratico. L'espressione di un giudizio di valore sul procedimento di valutazione dei rischi dovrà pertanto tenere in considerazione, in modo forse più determinante che per le altre componenti del sistema di controllo interno, della realtà in cui lo stesso procedimento di analisi è stato implementato. L'attenzione dovrà essere posta in particolare sull'iter seguito dal management per determinare gli obiettivi, per valutare i rischi e gestire i cambiamenti, tenendo in considerazione anche le relazioni e la pertinenza con le diverse attività dell'azienda.[56]

[56] PricewaterhouseCoopers, 2006

3.3.3 L ’attività di controllo

Le attività di controllo si possono definire come l’applicazione delle politiche e delle procedure che garantiscono al management l’attuazione pratica delle sue direttive. Esse garantiscono l’adozione dei provvedimenti necessari per far fronte ai rischi che potrebbero minacciare la realizzazione degli obiettivi aziendali e, sulla base di questi ultimi, si possono suddividere in tre categorie:

- attività di controllo relative agli aspetti operativi;
- attività di controllo sulle informazioni di bilancio;
- attività di controllo sul rispetto dei vincoli legali e regolamentari.

La natura delle attività di controllo, a differenza delle altre componenti del sistema, è definita sulla base della singola realtà aziendale e deve tener conto del settore in cui l’impresa opera, delle sue dimensioni, della missione e, naturalmente, degli obiettivi e dei rischi specifici.

Il CoSO Report pertanto si limita solo a menzionare alcuni tipi di attività di controllo applicabili in termini generali. A titolo di esempio vengono citate le seguenti categorie (PricewaterhouseCoopers, 2002):

- controlli preventivi, contestuali o successivi all’attività specifica da verificare, tra i quali vengono incluse anche le analisi svolte dall’alta direzione sulle performance aziendali comparate con i budget, le proiezioni e i risultati dei prece denti periodi o dei concorrenti;

- controlli manuali o automatizzati, con particolare cura, nel caso siano attuati i controlli del primo tipo, al rispetto del principio della separazione dei compiti finalizzato alla riduzione del rischio di errori e di irregolarità.

È rilevante pertanto accertare che, ad esempio, le attività di autorizzazione delle operazioni, di contabilizzazione delle stesse e di gestione dei beni corrispondenti siano svolte da persone diverse, o ancora verificare che la persona che autorizza le vendite a credito non sia anche responsabile della tenuta della contabilità clienti e non abbia accesso agli incassi:

- controlli direzionali e tecnico – operativi;

- controlli fisici o attraverso indicatori, i primi consistenti nell'inventario di attrezzature, scorte, titoli, liquidità e altre attività che vengono confrontati con le risultanze contabili, i secondi utili per effettuare delle analisi comparate di dati, operativi o finanziari. Le informazioni ottenute da queste verifiche possono essere utilizzate sia per prendere decisioni gestionali, sia per verificare risultati inattesi evidenziati dal sistema contabile, contribuendo in tal modo non solo all'effettuazione dei controlli operativi, bensì anche di quelli relativi alle informazioni di bilancio;

- controlli sui processi e sui dati, eseguiti per verificare l'accuratezza, la completezza e l'adeguata registrazione delle operazioni. I dati inseriti nei sistemi sono sottoposti, attraverso questa tipologia di riscontri, a procedure automatiche di controllo e sono confrontati con archivi di verifica approvati;

- controlli mirati alla verifica delle corrette procedure di autorizzazione che possono essere di tipo generale, se si riferiscono ad operazioni della medesima specie, o specifiche, se riguardanti un singolo caso.

Il CoSO Framework dedica inoltre un intero capitolo ai sistemi informativi e fornisce in merito le seguenti indicazioni. Innanzitutto, viene specificato come i controlli applicati ai sistemi informativi gestiti con mezzi unicamente manuali siano differenti da quelli attuati sui sistemi computerizzati, nonostante le due tipologie di controlli si basino su concetti identici.

In generale, infatti, le attività di verifica sui sistemi informativi si possono suddividere in due gruppi: i controlli generali e i controlli applicativi. I primi interessano principalmente le operazioni svolte dal CED10, l'acquisto, lo sviluppo nonché la manutenzione del software di sistema e la protezione degli accessi. I controlli applicativi, invece, comprendono le procedure automatizzate e le relative procedure manuali per verificare l'elaborazione delle diverse operazioni.

Tali attività servono per controllare il corretto funzionamento dei programmi, assicurando la completezza e l'accuratezza dell'elaborazione delle operazioni, la loro autorizzazione e la il ro validità (PricewaterhouseCoopers, 2006). La situazione in Italia, in merito alle attività di controllo sui sistemi informativi, mostra come tutte le realtà svolgano solo alcune delle attività sopramenzionate e consigliate.

Mentre infatti si fanno spesso le procedure di verifica più semplici come quelle aventi ad oggetto gli accessi alle informazioni o le attività di back – up, risultano essere ancora piuttosto trascurate altre tipologie di controlli, come il frequente cambio delle password o lo sviluppo di un piano informatico in caso di emergenza.

Nelle realtà medio – piccole, inoltre, certe attività di controllo non saranno mai adottate, in particolare in presenza di un controllo efficace del management. In queste organizzazioni, per di più, si possono addirittura incontrare delle difficoltà per quanto riguarda l'implementazione di certe attività di controllo.

Si pensi alla separazione dei compiti, che in una realtà aziendale numericamente limitata può rivelarsi anche impossibile. In questi casi, tuttavia, si può sopperire all'inconveniente garantendo una supervisione diretta del titolare dell'impresa sulle attività incompatibili, che assicuri in tal modo il necessario controllo.

Ad esempio, non è raro, nel momento in cui esiste un rischio di pagamenti irregolari, che sia il proprietario stesso dell'impresa il solo autorizzato a sottoscrivere gli assegni o che venga richiesto alla banca di inviare al titolare gli estratti conto mensili in busta chiusa per una verifica degli assegni emessi. Nelle piccole – medie imprese si possono verificare inoltre problemi legati ai controlli sul sistema informatico, dovuti a una scarsa formalizzazione delle verifiche che lo riguardano.

Anche in questi casi la soluzione può derivare da un maggiore coinvolgimento del vertice nelle operazioni di gestione, coinvolgimento che gli consentirebbe di utilizzare più spesso e conseguentemente valutare le informazioni prodotte dal sistema, tenendo conto anche della sua conoscenza diretta dell'attività, individuando così, con una ragionevole sicurezza, i potenziali errori.

La realtà italiana, per quanto riguarda l'implementazione di questa componente del sistema di controllo interno, dimostra di non aver ancora sviluppato delle tecniche di controllo raffinate, piuttosto di aver introdotto procedure di verifica solo in conseguenza di situazioni di emergenza, che si sono stratificate l'una sull'altra, molte volte anche in modo scoordinato. Nelle nostre imprese occorre pertanto procedere a una rivisitazione delle attività di controllo, per evidenziare processi obsoleti, inutili duplicati o semplicemente non più adeguati e soprattutto per individuare le aree a rischio non adeguatamente presidiate. In seguito, sono riportate alcune linee guida che offrono uno spunto per effettuare tale analisi.

3.3.4 L'informazione e la comunicazione

Le informazioni sono fondamentali per il governo dell'azienda. Indipendentemente dal fatto che siano elaborate manualmente piuttosto che con supporti informatici, esse sono lo strumento che consente di gestire e controllare tutti i processi aziendali nonché di presidiare le variabili esterne che incidono sulla realtà d'impresa.

Dalla qualità e dalla quantità di informazioni diffuse all'interno di un "organizzazione dipende inoltre la valutazione in merito all'efficacia e all'efficienza della gestione, all'attendibilità delle informazioni di bilancio e alla conformità alle leggi. La maggiore problematica connessa a questa componente del sistema di controllo interno interessa da un lato la qualità delle informazioni fornite, da intendersi in termini di contenuto, puntualità, aggiornamento, precisione e comprensibilità, e dall'altro l'efficienza dell'elaborazione dei dati. Il contesto italiano, da questo punto di vista, non è molto differente da quello presente in altri Paesi, in primis gli stessi Stati Uniti, e come questi può essere ancora notevolmente migliorato.

Un aspetto assolutamente fondamentale da tenere in considerazione nel momento in cui si analizza la componente informativa di un sistema di controllo interno è la tempestività dei dati forniti ai vari soggetti dell'impresa. [57]

Rendere disponibile un "informazione in ritardo, con tempi non coerenti con il processo o il periodo a cui essa si riferisce, rende il dato stesso del tutto inutile ed inefficace, non essendo più possibile, ad esempio, modificare una circostanza del passato. Un sistema informativo lento rischia di produrre unicamente informazioni ridondanti, duplicate, assolutamente non efficaci per la direzione e per tutti coloro che sono coinvolti nell'attività di controllo.

[57] Monda B., Giorgino M., "An ERM maturity model"

Per tale ragione è importante non solo individuare in modo puntuale le informazioni di cui si ha effettivamente bisogno, ma persino pianificare il sistema informativo nel suo complesso, verificandone la coerenza con gli obiettivi, le strategie e i fattori critici di successo dell'azienda.

Purtroppo, nella realtà italiana, come anche nelle realtà di altri Paesi, il concetto di sistema informativo richiama spesso quello di tecnologia, con la conseguenza che molte imprese si preoccupano più di implementare l'ultima novità in ambito informativo, piuttosto che di attuare un sistema che sia davvero adeguato alle loro esigenze aziendali.

Spesso può essere un errore ritenere che le nuove tecnologie, solo in quanto tali, siano in grado di garantire un maggiore controllo o una migliore fornitura di dati e informazioni. In certe realtà, infatti, vale esattamente il contrario: le esigenze dell'impresa sono maggiormente soddisfatte da un sistema che, seppur sorpassato, risulta essere collaudato e soprattutto costruito intorno alle necessità della società. Accanto alle informazioni, assume un ruolo altrettanto critico la comunicazione. Essa è una funzione intrinseca ai sistemi informativi e può riguardare interlocutori interni piuttosto che esterni.

Nel primo caso la comunicazione deve perseguire l'obiettivo di rendere ciascun membro dell'organizzazione cosciente delle responsabilità a lui attribuite e delle aspettative nutrite nei suoi confronti in modo tale da consentirgli di segnalare ogni eventuale problema relativo la sua attività e, in particolare, il sistema di controllo. La comunicazione, all'interno di una realtà aziendale, deve fluire costantemente in ogni direzione: verso il basso, verso l'alto e trasversalmente. Un "indagine svolta presso alcune grandi organizzazioni in Europa, compresa l'Italia, ha evidenzia to come nelle imprese vengano spesso attuate reti di comunicazione informali molto più efficaci e consolidate di quelle formali, legate alla gerarchia aziendale.

Lo studio ha perciò raccomandato come sia molto importante individuare e comprendere anche questi canali, che non vanno assolutamente tralasciati e che, comunque, possono essere utili per sviluppare un sistema di comunicazione consono alle necessità di governo e controllo aziendale (PricewaterhouseCoopers, 2002). Altrettanto importante è la comunicazione verso l'esterno. Con ciò non si intendono solo le informazioni indirizzate ai soci, alle autorità, agli analisti e alla stampa, ma anche i dati forniti ai clienti, ai fornitori e alle banche, ovvero agli interlocutori quotidiani dell'impresa. La comunicazione verso soggetti esterni deve essere anch'essa adeguatamente pianificata e deve essere valutato attentamente persino il canale comunicativo da utilizzare, ponendo in particolare l'attenzione non solo sui contenuti, ma anche sulle modalità e sui tempi. Tale comunicazione può essere migliorata da un lato fornendo un maggior numero di informazioni in merito ai bilanci e alle relazioni periodiche, o incrementando la loro trasparenza, dall'altro richiedendo, con chi ha un interesse, anche non societario, nell'impresa, incontri periodici più frequenti che consentono non solo di consolidare il governo e il controllo societario, ma addirittura arricchiscono l'intero sistema in cui l'azienda è inserita e opera (PricewaterhouseCoopers, 2002). In generale, le comunicazioni possono assumere diverse forme: si individuano infatti manuali, bollettini, promemoria, fogli in bacheca, messaggi vocali o videomessaggi, per i quali assume un ruolo molto importante anche il tono della voce e la gestualità. Nelle piccole aziende, in genere, i sistemi informativi sono meno formali di quelli implementati nelle realtà di grandi dimensioni, nonostante il loro ruolo sia pur sempre importante. Tuttavia, con la moderna tecnologia informatica, la formulazione dei dati interni avviene con la medesima efficacia in gran parte delle imprese, a prescindere dalle loro dimensioni.

Nelle società più piccole si riscontra sicuramente un vantaggio che nelle altre imprese non è individuabile, ossia una molto più agevole comunicazione interna tra l'alta direzione e i dipendenti, che risulta essere più efficace grazie appunto alle ridotte dimensioni organizzative, alla limitata gerarchia e alla maggiore disponibilità e presenza del top management. Tali contatti interpersonali più frequenti sopperiscono molto spesso alla mancanza di un sistema di comunicazione formale e pertanto vanno assolutamente tenuti in considerazione al momento della valutazione di questa componente del sistema di controllo interno, come è indicato, in analogia alle altre componenti fin qui presentate, nella seguente traccia di analisi.

3.3.5 Il monitoraggio

I sistemi di controllo interno mutano nel tempo, così come possono cambiare anche le condizioni per le quali era stato originariamente pensato l'intero sistema. Per tale ragione è necessario che il management determini periodicamente se la struttura dei controlli esistente sia ancora valida, adatta e pertinente alla gestione dei rischi. Il monitoraggio è proprio quella componente del sistema che assicura che il controllo interno continui a funzionare efficacemente. Tale processo consiste nella valutazione critica del modo con cui sono disegnati i controlli, dei tempi di esecuzione e delle modalità con cui vengono adottati i provvedimenti necessari. Il monitoraggio può essere effettuato in due modi; si parla infatti di attività di monitoraggio continuo e di interventi di valutazione specifici.

Con le prime si intendendo le procedure di controllo che vengono effettuate automaticamente dal sistema stesso e che quindi sono integrate nelle normali attività operative dell'azienda. Proprio perché tali operazioni sono svolte in tempo reale, consentono di reagire immediatamente ai cambiamenti interni ed esterni e sono più efficaci rispetto al monitoraggio effettuato con mezzi di valutazione distinti. Quanto più il monitoraggio continuo è efficiente, tanto minore sarà la necessità di ricorrere a strumenti specifici di valutazione.

Tra i controlli effettuati in via continuativa da un "impresa si possono annoverare le attività di supervisione e di gestione corrente, le analisi comparative e le riconciliazioni effettuate con documenti forniti da terzi (PricewaterhouseCoopers, 2006).

Nonostante le procedure di monitoraggio continuo forniscano interessanti informazioni sul funzionamento di tutte le componenti del sistema di controllo interno, è importante periodicamente concentrarsi in modo più attento e specifico sull'efficacia del sistema nel suo complesso, eseguendo delle valutazioni più dettagliate.[58]

[58] 27. Bertinetti G., Cavezzali E., Gardenal G., 2013, "The effect of Enterprise Risk Management implementation on the firm value of European companies".

Queste consistono solitamente in autovalutazioni attraverso le quali i soggetti a cui è delegata la gestione di un "unità o funzione stabiliscono di fatto l'efficacia dei controlli all'interno della propria attività. Chi effettua una valutazione deve mirare a comprendere sia ognuna della singole attività dell'impresa che ciascun componente del sistema di controllo interno; questo obiettivo può essere perseguito unicamente relazionandosi con le persone che quotidianamente si raffrontano con le procedure aziendali e che ogni giorno svolgono o sono sottoposte ai controlli del sistema.

Esiste un ampio range di metodi e strumenti di valutazione utilizzabili, quali check list, questionari o diagrammi di flusso. Alcune imprese adottano addirittura un benchmark di riferimento, solitamente un sistema implementato in un "altra società, e raffrontano la loro situazione attuale con quest'ultima, rappresentante, nella loro valutazione, il modello ideale da perseguire.

I soggetti incaricati per la prima volta di eseguire una valutazione dei sistema di controllo interno possono fare riferimento, ad esempio, alla seguente procedura, che illustra il punto di partenza del procedimento e lo sviluppo dello stesso:

1. determinare le categorie di obiettivi, le componenti del controllo interno e le attività da studiare, ovvero definire il campo d'azione della valutazione;
2. identificare le attività di monitoraggio continuo insite nel sistema di controllo interno che ne confermano il corretto funzionamento;
3. valutare l'analisi dei controlli svolta dai revisori interni, come anche i rilievi emersi durante gli interventi dei revisori esterni;
4. determinare le priorità per aree ad alto rischio che richiedono un "immediata attenzione;
5. sulla base dei risultati fin qui ottenuti, delineare un programma di valutazione organizzato in interventi a breve e a lungo termine;

6. riunire i soggetti che si occuperanno praticamente della valutazione, studiare con il team non solo l'ambito e i tempi di realizzazione, ma anche la metodologia, gli strumenti, le informazioni fornite dai revisori interni e dalle autorità, i mezzi per rendere noti i rilievi e la documentazione da elaborare;

7. monitorare l'avanzamento della valutazione ed esaminare quanto da questa emerso;

8. verificare se siano state attivate azioni correttive e modificare, se necessario, i punti successivi del programma valutativo.

Nel momento in cui, durante l'attività di monitoraggio, viene riscontrata una carenza, potenziale o reale, o è stato individuato un punto del sistema di controllo che potrebbe essere migliorato e rafforzato, è indispensabile che il valutatore, nel minor tempo possibile, riporti quanto appurato all'attenzione del responsabile aziendale che ha l'autorità di provvedere alle adeguate azioni correttive.

Ovviamente il maggiore o minore grado di formalità dell'intero processo sarà funzione della cultura e delle dimensioni della società, anche se in linea generale la valutazione dei sistema segue le stesse linee in qualunque tipo di impresa. Le affermazioni raccolte in seguito rappresentano una sorta di linee guida da seguire nel procedimento di monitoraggio del sistema di controllo e integrano il procedimento menzionato in questo paragrafo.

3.4 La gestione del rischio aziendale

Successivamente al Report del 1992 la Committee of Sponsoring Organizations of the Treadway Commission (CoSO) ha pubblicato nel 2004 un nuovo Framework di riferimento per aiutare le società a disegnare ed implementare efficaci approcci per la gestione del rischio. Alcuni studiosi hanno parlato pertanto di una sorta di nuova versione del CoSO Report, un modello di sistema di controllo interno aggiornato e integrato con nuove componenti. In realtà, il nuovo Framework presentato nel 2004 è qualcosa di più ampio rispetto al Report del 1992 e si focalizza maggiormente sul concetto di rischio, tant'è che il modello è stato proprio definito Enterprise Risk Management.

Con tale pubblicazione la Committee si è posta l'obiettivo di definire le principali componenti del processo di gestione del rischio aziendale, di individuare un linguaggio comune e di fornire una chiara Guidance per le imprese impegnate in tale attività di gestione. L"ERM perciò risulta essere uno schema di riferimento più ampio rispetto al CoSO Report in quanto ricomprende sicuramente i concetti relativi al sistema di controllo interno già espressi nel documento del 1992, ma li integra anche elaborando una più ampia definizione di controllo maggiormente focalizzata sui rischi aziendali.

I due Framework non sono incompatibili tra loro, ma anzi si basano di fatto sui medesimi concetti, tant'è che il modello presentato nel Report del 2004 riprende tutte e cinque le componenti del sistema di controllo interno fin qui delineate e le arricchisce e le integra con altre tre. Esistono tuttavia alcune differenze concettuali tra quanto esposto nella pubblicazione del 1992 e quella del 2004, tra cui il fatto che l'attività di gestione dei rischi considera questi ultimi all'interno del procedimento di elaborazione delle strategie aziendali e che quindi richiede al management di formulare ipotesi circa il livello di incertezza che la società è in grado di sopportare.[59]

Un "ulteriore distinguo che deve essere effettuato in merito ai due modelli riguarda le categorie di obiettivi che essi definiscono e mirano a perseguire con il loro Framework; il primo CoSO Report aveva individuato tre tipologie di obiettivi: operativi, di reporting finanziario e di conformità. Questi vengono tutti ripresi dal modello ERM, il quale amplia tuttavia la seconda categoria riferendosi con essa non solo ai bilanci pubblicati e soprattutto alla loro attendibilità, ma includendo nell'obiettivo di reporting qualunque tipo di documento elaborato dalla società, internamente o esternamente, a prescindere dalle informazioni in esso contenute, siano esse finanziarie o meno (Livatino M., et al., 2006). In aggiunta a queste tre classi di obiettivi, l"ERM ne identifica una quarta, quella degli obiettivi strategici, che solitamente operano a livelli sopraelevati rispetto alle altre categorie.

[59] 28. D'Arcy S., Brogan J., 2001, "Enterprise risk management", Journal of Risk Management of Korea 12 (1).

Questi ultimi, infatti, discendono direttamente dalla missione aziendale e determinano poi tutti gli altri obiettivi. In aggiunta a queste differenze, va annoverata l'importante novità introdotta dall"ERM, ovvero i nuovi concetti di rischio accettabile e di tolleranza al rischio, non considerati in precedenza dalla Committee.

Con il primo si intende il livello di rischio che una società è disposta ad affrontare pur di perseguire i suoi scopi e il suo oggetto sociale; è una sorta di parametro di riferimento indispensabile nella definizione delle strategie elaborate di volta in volta. Il rischio accettabile dipende fortemente dalla filosofia della società e a sua volta impatta in modo notevole sulla cultura e sull'operatività della società.

Spesso viene definito in termini qualitativi, ossia utilizzando aggettivi come "alto", "moderato", "basso"; talvolta al contrario le imprese mirano proprio a quantificare e misurare questo parametro, determinando target di crescita, redditività e rischio. Il concetto di tolleranza al rischio, invece, identifica lo scostamento accettato e ammesso rispetto a un dato obiettivo da conseguire; ad esempio un "impresa può preporsi il seguente obiettivo: il 98% delle consegne devono essere effettuate nei termini e nei tempi concordati, con una variazione accettabile che oscilla da un minimo di 97% a un massimo del 100%. Una volta individuate le somiglianze e le differenze tra questi due Framework proposti dal CoSO, è possibile ora analizzare meglio "Enterprise Risk Management, focalizzandosi anche sulle sue componenti e in particolare su quelle introdotte ex novo rispetto al modello del sistema di controllo interno.

L"ERM è definito, nel Report del 2004, come un processo posto in essere dal Consiglio di Amministrazione, dal management e da altri operatori della struttura aziendale, impiegato al fine di formulare delle strategie che interessino tutta l'organizzazione. Esso è progettato per individuare eventi potenziali che possano influire sull'attività aziendale, per gestire il rischio entro i limiti fissati dal rischio accettabile e per fornire con una ragionevole sicurezza il perseguimento degli obiettivi d'impresa (Associazione Italiana Internal Auditors, PricewaterhouseCoopers, 2006).

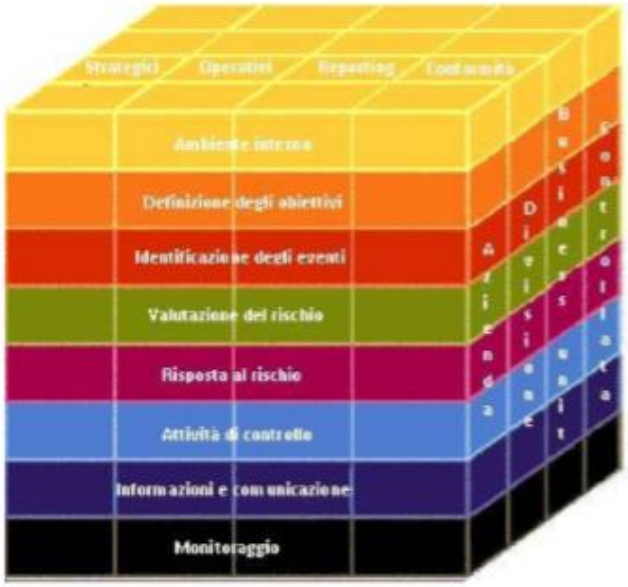
Leggendo questa definizione emergono molto chiaramente e palesemente altre somiglianze con la definizione che era già stata fornita per il sistema di controllo interno; in entrambi i casi, infatti, si parla di un processo dinamico, svolto da persone collocate a tutti i livelli organizzativi di una società che utilizzano poi il modello per la definizione e implementazioni di tutti i target aziendali, siano essi di carattere generale o di tipo specifico, legati a un "intera divisione o riservati a una singola attività. Anche per quanto riguarda l'affidabilità del metodo, la Committee si è premurata di inserire nella definizione dall" ERM il fatto che anche questo strumento potrà garantire unicamente una ragionevole certezza ai soggetti apicali delle società che lo implementeranno, senza assicurare pur tuttavia una certezza assoluta.

L'entreprise Risk Management si compone di otto elementi:

1. l'ambiente interno, ovvero la filosofia di base della società da cui dipende il livello di rischio accettabile;
2. la definizione degli obiettivi, procedimento che deve intervenire antecedentemente all'identificazione degli eventi che possono rappresentare una minaccia al conseguimento dei target aziendali;
3. l'identificazione degli eventi, momento del processo che consente di comprendere quali sono le situazioni, definite eventi potenziali, che possono avere un impatto sull'attività aziendale sia in termini positivi che negativi;
4. la valutazione del rischio, che consente di analizzarlo e gestirlo;
5. la risposta al rischio, elaborata dal management e solitamente identificabile in una delle seguenti opzioni: evitare, accettare, ridurre e compartecipare;
6. le attività di controllo, volte ad assicurare che le risposte al rischio precedentemente prefissate siano davvero eseguite in modo efficiente;
7. le informazioni e le comunicazioni, necessarie a ogni livello aziendale per diffondere i valori aziendali e le scelte strategiche ed operative della società;
8. il monitoraggio, fondamentale per garantire una celere risposta ai cambiamenti di fattori sia interni che esterni.

Così come per il sistema di controllo interno, è possibile dare una rappresentazione grafica dall" ERM, fornita proprio all'interno del Report del 2004.

Tab 3.4.1 Rappresentazione dall" ERM esposto nel CoSO Framework del 2004.



La matrice tridimensionale esprime a pieno il rapporto diretto che esiste tra gli obiettivi di un "impresa e i componenti dall" ERM: questi ultimi sono tutti indispensabili per conseguire le quattro tipologie di target prefissate dall'impresa e, viceversa, ciascuna delle categorie di obiettivi è applicabile a ognuna delle otto componenti. Per poter stabilire l'efficacia di un modello ERM è necessario valutare non solo la presenza delle otto componenti ma anche il loro corretto funzionamento, singolarmente e nel complesso; le varie funzioni infatti possono anche compensarsi tra loro e sopperire vicendevolmente alle loro manchevolezze.

Come il modello presentato nel CoSO Report del 1992, anche l"ERM è applicabile a ogni tipo di azienda, indipendentemente dalle sue dimensioni, nonostante le piccole e medie imprese possano in realtà disporre di un sistema di gestione del rischio costruito in modo un po'" differente rispetto ai modelli implementati nelle grandi società (Associazione Italiana Internal Auditors, et al., 2006).[60]

[60] 26. "The Trouble with COSO", March 15, 2006, accessed March 23, 2011.

Tornando alle singole componenti dell'entreprise Risk Management, è opportuno focalizzarsi maggiormente solo sulle tre che sono state introdotte ex novo rispetto al precedente modello del sistema di controllo interno; l'ambiente di controllo, la valutazione del rischio, l'attività di controllo, le informazioni/comunicazioni e il monitoraggio sono infatti sostanzialmente ripresi dal CoSO Framework del 1992, pur ponendo maggiore attenzione, in questa loro seconda versione, al concetto di rischio in termini di probabilità che si verifichi e in termini di impatto potenziale.

Vengono introdotti inoltre i concetti di rischio inerente, ossia il rischio che un "azienda si assume nel momento in cui la direzione non mette in atto alcun tipo di soluzione per intervenire su di esso, e rischio residuo, ovvero rischio che rimane dopo aver attivato misure di risposta, da valutare entrambi con le medesime unità di misura con cui vengono quantificati gli obiettivi che essi stessi minacciano.

Viene infine posta sicuramente più enfasi sulla componente informazioni e comunicazioni, che non tiene più solo in considerazione i dati presenti che dovrebbero fluidamente circolare all'interno dell'impresa, ma spazia ora dai dati provenienti dal passato a quelli inerenti eventi potenziali, considerando nell'intermezzo quelli attuali.

L'aspetto innovativo dall" ERM rispetto al sistema di controllo interno è tuttavia rappresentato non da queste "lievi" migliorie, bensì dall'introduzione di tre nuovi componenti:

- la definizione degli obiettivi;
- l'identificazione degli eventi;
- la risposta al rischio.

3.4.1 La definizione degli obiettivi

La definizione degli obiettivi rappresenta la componente dall" ERM fondamentale per un "adeguata identificazione degli eventi, valutazione dei rischi e risposta del management a questi. Il punto di partenza per una corretta definizione degli obiettivi aziendali è costituito dalla missione sociale sulla base della quale è possibile formulare gli obiettivi strategici da cui si potranno poi in seguito derivare target di tipo operativo, di conformità e di reporting (Olson D. L., et al., 2008). I primi riguardano principalmente l'efficacia e l'efficienza delle attività operative dell'impresa e dipendono fortemente dalle scelte del management in merito alla struttura organizzativa e al livello di performance che si vuole conseguire.

È assolutamente importante che essi rispecchino il contesto ambientale in cui l'impresa opera ed è altrettanto fondamentale che siano reali, adeguati al mercato e alle sue richieste e che siano espressi in modo tale da consentire una loro valutazione. Gli obiettivi di reporting interessano, invece, le relazioni che vengono elaborate e redatte dai membri della società, a prescindere dalla loro destinazione, se interna o esterna. Le informazioni contenute in questi report devono essere accurate e coerenti con i fini perseguiti.

Gli obiettivi di conformità, infine, si riferiscono al rispetto da parte della società delle leggi e dei regolamenti che vengono fissati a livello di settore o addirittura a livello nazionale (Associazione Italiana Internal Auditors, et al., 2006). L'allineamento degli obiettivi alla strategia è un requisito assolutamente fondamentale per garantire un certo successo all'impresa ed è per tale ragione che periodicamente sarebbe opportuno che il management riveda gli obiettivi fissati dalla società, essendo comunque la strategia dinamica e soggetta a rettifiche e cambiamenti a seconda anche delle condizioni ambientali interne ed esterne all'impresa.

Nell'individuare gli obiettivi la direzione aziendale deve preoccuparsi non solo di delinearli in modo chiaro ma anche di fornire contestualmente degli strumenti di misura degli stessi e del loro grado di conseguimento. Oltre alle categorie fin qui delineate ed esplicitamente previste dal modello descritto nel Framework del 2004 è possibile talvolta individuare, come obiettivo aziendale, anche quello definito come salvaguardia delle risorse, con il quale si intendono tutte quelle procedure finalizzate ad impedire perdite o danni ad attività patrimoniali dovuti a furti, sperperi o inefficienze.

La definizione degli obiettivi può seguire un procedimento più o meno formalizzato, sicuramente più elastico e conseguentemente meno rigido nelle imprese di dimensioni limitate, dove spesso i target della società sono comunicati verbalmente ai singoli dipendenti. Come per le componenti del sistema di controllo interno è possibile anche per questi ulteriori elementi delineati dall"ERM formulare delle linee guida per una loro valutazione ex post; a riguardo, in merito alla componente fin qui presentata, si può fare riferimento alle seguenti che ne sintetizzano i principi chiave.

3.4.2 L'identificazione degli eventi

Per evento si intende un fatto determinato da fonti interne o esterne all'impresa che impatta sull'implementazione della strategia o sul perseguimento degli obiettivi (Associazione Italiana Internal Auditors, et al., 2006). Esso può essere facilmente rileva bile piuttosto che di difficile individuazione e può avere conseguenze dall'impatto più o meno consistente sull'andamento dell'impresa. Per poter identificare tali eventi è importante che il management prenda prima in considerazione i fattori esterni ed interni che danno origine ad essi ed è importante che sviluppi una certa conoscenza degli stessi e della tipologia di eventi riferibili a ciascuno.[61]

[61] 27. Bertinetti G., Cavezzali E., Gardenal G., 2013, "The effect of Enterprise Risk Management implementation on the firm value of European companies".

Tra i fattori esterni su cui porre particolare attenzione si possono menzionare:

i. l'economia, da cui dipendono le oscillazioni dei prezzi, la disponibilità dei capitali, le barriere all'entrata di un determinato settore;
ii. l'ambiente, che può determinare eventi quali inondazioni, incendi o altre calamità naturali;
iii. la politica, da cui possono derivare cambi di programmi politici, nuove leggi o nuovi vincoli all'accesso di mercati internazionali piuttosto che nuove liberalizzazioni;
iv. la tecnologia, che con le sue innovazioni può determinare un aumento dei dati disponibili, una riduzione dei costi di struttura piuttosto che un incremento della domanda di servizi tecnologici.
v. Un simile elenco può essere stilato anche per i fattori interni, tra i quali si possono annoverare:
vi. le infrastrutture, che possono comportare ad esempio investimenti aggiuntivi di capitale;
vii. il personale, i cui eventi correlati possono consistere in infortuni sul lavoro, in contratti in scadenza che originano scioperi e dimissioni;
viii. i processi, da cui possono derivare eventi quali la modifica di un protocollo o l'individuazione di errori nello svolgimento di una certa attività (Associazione Italiana Internal Auditors, et al., 2006).

Una volta individuati i fattori principali, il management ha l'opportunità di valutare la loro importanza e la loro rilevanza nonché le tipologie e la natura di eventi che possono da essi scaturire. Un evento, infatti, può avere un impatto negativo o positivo. Nel primo caso esso si qualificherà come un rischio e, se si realizzerà, potrà pregiudicare il conseguimento degli obiettivi aziendali: il management, pertanto, dovrà sviluppare una certa strategia di risposta che consenta di salvaguardare i target fissati dall'organizzazione.

Al contrario, nell'eventualità in cui l'evento abbia il connotato della positività, sarà definibile come un "opportunità, ossia un evento che può incidere positivamente sul perseguimento degli obiettivi e sulla creazione di valore. Le opportunità richiedono comunque una risposta del management, in termini di riformulazione della strategia, che tenga conto a questo punto delle nuove condizioni di cui il vertice è venuto a conoscenza.

Diverse sono le tecniche che possono essere utilizzate al fine di identificare gli eventi; si può ad esempio ricorrere a delle analisi interne che, in corrispondenza del processo di pianificazione e controllo, attraverso degli incontri con il personale delle varie unità operative, mirano proprio a evidenziare gli eventi più probabili. Si può, però, prestare attenzione anche a segnalatori di criticità, meccanismi di controllo impiegati per avvisare la direzione aziendale della problematicità di una situazione in cui si può trovare la società in quel frangente; tali meccanismi, mediante un confronto diretto degli eventi con dei parametri predeterminati, sono in grado di individuare quelle situazioni in cui i livelli di tolleranza predefiniti sono stati superati, richiedendo così una risposta da parte della direzione aziendale.

Un "ulteriore tecnica che può essere portata a titolo di esempio per l'identificazione degli eventi è quella incentrata su workshop e interviste, che ricorrono alle conoscenze e all'esperienza del management, del personale o di altri stakeholder attraverso incontri organizzati (Associazione Italiana Internal Auditors, et al., 2006). L'analisi degli eventi non riguarda solo gli stessi considerati individualmente, ma anche in correlazione tra di loro; per tale ragione spesso è utile effettuare dei raggruppamenti degli eventi potenziali in categorie, orizzontali se l'accento viene posto sul livello aziendale, verticali se l'attenzione si sposta sulle unità operative. Al fine di valutare l'efficacia del procedimento con cui un "impresa individua e analizza gli eventi potenziali, è utile fare riferimento ad alcuni parametri, sintetizzati in seguito.

3.4.3 La risposta al rischio

Dopo aver valutato i rischi, viene richiesto al management di adottare una o più risposte alle situazioni potenziali o reali identificate, risposte che possano evitare fallimenti nel perseguimento degli obiettivi. Tutte le possibili risposte adottabili dalla direzione aziendale possono essere raggruppate in quattro categorie:

1. evitare il rischio, ad esempio eliminando una certa linea di produzione o rinunciando ad entrare in un dato mercato;
2. ridurre il rischio, intraprendendo azioni volte a diminuire la probabilità o le conseguenze del rischio stesso;
3. condividere il rischio, trasferendone una parte a un terzo soggetto;
4. accettare il rischio, senza implementare alcun tipo di sistema di protezione né di risposta. [62]

Prima e durante la formulazione di una risposta al rischio, il management deve tenere in considerazione non solo gli effetti che si potrebbero produrre in termini di probabilità e di impatto del rischio sulla situazione attuale, ma anche i costi e i benefici delle risposte potenziali. La risposta individuata non deve comportare necessariamente l'eliminazione del rischio, cosa assolutamente impossibile da realizzare data la scarsità delle risorse disponibili all'interno delle società e data l'incertezza del futuro, ma una riduzione del livello di rischio coerente e conforme alla tolleranza al rischio predeterminata dall'impresa.

[62] *Queste quattro tipologie di risposta sono state riassunte, nella formulazione inglese del modello, con l'appellativo delle quattro T's (Olsen D. L., et al., 2008): - treating a risk (accept it); - terminate a risk (avoid it); - transfer a risk (reduce it); - take or tolerate a risk (seek it).*

Nell'eventualità in cui il livello si dovesse mantenere ancora su indici piuttosto elevati rispetto allo standard prefissato, sarebbe opportuno da parte del management riesaminare e rettificare la risposta selezionata piuttosto che ridefinire il livello di tolleranza stabilito. Una volta individuata la risposta, potrebbe essere necessario sviluppare ed implementare un piano per la sua attuazione, controllato e monitorato attraverso la componente dell'attività di controllo. Per quanto concerne questa componente dell"ERM, risulta essere particolarmente difficile effettuare una valutazione di quanto deciso dal management, in quanto si rischierebbe di andare a giudicare un comportamento e un atteggiamento del tutto soggettivi: non è possibile infatti sindacare le scelte manageriali di un vertice aziendale che, nella sua posizione, può prendere le decisioni che meglio crede per conseguire i propri obiettivi.

È tuttavia possibile per lo meno analizzare ed esprimersi sul processo decisionale che porta alla formulazione di una risposta piuttosto che di un "altra per verificare, per lo meno, che la decisione non sia del tutto arbitraria e insensata, ma sia piuttosto razionale e giustificabile, per quanto, si ripete, opinabile. I punti di seguito elencati possono essere gli elementi da prendere in considerazione nello svolgimento di tale valutazione.

3.5 Coso Report & ERM

Il CoSO Report è il precursore di un modello di gestione del rischio più recente che prende il nome di modello ERM (Enterprise Risk Management). Poiché l'ERM integra amplia le funzioni del CoSO Report si è pensato fosse interessante descrivere questo nuovo approccio all'interno del presente capitolo così da offrire al lettore una panoramica più completa sui sistemi di gestione del rischio e controllo interno da un lato e un confronto tra le ultime innovazioni della teoria del risk management con ciò che invece avviene nella pratica lavorativa dall'altro.[63]

[63] 22. "Disegno e funzionamento del Sistema integrato di Controllo Interno" della Associazione Italiana Internal Auditors, Milano, 2008

L'ERM, che tratta dei rischi e delle opportunità che influenzano la creazione o la preservazione di valore, è definito come segue:

La gestione del rischio aziendale è un processo, posto in essere dal consiglio di amministrazione, dal management e da altri operatori della struttura aziendale; utilizzato per la formulazione delle strategie in tutta l'organizzazione; progettato per individuare eventi potenziali che possono influire sull'attività aziendale, per gestire il rischio entro i limiti del rischio accettabile e per fornire una ragionevole sicurezza sul conseguimento degli obiettivi aziendali

Questa definizione riflette alcuni concetti fondamentali. L'ERM è:

- un processo continuo e pervasivo che interessa tutta l'organizzazione;
- svolto da persone che occupano posizioni a tutti i livelli della struttura aziendale;
- utilizzato per la formulazione delle strategie;
- utilizzato in tutta l'organizzazione: sia nelle sue singole attività (in ogni livello e in ogni unità della struttura), che nella sua attività complessiva. Esso include una visione del rischio che considera l'azienda nel suo complesso;

  • progettato per identificare eventi potenziali che potrebbero influire sull'attività aziendale e per gestire il rischio entro i limiti del rischio accettabile;

  • in grado di fornire una ragionevole sicurezza al consiglio di amministrazione e al management;

  • in grado di conseguire obiettivi relativi a una o più categorie distinte, ma che si possono sovrapporre.

  Questa definizione è intenzionalmente estensiva e racchiude i concetti chiave, fondamentali per capire come le aziende devono gestire il rischio; fornisce i criteri di base da applicare in tutte le organizzazioni, quale che sia la loro natura. Si focalizza direttamente sul raggiungimento degli obiettivi di una specifica organizzazione e fornisce i criteri per valutare l'efficacia dell'ERM.[64]

[64] D'Arcy S., Brogan J., 2001, "Enterprise risk management", Journal of Risk Management of Korea 12 (1).

Nell'ambito della missione e della visione aziendale, il management definisce gli obiettivi strategici, sceglie la strategia e fissa gli obiettivi specifici, coerenti con la strategia, e li assegna a vari livelli della struttura organizzativa. L'ERM è finalizzato al conseguimento degli obiettivi aziendali rientranti nelle seguenti categorie:

- *strategici* - sono di natura generale e definiti ai livelli più elevati della struttura organizzativa, allineati e a supporto della missione aziendale;
- *operativi* - riguardano l'impiego efficace ed efficiente delle risorse aziendali;
- di *reporting* - riguardano l'affidabilità delle informazioni fornite dal
- *reporting*; di conformità - riguardano l'osservanza delle leggi e dei regolamenti in vigore.

Questa classificazione degli obiettivi aziendali consente di approfondire differenti aspetti della gestione del rischio. Queste categorie distinte, ma connesse o sovrapponibili (un determinato obiettivo può rientrare in più di una categoria) riguardano esigenze diverse dell'azienda e possono essere di competenza diretta di più manager. Questa classificazione consente inoltre di distinguere quanto ci si può attendere da ciascuna categoria di obiettivi. Un'altra categoria che riguarda la "salvaguardia delle risorse", adottata da qualche azienda, è descritta nel prosieguo di questo studio.

I componenti dell'ERM L'ERM è costituito da otto componenti interconnessi. Essi derivano dal modo in cui il management gestisce l'azienda e sono integrati con i processi operativi. Questi componenti sono:

a. *Ambiente interno* - L'ambiente interno, che costituisce l'identità essenziale di un'organizzazione, determina i modi in cui il rischio è considerato e affrontato dalle persone che operano in azienda, come pure la filosofia della gestione del rischio, i livelli di accettabilità del rischio, l'integrità e i valori etici e l'ambiente di lavoro in generale.

b. *Definizione degli obiettivi* - Gli obiettivi devono essere fissati prima di procedere all'identificazione degli eventi che possono potenzialmente pregiudicare il loro conseguimento. L'ERM assicura che il management abbia attivato un adeguato [65]processo di definizione degli obiettivi e che gli obiettivi scelti supportino e siano coerenti con la missione aziendale e siano in linea con i livelli di rischio accettabile.

c. *Identificazione degli eventi* - Gli eventi esterni e interni, che influiscono sul conseguimento degli obiettivi aziendali, devono essere identificati distinguendoli tra "rischi" e "opportunità". Le opportunità devono essere valutate riconsiderando la strategia definita in precedenza o il processo di formulazione degli obiettivi in atto.

d. *Valutazione del rischio* - I rischi sono analizzati, determinando la probabilità che si verifichino in futuro e il loro impatto, al fine di stabilire come devono essere gestiti. I rischi sono valutati in termini di rischio inerente (rischio in assenza di qualsiasi intervento) e di rischio residuo (rischio residuo dopo aver attuato interventi per ridurlo).

e. *Risposta al rischio* - Il management seleziona le risposte al rischio emerso (evitarlo, accettarlo, ridurlo, comparteciparlo) sviluppando interventi per allineare i rischi emersi con i livelli di tolleranza al rischio e di rischio accettabile.

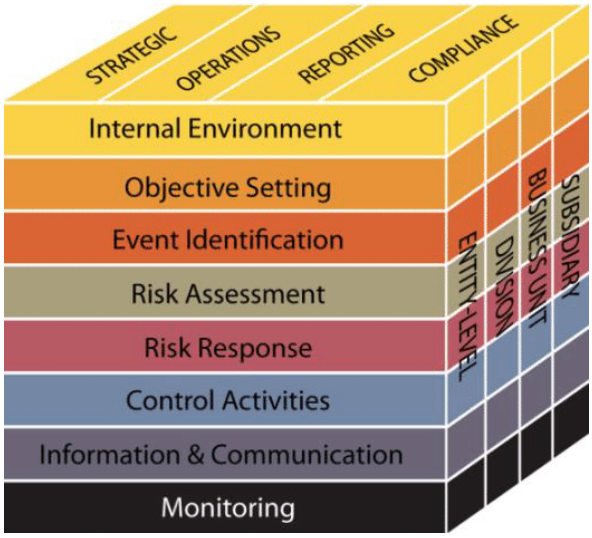
f. *Attività di controllo* - Devono essere definite e realizzate politiche e procedure per assicurare che le risposte al rischio siano efficacemente eseguite.

g. *Informazioni e comunicazione* - Le informazioni pertinenti devono essere identificate, raccolte e diffuse nella forma e nei tempi che consentano alle persone di adempiere correttamente le proprie responsabilità. In linea generale, si devono attivare comunicazioni efficaci, in modo che queste fluiscano per l'intera struttura organizzativa: verso il basso, verso l'alto e trasversalmente.

[65] 27. Bertinetti G., Cavezzali E., Gardenal G., 2013, "The effect of Enterprise Risk Management implementation on the firm value of European companies".

h. *Monitoraggio* - L'intero processo dell'ERM deve essere monitorato e modificato ove necessario. Il monitoraggio si concretizza in interventi continui integrati nella normale attività operativa aziendale o in valutazioni separate, oppure in una combinazione dei due metodi. L'ERM non è un procedimento strettamente sequenziale, nel quale un componente influisce solo sul successivo. Si tratta, invece, di un processo interattivo e multidirezionale in cui ogni componente può influire o influisce su un altro componente, indipendentemente dalla sequenza del processo.

Tab 3.5.1 Enterprise Risk Management



Esiste un rapporto diretto tra obiettivi, ossia ciò che un'azienda si sforza di conseguire, e i componenti dell'ERM, ovvero ciò che occorre per conseguire gli obiettivi. Questo rapporto è schematizzato in una matrice tridimensionale a forma di cubo. Le quattro categorie di obiettivi – strategici, operativi, di reporting e di conformità – sono rappresentate nelle colonne verticali del cubo, gli otto componenti sono invece rappresentati nelle righe orizzontali del cubo, e le unità operative dell'organizzazione sono rappresentate dalla terza dimensione della matrice.[66]

[66] Bertinetti G., Cavezzali E., Gardenal G., 2013, "The effect of Enterprise Risk Management implementation on the firm value of European companies".

Questo schema fa capire l'estrema flessibilità del modello, che qui si illustra: esso può essere applicato, sia all'intero processo di gestione del rischio aziendale, sia distintamente alle singole categorie di obiettivi, ai componenti, alle singole unità operative e alle singole sub unità di queste ultime.

La valutazione dell'efficacia del processo di gestione del rischio aziendale è un giudizio soggettivo, fondato sulla presenza degli otto componenti e sul loro corretto funzionamento. Pertanto, i componenti costituiscono anche dei criteri di efficacia. Così, se in un processo tutti gli otto componenti sono presenti e funzionano correttamente, ciò rappresenta una prova dell'assenza di debolezze significative e che i rischi che si vogliono affrontare sono al di sotto del livello di rischio ritenuto accettabile.
Quando un processo di gestione del rischio aziendale è giudicato efficace per ciascuna delle quattro categorie di obiettivi, ciò significa che il consiglio di amministrazione e il management hanno una ragionevole sicurezza di venire a conoscenza della misura in cui gli obiettivi strategici e operativi si stanno conseguendo, che i report sono affidabili e che le leggi e i regolamenti in vigore sono osservati. Gli otto componenti non funzionano in modo identico in ogni azienda. L'applicazione del modello, in aziende medio-piccole, per esempio, potrebbe essere meno formale e meno strutturata. Ciò nondimeno, le piccole aziende possono avere un efficace processo di gestione del rischio, purché ciascun componente sia presente e funzioni correttamente.

Sebbene l'ERM procuri importanti benefici, tuttavia, esistono dei limiti. Oltre ai fattori illustrati in precedenza esistono dei limiti dovuti a possibili errori di giudizio quando si prendono decisioni gestionali, all'impossibilità di proteggersi da tutti i rischi anche perché il rapporto costi-benefici diverrebbe gravoso, a errori umani che possono procurare danni involontari, alla possibilità che i controlli siano aggirati da parte di due o più persone in collusione e al management che può eludere le decisioni sulla gestione dei rischi.

Queste limitazioni non consentono al consiglio di amministrazione e al management di ottenere una sicurezza assoluta sul conseguimento degli obiettivi aziendali. Il controllo interno è parte integrante dell'ERM, che qui si presenta. Pertanto, il modello di gestione del rischio aziendale incorpora il controllo interno fornendo un più completo strumento per il management. Il controllo interno è definito e descritto nella pubblicazione intitolata "ill sistema di controllo interno".

Poiché questa pubblicazione ha superato bene la "prova del tempo" e ha costituito la base per regolamenti e leggi attualmente in vigore, essa rimane ancora valida come pure la definizione e il modello di controllo interno. Sebbene solo una parte della pubblicazione" Il sistema di controllo sia riprodotta in questo studio, ciò nondimeno questa pubblicazione è da considerarsi virtualmente parte integrante del presente volume.

3.5.1 Coso Report: principio 8 nell'ambito del risk assessment.

Il merito al "*Modello di organizzazione gestione e controllo ai sensi del D.LGS 231/2001*" tenendo fede al documento di risk assessment-Anticipazione L190/12; Sezione III Piano di prevenzione della corruzione, ritengo importante a questo punto dell'elaborato soffermarsi sulla categorizzazione dei reati, in particolare sui reati corruttivi. Il documento sopra riportato[67], mappa i diversi rischi di corruzione identificando 58 casistiche diverse. Il reato riconosciuto con il numero 8 riguarda "*Reati corruttivi previsti dal Codice penale (reati contro la PA) non rientranti nei reati di cui al D.lgs. 231/01. Comportamenti non penalmente rilevanti che denotano situazioni di cattiva amministrazione a causa di interessi privati che condizionano impropriamente l'azione dell'amministrazione*". In particolare, si fa riferimento:

[67] *Modello di organizzazione gestione e controllo ai sensi del D.LGS 231/2001*

(Reati strumentali). Corruzione per un atto contrario ai doveri di Ufficio (art. 319), Induzione indebita a dare o promettere utilità (art. 319 quater), Istigazione alla Corruzione (art. 322), Abuso d'ufficio (Art. 323). Abuso del potere affidato per ottenere vantaggi privati, altre fattispecie penalmente non rilevanti.

Il reato potrebbe concretizzarsi, in linea di principio, attraverso l'alterazione di dati relativi alla ripartizione delle spese a carico dei condomini e degli assegnatari, determinando così un falso nel bilancio delle autogestioni e dei condomini. I reati strumentali alla commissione del reato descritto sono le condotte corruttive messe in atto, anche in ipotesi di concorso, sia da assegnatari, sia da esponenti dell'Ente.

3.5.2 I benefici dell'applicazione di un sistema di controllo interno

L'implementazione di un sistema di controllo interno e l'attuazione di un processo di gestione dei rischi non sono sicuramente di facile e immediata realizzazione, tenendo conto del fatto che, anche se progettati al meglio, non garantiscono la certa realizzazione degli obiettivi preposti dal management. Infatti, nonostante un "*accurata pianificazione dei procedimenti*" e un "attenta cura alla loro realizzazione, non è comunque possibile evitare errori umani nell'operatività o nel processo decisionale, disfunzioni del sistema di controllo stesso, eccezioni stabilite dal vertice aziendale piuttosto che mala gestione da parte dei soggetti responsabili [68].

Inoltre, un fattore a sfavore dell'attuazione di questi modelli riguarda il loro costo, particolarmente gravoso per le società medio piccole; l'aspetto critico, per di più, non risiede solamente nell'ingente valore che possono raggiungere tali costi, ma anche nella loro aleatorietà, in quanto difficili da valutare e da prevedere.

[68] PricewaterhouseCoopers, 2002

Ciò nonostante, l'implementazione di un sistema di controllo interno non presenta solo elementi a proprio svantaggio, ma, al contrario, annovera molti benefici, primo fra tutti la possibilità di avere a disposizione dati finanziari precisi, con tutte le conseguenze positive in termini di accesso agevolato al mercato dei capitali e facilitazione nell'approvvigionamento di risorse monetarie.

Un ulteriore beneficio riguarda inoltre l'opportunità di fruire di informazioni affidabili e tempestive utili sia per il processo decisionale manageriale, che risulta essere così sicuramente accelerato e più attendibile, sia per la comunicazione dei dati aziendali a soggetti interni ed esterni la società (Associazione Italiana Internal Auditors, PricewaterhouseCoopers, 2008). L'implementazione di un sistema di controllo interno, inoltre, protegge la reputazione della società in quanto garantisce la compliance da parte di quest'ultima alle norme, ai regolamenti e alle best practice di corporate governance.

L'adozione di controlli societari, in aggiunta, garantisce una migliore allocazione delle risorse, riducendo così sia le perdite che la volatilità dei risultati e massimizzando, alla fine, il profitto. Da ultimo è importante sottolineare, soprattutto ai nostri fini, come l'esistenza di procedure più o meno formalizzate di controllo e monitoraggio all'interno di un "impresa. abbassino il rischio di commissione di una frode poiché non solo riducono le opportunità di una sua realizzazione ma lasciano anche pochi spazi di movimento ai perpetratori che, costantemente sotto osservazione, hanno minori probabilità di successo nelle loro attività illecite.

I sistemi di controllo interno, in pratica, aiutano un "organizzazione a perseguire la sua missione, i suoi target di profittabilità, in quanto rappresentano un modo per gestire il rischio e assicurano che le direttive, le politiche, le procedure e le pratiche disegnate e approvate dalla direzione aziendale siano messe in atto e siano funzionanti così come previsto.

Sebbene sia molto più facile per una società introdurre semplicemente nuove procedure, aggiungendole a quelle già esistenti, risulta essere molto più produttivo concentrarsi sulle procedure già disponibili, rielaborandole ed integrandole in modo da pervenire a una corretta gestione e valutazione dei rischi. L'accumulazione delle prassi luna sull'altra, nonostante molto più veloce da attuare, rischia infatti solo di risultare un groviglio di meccanismi, poco integrati tra loro ed inutili per la gestione e l'organizzazione della società.

Un "impresa può sempre decidere di implementare un sistema di controllo, indipendentemente dal livello di procedure che ha già in atto al suo interno, tenendo conto del fatto che, una volta sviluppato un sistema, questo non potrà essere mantenuto invariato nel tempo, ma avrà comunque sempre bisogno di aggiornamenti, non fosse altro per cogliere le nuove opportunità fornite dal mercato o per adeguarsi ai recenti cambiamenti intervenuti nel settore.

CAPITOLO 4

TIPOLOGIE DI FRODE E RELATIVI STRUMENTI DI PREVENZIONE

Nel capitolo in oggetto andremo a parlare dei più diffusi schemi fraudolenti in diversi settori economici. L'analisi verrà svolta focalizzandosi sull'identificazione ed analisi dei principali red flag e sulle strategie in tema di prevention e detection.

4.1 Frodi bancarie

Gli istituti finanziari per moli di transazioni, sensibilità delle informazioni trattate e opportunità di profitto risultano generalmente tra i player maggiormente colpiti da eventi fraudolenti. Inoltre, a fronte dello sviluppo tecnologico in cui stanno investendo, le banche sono chiamati a fronteggiare nuovi rischi di frode dettati principalmente dall'introduzione di nuovi strumenti di pagamento digitali e dall'utilizzo dell'home banking e dallo sviluppo dell'open banking [69]da parte della propria clientela.

[69] L'open banking è una condivisione dei dati tra i diversi attori dell'ecosistema bancario, naturalmente autorizzata dai clienti. Nasce con la PSD2 (Payment Services Directive 2), direttiva europea sui pagamenti digitali, emanata nel 2018. Per la prima volta questa direttiva obbliga le banche europee ad aprire le proprie API (Application Program Interface) a società del fintech (tecnologia applicata alla finanza) e altre aziende che si occupano di prodotti e servizi finanziari. Questo cambiamento consentirà alle società esterne (le cosiddette terze parti) accesso ai dati di pagamento: in sostanza significa che ci sarà maggiore competizione nelle aree di tradizionale dominio delle banche.

Principali fattori di rischio dell'Industry

1. *Open banking*

   Le informazioni sensibili condivise con terze parti autorizzate potenzialmente intercettabili da soggetti terzi

2. *Nuovi strumenti di pagamento*

   Con una forte propensione tecnologica, gli strumenti di pagamento sono personali, in real time e supportati da diversi device/piattaforme terze

3. *Digital banking*

   Con una forte propensione tecnologica, gli strumenti di pagamento sono personali, operano in real time e sono supportati da diversi device/piattaforme terze

4. *Elevata liquidità*

   Il rischio di appropriazione indebita è favorito dall'utilizzo del contante o strumenti di pagamento di esigibilità equivalente

5. *Intermediari e controllo a distanza*

   Operatori di filiale ed ulteriori terze parti aumentano il rischio di perdita di controllo, trasparenza, adozione di standard qualitativi comuni

6. *Sistema di incentivazione*

   Quota parte di remunerazione di operatori bancari basata su volume d'affari generato in specifici archi temporali facilita comportamenti distorsivi

7. *Competitività del mercato*

- Prodotti non molto differenziabili favoriscono:
- Politiche aggressive di prezzo per ottenere clienti
- Comportamenti opportunistici della clientela

8. Frazionamento del rischio

- Antieconomicità della *detection* quando il rischio è di importo contenuto e stratificato su più clienti

I principali schemi di frode

Tenendo conto di quelli che sono gli schemi fraudolenti di pagamento; riconosciamo come strumenti principali:

a) Frodi con carte
b) Frodi con assegni
c) Frodi con money transfer
d) Transazioni non autorizzate
e) Transazioni autorizzate

Frodi con carte

Le principali condotte fraudolente in questo ambito riguardano:

1. Falsificazione di identità: il frodatore, una volta ottenuti fraudolentemente i dati identificativi di un cliente (ad esempio attraverso phishing), si finge quest'ultimo per ottenere il controllo su una carta già esistente, richiederne la riemissione o la modifica dei codici di sicurezza;
2. Contraffazione dello strumento di pagamento: il frodatore crea fraudolentemente una banda magnetica utilizzando come base una carta legittima (in questo caso il frodatore applica specifici device agli ATM atti a replicare i dati necessari per la successiva esecuzione delle transazioni);
3. Furto dello strumento di pagamento: il frodatore commette l'azione illecita utilizzando (i) una carta fisica rubata per acquisti presso merchant fisici e prelievi presso ATM o (ii) si appropri fisicamente dei codici dispositivi ad esempio intercettando le comunicazioni tra Banca e cliente.

Frodi con assegni

La contraffazione si ha con assegni non su carta intestata dell'istituto finanziario tratto sul c/c del frodatore, legittimo titolare. La classificazione è la seguente:

1. *Forged cheque fraud*: furto di assegno legittimo e compilazione dei dati necessari a beneficio del frodatore
2. *Fraudolently altered cheques*: modifica da parte del frodatore dei dati del beneficiario di un assegno emesso legittimamente dal proprietario
3. *Frode commessa sia da soggetti esterni* che da dipendenti, separatamente o in collusione

Frodi con money transfer

1. *Finta lotteria*: il frodatore comunica alla vittima di aver vinto un cospicuo premio, inoltra un assegno falso e richiede un money transfer per far fronte a oneri di tassazione e spese di processamento
2. *Finta/o compagna/o*: dopo aver instaurato una finta relazione a sfondo sentimentale su internet, il frodatore, attraverso un profilo falso, richiede money transfer alla vittima per importi sempre più consistenti per far fronte a necessità improvvise e critiche
3. *Finto arresto:* il frodatore si finge un conoscente della vittima e richiede un money transfer per pagare la cauzione ed uscire di prigione
4. *Individuazione del target*: reddito medio-basso, dati di contatto disponibili su piattaforme online, modesta educazione finanziaria
5. *Compromissione di integrità, autenticità' e confidenzialità' della transazione,* attraverso misrepresentation dell'identità

Transazioni non autorizzate

Il legittimo titolare di un conto non autorizza da nessun canale (face to face, voice, digital) un pagamento, la cui esecuzione viene richiesta dal frodatore verso un mule account controllato da quest'ultimo o un intermediario. Il frodatore esterno, tramite ottenimento fraudolento dei dati (ad esempio phishing), impersona un cliente legittimo dell'istituto finanziario impartendo all'operatore istruzioni volte a sottrarre risorse al danneggiato.

Il frodatore interno, in virtu' degli accessi/autorizzazioni derivanti dal ruolo che ricopre, opera sul conto corrente di clienti legittimi individuati per specifiche caratteristiche (anziani, dormant account):

1. Sottraendo risorse dal conto corrente del cliente per godimento personale;
2. Modificando dati sensibili: dati per contatto, codici di sicurezza, beneficiari, soggetti autorizzati ad operare.
3. La collusione tra soggetti può avvenire su diversi livelli:
4. Frodatore esterno minaccia o promette compenso ad un soggetto interno con l'obiettivo di accedere fraudolentemente al conto di un cliente legittimo;
5. Frodatore interno che materialmente esegue le condotte descritte precedente collude con il collega incaricato di svolgere attività di Transaction monitoring accordandosi affinché' l'eventuale alert riferito alla transazione fraudolenta non venga segnalato.

Transazioni autorizzate

Il legittimo titolare di un conto autorizza da qualsiasi canale (face to face, voice, digital) un pagamento verso un mule account [70]a disposizione del frodatore o di un intermediario.

I principali schemi di frode riguardano:

a) Purchase scam: in una transazione commerciale solitamente di importo contenuto, la vittima, attratta su una piattaforma online falsa da forti scontistiche, paga in anticipo un bene/servizio che non riceverà
b) Business e-mail compromise (BEC): il frodatore impersonificata un ruolo apicale dell'azienda e chiede all'addetto ai pagamenti di effettuare un bonifico verso un conto controllato dal frodatore o un intermediario
c) Impersonification scam:

- Il frodatore finge di essere un operatore della banca e convince il cliente a trasferire i fondi dal proprio c/c, giudicato non più sicuro (i.e. Appropriazione indebita in atto) ad un altro controllato dal frodatore o un intermediario;
- Il frodatore finge di essere un ufficiale di polizia ed intima il cliente a pagare una multa fittizia su un c/c da lui o da un intermediario controllato

d) Il mule account è aperto esclusivamente per perpetrare la frode ed ha un'operatività generalmente limitata a circa 90 giorni

Gli schemi di frode nel contesto bancario possono essere messe in atto seguendo due vie differenti:

1) Richiesta fraudolenta di credito
2) Concessione fraudolenta di credito

[70] Possono essere conti creati da criminali che utilizzano identità rubate o sintetiche oppure Conti appartenenti a clienti legittimi che hanno permesso ai criminali di utilizzare il loro conto per motivi illegittimi.

1) Richiesta fraudolenta di credito

È uno schema di frode messo in pratica nella fase di richiesta del finanziamento. I frodatori generalmente sono soggetti esterni, talvolta in collusione con soggetti interni. Le vittime sono istituti finanziari. L' obiettivo è di ottenere l'affidamento e successivamente rendersi irreperibili per evitare di ripagarlo. Il frodatore richiede direttamente il finanziamento o si serve di un prestanome/intermediario. Le somme ottenute attraverso l'affidamento non sono utilizzate per gli scopi dichiarati.

A sua volta la richiesta fraudolenta si sviluppa in:

a) false informazioni sul soggetto

l'obiettivo creazione fraudolenta di un profilo cliente per facilitare l'ottenimento del credito. Le vie intraprese sono: 1) Falsificazione identità: utilizzo di documento contraffatto/ rubato in processo di riconoscimento diretto/ a distanza; 2) Falsificazione documentazione a supporto, anche tramite società create ad hoc: busta paga, contratto di impiego, lettera di facilitazione da parte del datore di lavoro, cariche sociali; 3) Creazione di provviste su c/c coerenti con il profilo cliente che si intende creare.

b) false informazioni sul sottostante. l'obiettivo: creare/ aumentare fraudolentemente il valore del bene oggetto di finanziamento per ottenere un credito superiore poi non rimborsato. Le vie intraprese sono: 1) Richiesta finanziamento per bene inesistente (perizie false); 2) Serie di compravendite fittizie per aumentare il valore del bene; 3) Soggetto che cede bene per cui acquirente chiede il finanziamento non è intitolato a eseguire la compravendita; 4) Dichiarazione di uso del bene finanziato, generalmente immobile, diverso da quello reale; 5) Creazione di fatture attive false per accrescere fraudolentemente l'ammontare dei crediti e rispettare convenant per finanziamenti in essere.

2) Concessione fraudolenta di credito

È uno schema di frode messo in pratica nella fase di richiesta/delibera del finanziamento. I fondatori sono generalmente soggetti interni, talvolta in collusione con soggetti esterni. Le vittime sono clienti e istituti finanziari. L'obiettivo è di concedere un finanziamento ad un soggetto terzo non meritevole/ a condizioni vantaggiose al fine di ottenere un beneficio. A sua volta la concessione fraudolenta si sviluppa in;

a) violazione delle procedure interne

Si intende la falsificazione del processo di onboarding; la mancata/falsa valutazione del razionale della richiesta del cliente; mancata/falsa valutazione del merito creditizio della controparte & la violazione delle deleghe e dei poteri di delibera ed affidamento.

b) operazioni baciate

L'operatore finanziario induce il cliente a sottoscrivere azioni dell'istituto a fronte di agevolazioni sulla concessione di credito. La sottoscrizione delle azioni è condizione vincolante all'erogazione del credito, vera necessità del cliente. L'obiettivo è mostrare al mercato una solidità patrimoniale superiore a quella reale. Generalmente azioni acquistate attraverso le disponibilità ottenute con l'affidamento. Violazione normativa su limiti acquisto azioni proprie. Potenziale connivenza di soggetti apicali dell'istituto finanziario.

Le principali condotte fraudolente in questo ambito riguardano:

Falsificazione di identità: il frodatore, una volta ottenuti fraudolentemente i dati identificativi di un cliente (ad esempio attraverso phishing), si finge quest'ultimo per ottenere il controllo su una carta già esistente, richiederne la riemissione o la modifica dei codici di sicurezza;

Contraffazione dello strumento di pagamento: il frodatore crea fraudolentemente una banda magnetica utilizzando come base una carta legittima (in questo caso il frodatore applica specifici device agli ATM atti a replicare i dati necessari per la successiva esecuzione delle transazioni);

Furto dello strumento di pagamento: il frodatore commette l'azione illecita utilizzando (i) una carta fisica rubata per acquisti presso merchant fisici e prelievi presso ATM o (ii) si appropri fisicamente dei codici dispositivi ad esempio intercettando le comunicazioni tra Banca e cliente.

I principali red flag

I principali comportamenti che risultano segnali di frodi commesse con carte di pagamento riguardano: acquisti svolti su canale fisico in un arco temporale contenuto con controparti localizzate in Stati diversi, richiesta di aggiornamento di credenziali per accesso al conto attraverso canali non tradizionali, discrepanze tra indirizzo di spedizione e fatturazione nei casi di acquisti su canali digitali, tempistica insolita per la consegna della carta all'indirizzo segnalato dal cliente, transazioni di acquisto difformi dal comportamento abituale del cliente in termini di frequenza ed importi delle stesse. Come detto anticipatamente la richiesta & la concessione fraudolenta rappresentano due facce della stessa medaglia. Andiamo ora a prendere in considerazione quelli che sono i principali red flag per atto fraudolento.

Richiesta fraudolenta di credito

- Comportamenti insoliti del cliente in fase di identificazione face to face
- Accesso tramite canale digitale/vocale da nuovi device
- Numerose application per ottenimento finanziamento anche presso istituti finanziari terzi
- Perizia redatta da esperto apparentemente non iscritto a nessun Albo di riferimento
- Informazioni vaghe su motivazioni alla base della richiesta di finanziamento
- Numerose compravendite del bene oggetto di finanziamento in un arco temporale ristretto
- Risultati di crediti a sofferenza da analisi CR

Concessione fraudolenta di credito:

- Analisi del merito creditizio superficiale o assente
- Valutazione delle motivazioni di richiesta finanziamento superficiale o assente
- Pressione sull'operatore/organo dell'istituto atto a deliberare l'affidamento
- Sottoscrizione titoli azionari dell'istituto contestuali alla richiesta di affidamento

<u>Le principali attività di prevention</u>

La prevenzione di frodi con carte di pagamento avviene generalmente attraverso:

1. Tools di machine learning e intelligenza artificiale che, tramite attività di transactions monitoring, identificano, aggiornano e prevedono, tramite data analytics, il comportamento abituale di ogni cliente e le principali controparti. Lo strumento garantisce:

- Una mappatura totale di ogni transazione avvenuta con carte di pagamento emesse dall'istituto finanziario;
- Il risk scoring di ogni transazione suddiviso per strumento di pagamento, importo, localizzazione, tipologia e comportamento della controparte;
- La clusterizzazione, sulla base dell'analisi storica delle transazioni, del comportamento di ciascun cliente e la conseguente identificazione in real time di discrepanze rispetto comportamento atteso;

- L’individuazione di trend e nuovi pattern fraudolenti volti ad implementare la fase di prevention e migliorare la fase di detection;
- L’alimentazione puntuale ed efficiente dello storico dei casi di frode individuati e la creazione di white e black list di clienti e merchant.

2. L’implementazione di sistemi di conferma della transazione da parte del pagatore attraverso solamente device preregistrati;
3. L’introduzione di alert atti ad individuare anomalie comportamentali (richiesta di emissione di una nuova carta e modifica dei codici di sicurezza);
4. L’applicazione di limiti ad ammontare e frequenza di operazioni;
5. La fornitura del servizio di SMS alert per transazioni con carte e prelievi; L’introduzione di metodi semplici e tempestivi per il blocco delle carte e l’invio separato di carte e relativi PIN.

Le principali attività di detection

La detection riguarda un approfondimento sulle transazioni che, a seguito del processo di monitoring, presentano indici di anomalia. L’attività consiste generalmente di: 1) Contatto con il cliente per verificare la legittimità dell’operazione; 2) Individuazione di eventuali IP di accesso usato per effettuare le transazioni (verifica con le aspettative di comportamento del cliente e la lista di device preregistrati), frequenza e geolocalizzazione delle transazioni per delimitare il perimetro della frode; 3) Quantificazione degli importi oggetto di transazioni anomale; 4) Identificazione di ATM e merchant compromessi; 5) Exit dei clienti coinvolti della frode.

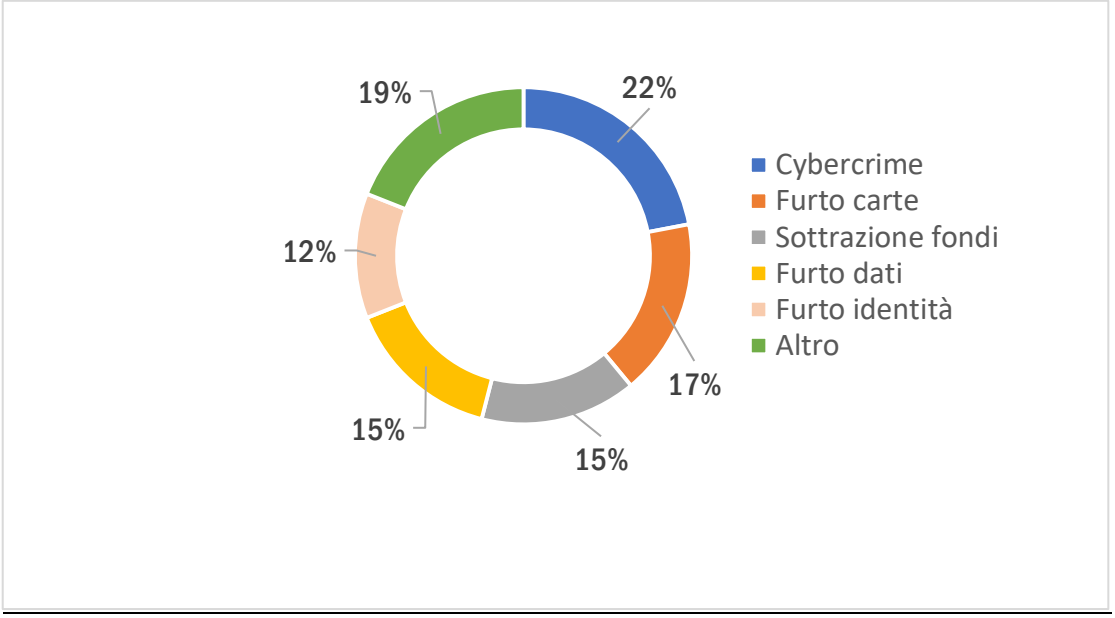
Come emerso dalla sintesi sull’argomento, l’analisi tempestiva e continua di una mole ingente di transazioni attraverso sistemi di machine learning e intelligenza artificiale rappresenta il sistema di contrasto alle frodi su carte attualmente più efficace ed efficiente. L’implementazione di tale processo infatti permette l’individuazione in real time di anomalie a cui dar seguito con un’investigation puntuale per confermare o meno l’avvenuta frode o il tentativo di commissione della stessa. La tempestività

nel processo descritto assume una valenza significativa in quanto, ove possibile, la conferma dell'avvenimento dell'illecito all'interno del lag temporale tra effettuazione della transazione con carta e disponibilità delle relative somme per il beneficiario, inibisce a monte il frodatore dal poter ricevere i proventi oggetto della condotta fraudolenta. Tale processo pertanto riduce i costi e massimizza il risultato della recovery rispetto ad alternative come il tentativo di chargeback o lo svolgimento di indagini successive di varia natura, incluso il coinvolgimento di Autorità esterne.[71]

Le frodi nel contesto bancario & Alcuni numeri

Tenendo fede da quanto dichiarato dalle fonti nel 2017/2018 riconosciamo in queste percentuali lo sviluppo dei canali usati per frodi su carte di pagamento & i maggiori rischi percepiti dagli Intermediari finanziari.

Tab. 4.1.1 Maggiori rischi percepiti dagli Intermediari Finanziari[72]

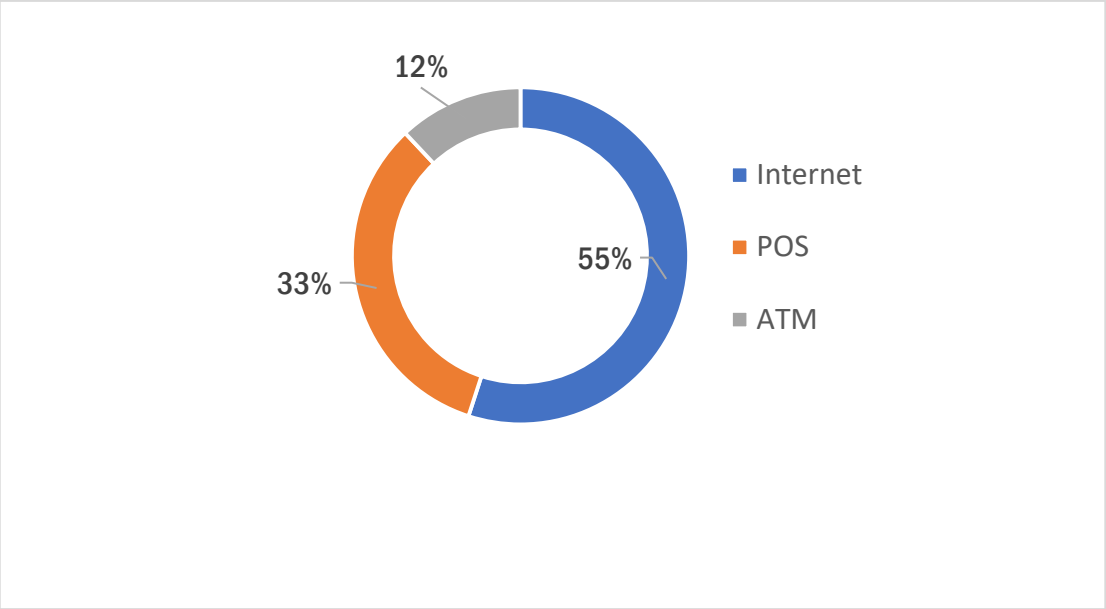


[71] *Le frodi commesse attraverso carte di pagamento*-Andrea D'Andrea - Associate Partner e Stefano Mango - Senior Consultant | EY Forensics – FSO

[72] Fonte: Osservatorio Crif, dicembre 2018.

Dall'analisi del grafico possiamo notare come il cybercrime viene percepito dagli intermediari finanziari come lo scompartimento del settore bancario più sensibile con una percentuale del 22%. Trova ultimo posto il furto di identità con un valore pari al 12%.

Tab. 4.1.2 Canali frodi su carte di pagamento[73]



Dall'analisi del grafico possiamo notare lo strumento di transizione di maggiore rischio è quello informatico con un rischio pari al 55% dei mezzi di transazione bancari. Viene percepito come il meno rischioso il pagamento tramite l'utilizzo degli ATM, rappresentanti uno degli ultimi strumenti di transazione fisico. Da una analisi congiunta dei due grafici emerge come cybercrime ed internet possono rappresentare territori fertili per il perseguirsi di frodi bancarie.

[73] Fonte: MEF, Rapporto statistico sulle frodi con carte di pagamento no. 7/2017, 2017.

4.2 Frodi assicurative

Per "*Frode assicurativa*[74]" si intende qualsiasi comportamento intenzionale posto in essere con l'inganno e in generale disonestamente da uno o più soggetti con l'obiettivo di ottenere un vantaggio personale o di terzi, causando un danno diretto o indiretto alla compagnia assicuratrice, un agente o broker o un cliente. La frode può avvenire in tutte le fasi tra la sottoscrizione della polizza ed il pagamento dell'indennizzo.

Come detto nel *Primo Capitolo* gli atti fraudolenti si caratterizzano per la presenza di uno schema comportamentale di base condiviso per tipologia di frode. Nel caso delle frodi assicurative ritroviamo:

- Il Frodatore: è il soggetto attivo nella frode, il quale usa strumenti come; Sottoscrittori di polizze Detentori di polizze; Terze parti reclamanti; Collaboratori dell'assicurazione; Professionisti a servizio di reclamanti.
- L'inganno: sono le azioni intraprese dall'attore per raggirare la vittima. Possono essere:

1. *Hard fraud*: evento sfavorevole non accaduto;
2. *Soft fraud*: evento sfavorevole accaduto ad un'intensità minore di quella dichiarata

- La vittima: è l'assicurazione che subisce la frode.
- Il danno patrimoniale[75]: Lesione di un interesse patrimoniale, consistente sia in una diminuzione del patrimonio (c.d. danno emergente) e sia nel mancato guadagno determinato dal fatto dannoso (c.d. lucro cessante).

[74] Assicurazioni.Blog
[75]._Broccardi

La frode assicurativa: norme e regolamenti

- *Art. 642 c.p.*

  Fraudolento danneggiamento dei beni assicurati e mutilazione fraudolenta della propria persona: "Chiunque, al fine di conseguire per sé o per altri l'indennizzo di una assicurazione, distrugge, disperde, deteriora od occulta cose di sua proprietà, falsifica o altera una polizza o la documentazione richiesta per la stipulazione di un contratto di assicurazione è punito con la reclusione da uno a cinque anni. Alla stessa pena soggiace chi al fine predetto cagiona a sé stesso una lesione personale o aggrava le conseguenze della lesione personale prodotta da un infortunio o denuncia un sinistro non accaduto ovvero distrugge, falsifica, altera o precostituisce elementi di prova o documentazione relativi al sinistro".[76]

Riferimenti IVASS [77]

i. *Banche dati (Regolamento n. 23 del 1° giugno 2016)*

   Regolamento recante la disciplina della banca dati sinistri, della banca dati anagrafe testimoni e della banca dati anagrafe danneggiati.[78]

ii. *Referente antifrode (Lettera al mercato del 21 maggio 2014)*

   Nomina da parte delle imprese di assicurazione di un referente per l'attività antifrode.[79] In merito alle funzioni del referente antifrode la disposizione emanata dall'IVASS specifica tre mansioni principali; nell'ordine: 1) attività antifrode; 2) adempimenti riconducibili all'Archivio Informatico Integrato (AII); 3) attività di collegamento, coordinamento e collaborazione con gli organi di Polizia Giudiziaria.

[76] Art. 642 c.p.
[77] L'Istituto per la vigilanza sulle assicurazioni (noto con l'acronimo IVASS) è un'autorità amministrativa indipendente che esercita la vigilanza sul mercato assicurativo italiano, per garantirne la stabilità e tutelare il consumatore.
[78] i. Banche dati (Regolamento n. 23 del 1° giugno 2016)
[79] ii. Referente antifrode (Lettera al mercato del 21 maggio 2014)

Entrando, seppur sinteticamente, nel merito delle competenze richieste al RAF, si comprende subito che la disposizione dell'IVASS prevede un insieme di compiti vastissimo che il referente, con molta probabilità, dovrà gestire mediante un proprio team di esperti appositamente formato e dedicato.

iii. Indicatori e livelli di anomalia (Provvedimento n. 47 del 1° giugno 2016)

Definisce gli indicatori analitici ed i relativi parametri, le soglie dell'indicatore di anomalia di sintesi, i livelli di anomalia oltre i quali gli indicatori sono comunicati alle imprese di assicurazione coinvolte nel sinistro.[80] L'indicatore di anomalia di sintesi sul sinistro è costituito dalla somma dei pesi di ciascuno degli indicatori di anomalia analitici [81]attivati. Il valore dell'indicatore di sintesi [82]così determinato è classificato, in ottica antifrode, nullo, basso, medio e alto.

Gli indicatori analitici e i relativi parametri, nonché' le soglie dell'indicatore di anomalia di sintesi per la classificazione del sinistro sono determinati con provvedimento dell'IVASS.

Gli indicatori analitici sono calcolati avendo quale riferimento temporale la data di accadimento dell'evento. Ad ogni indicatore analitico è associato uno specifico punteggio, denominato anche score, che varia in funzione della rilevanza, in ottica antifrode, dell'indicatore stesso.

[80] iii. Indicatori e livelli di anomalia (Provvedimento n. 47 del 1° giugno 2016)

[81] Sulla base di ricorrenze e verifiche di veridicità e coerenza dei dati relativi ai sinistri, forniscono elementi per l'analisi antifrode dei sinistri

[82] Il punteggio di ciascuno dei 4 gruppi di indicatori di cui all'art. 6 (a. veicoli direttamente coinvolti nel sinistro;
b. soggetti direttamente coinvolti nel sinistro; c. altri soggetti interessati nel sinistro; d. altri aspetti inerenti al sinistro.) è ottenuto come somma degli score dei singoli indicatori analitici attivati in ciascuna area di analisi; la somma degli score dei 4 gruppi determina il valore dell'indicatore di sintesi, valore che compendia il livello di anomalia dell'evento esaminato.

I principali fattori di rischio dell'*Industry*

i. *Intermediazione*

Terze parti coinvolte nella fase di sottoscrizione contrattuale aumentano il rischio di perdita di controllo, trasparenza, adozione di standard qualitativi comuni

ii. *Asimmetria informativa*

Le parti nelle diverse fasi di vita della polizza tendono a non condividere informazioni che pregiudicherebbero il proprio interesse

iii. *Moral Hazard*

Dopo aver contratto le polizze, gli assicurati tendono a modificare il loro comportamento riducendo la prudenza.

iv. *Adverse selection*

Soggetti più esposti a eventi sfavorevoli tendono maggiormente ad assicurarsi rispetto a soggetti meno rischiosi.

v. *Elevata liquidità*

Il rischio di appropriazione indebita è favorito dalla raccolta del premio attraverso contante o strumenti di pagamento di esigibilità equivalente

vi. *Competitività del mercato*

Prodotti non molto differenziabili favoriscono: politiche aggressive di prezzo per ottenere clienti; comportamenti opportunistici della clientela

vii. *Nuovi canali di vendita*

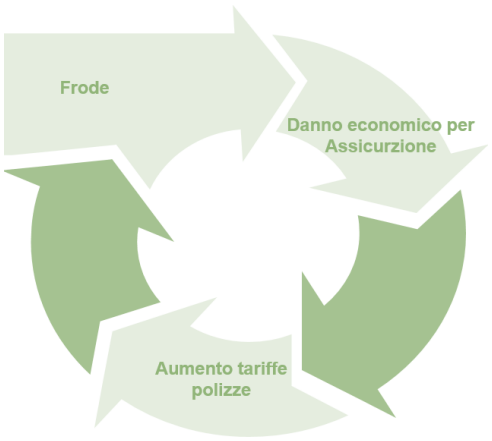
Contratti vocali e vendite online rendono più critico il monitoraggio della fase di sottoscrizione della polizza.

viii. *Frazionamento del rischio*

Antieconomicità della detection quando il rischio è di importo contenuto e stratificato su più clienti.

Come detto precedentemente riconosciamo nell'intermediazione il fattore di maggiore vulnerabilità all'interno del processo di stipula e sviluppo di una polizza assicurativa [83]di qualsivoglia tipologia.

Tab. 4.2.1 Le frodi assicurative & circolo vizioso



1. La frode nel business delle assicurazione alimenta un circolo vizioso.
2. L'evento fraudolento provoca una perdita economica per l'assicurazione che risponde attraverso un aumento delle tariffe delle polizze.
3. Dall'aumento del premio derivano un aumento della liquidità disponibile e del possibile indennizzo, fattori che rendono più probabile l'accadimento di un ulteriore caso di frode.

[83] Nel moderno gergo delle assicurazioni, la polizza è la parola che si usa per designare il contratto di assicurazione in quanto tale, quello mediante il quale l'assicuratore, previa la riscossione di un premio, si impegna a rivalere l'assicurato di un danno, qualora si verificasse, mediante il pagamento di un capitale o di una rendita_ articolo 1882 del Codice Civile

[…] I costi dei premi assicurativi sono troppo alti a causa delle attività speculative, ma è un circolo vizioso: si froda perché si ritiene elevato il costo dei premi assicurativi, si alzano i costi dei premi assicurativi perché si froda. Il truffatore ritiene di arrecare un danno alla compagnia assicurativa e non alla collettività, eppure per pagare tale frode la compagnia assicurativa attinge da un fondo rischi che tutti gli assicurati rimpinguano pagando le polizze […][84]

Sono queste le Parole usate da Riccardo Vizzino[85] ad un'intervista stesa negli ultimi mesi del 2019 per definire il concetto di "circolo vizioso" che nasce eseguendo frodi assicurative.

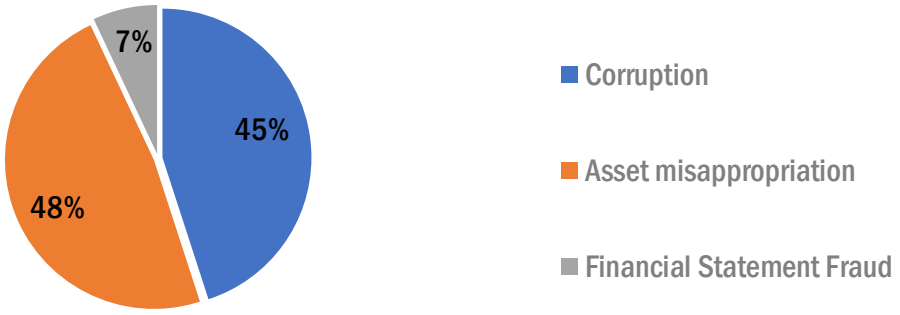
I fenomeni fraudolenti sono un problema internazionale che grava sulla società in diversi modi. Innanzitutto, le truffe hanno un costo che viene ripartito su tutti i cittadini, danneggiando chi vive ogni giorno di sacrifici e lavoro. La crisi economica degli ultimi anni ha contribuito ad aumentare tali attività illecite. Si è notato, infatti, che sono sempre di più le persone che in modo occasionale commettono reati contro il patrimonio a volte anche per indennizzi di piccolo ammontare. Segno della recessione e della disoccupazione, di questo periodo di estrema difficoltà. Si ritiene che la truffa sia una sorta di rivalsa per il mancato impiego, sia un guadagno "dovuto", un onere che lo Stato deve pagare per non aver provveduto al benessere di tutti.

<u>Le frodi assicurative & Alcuni numeri</u>

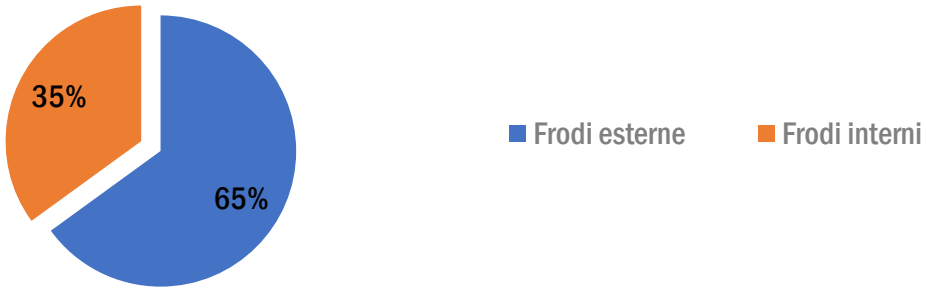
Tenendo fede da quanto dichiarato da ACFE nel 2019 riconosciamo in queste percentuali lo sviluppo del trinomio *corruption; asset misappropriation e financial statement fraud* in tema di frodi assicurative.

[84] https://www.ildenaro.it/frodi-assicurative-perche-sono-un-danno-per-tutta-la-collettivita/
[85] Avvocato a Napoli

Tab. 4.2.2. Albero frodi - Assicurazioni



Tab 4.2.3. Frodi esterni vs frodi interne – Assicurazioni



Tab 4.2.4. Tipologia frodi - assicurazioni

La frode più diffusa in ambito assicurativo è l'appropriazione indebita [86](48% dei casi). Generalmente è compiuta da soggetti esterni (65% dei casi) e riguarda il ramo danni [87]– RC auto (70% dei casi). Integra il reato di appropriazione indebita (art. 646 c.p.) la condotta dell'assicurato che ometta di comunicare tempestivamente il ritrovamento del veicolo rubato alla compagnia assicuratrice, che abbia già effettuato la liquidazione del danno in suo favore, considerato che in virtù del contratto di assicurazione quest'ultima acquista la proprietà dell'autoveicolo, con la conseguenza che l'assicurato deve comunicare tempestivamente il ritrovamento dell'autoveicolo e metterlo a disposizione della compagnia assicuratrice, non sussistendo invece alcuna cooperazione artificiosa della vittima né la perdita definitiva del bene da parte della società assicuratrice, necessari per l'integrazione del reato di truffa (art. 640 c.p.).[88]

Ivass, l'Istituto per la vigilanza sulle assicurazioni, evidenzia quanto la criminalità pesi sulle tasche delle famiglie. L'assicurazione RC Auto in Italia risente infatti dell'alto tasso di criminalità sulle strade in Italia, dove si paga 100 euro in più rispetto al resto d'Europa. Il divario è comunque calato perché fino a pochi anni fa era di 200 euro. Lo rilevano i dati dell'ultimo rapporto Ivass ripresi ed elaborati dal Corriere della Sera ed è l'effetto del ricarico imposto dalle compagnie assicurative per difendersi dalle molte truffe. Con 42,1 milioni di veicoli assicurati il conto aggiuntivo per l'Italia è di 4,2 miliardi: un carico che mina la nostra competitività. Il 46% di questi 100 euro sembra essere dovuto anche al fatto che abbiamo un numero più elevato di sinistri, strade in condizioni non sempre ottimali e risarcimenti più generosi in caso di vittime. Il restante 54% è meno spiegabile e pesa indirettamente sui contribuenti, poiché frodi e truffe devono essere gestite dall'apparato giudiziario statale.[89]

[86] L'appropriazione indebita, secondo l'art. 646 del codice penale, si ha quando qualcuno si appropria del denaro o di una cosa mobile di un'altra persona, procurandosi di conseguenza un ingiusto profitto. Come nel furto, si ha il reato appena descritto quando il vantaggio è esclusivamente patrimoniale. L'appropriazione si ha ogni volta che il soggetto tratta la cosa altrui come fosse propria.

[87] Le polizze del "ramo danni" tutelano l'assicurato da eventi che possono danneggiare singoli beni del suo patrimonio (ad esempio la casa o l'auto), le sue possibilità di guadagno, il patrimonio nel suo complesso o la sua persona.

[88] https://www.laleggepertutti.it/280344_truffa-e-assicurazione-ultime-sentenze

[89] https://www.assiteca.it/2020/03/rc-auto-frodi-sinistri/

Schemi di frodi assicurative

Principali schemi di frode assicurativa

I principali schemi di frode assicurative si suddividono in 5 tipologie differenti:

1. Frodi perpetrate da Agenti/Brokers:
2. Sottoscrizioni fraudolente
3. Schemi r.c.a.
4. Schemi assicurazione su beni
5. Schemi assicurazione vita/infortuni

Tab.4.2.5 I principali schemi di frode assicurative si suddividono in 5 tipologie differenti

Frodi perpetrate da Agenti/Brokers	Sottoscrizioni fraudolente	Schemi r.c.a	Schemi assicurazione su beni	Schemi assicurazione/infortuni
1)Incasso fraudolento dell'indennizzo	1)False rappresentazione assicurazione-cliente	1)Post posting	1)Richiesta rimborso per beni inesistenti	1)Falsa dichiarazione di decesso
2)Incasso fraudolento del premio	2)Falsa rappresentazione cliente-assicurazione	2)Sopravvalutazione danni	2)Sopravvalutazione danni	2)Prestazioni sanitarie fraudolente
3)Polizze fittizie	3) Polizze fittizie	3)Inscenare/indurre un incidente		3)Inscenare un incidente
	4)Twisting			

Frodi perpetrate da Agenti/Brokers

- *Incasso fraudolento dell'indennizzo*

  In caso di sinistro, un agente/broker richiede un pagamento alla compagnia assicurativa per conto dell'assicurato, senza che quest'ultimo ne sia a conoscenza. Successivamente deposita la somma ottenuta in un conto deposito a suo nome o, più comunemente, intestato ad un prestanome. Per minimizzare la probabilità di essere scoperto, il frodatore può modificare le informazioni (c/c, indirizzo ecc.) relative al soggetto per conto del quale si richiede il rimborso, per poi ristabilirle alla conclusione del piano fraudolento.

- *Incasso fraudolento del premio*

  Un agente/broker incassa il premio ma non rimette l'assegno alla compagnia assicurativa.

- *Polizze fittizie*

  Un agente/broker sottoscrive finte polizze al fine di migliorare la sua performance ed ottenere un illecito guadagno.

Sottoscrizioni fraudolente

- *Falsa rappresentazione da assicurazione a cliente*

  Si configura una falsa dichiarazione quando un assicuratore, fornisce consapevolmente una falsa informativa sui termini della polizza con l'intento di farla sottoscrivere ad un cliente. L'obiettivo è indurre fraudolentemente il cliente a sottoscrivere una polizza, ottenendo un guadagno illecito, senza che questo conosca realmente i dettagli.

Di cui:

Sliding: l'assicuratore, a danno del cliente, include nella polizza clausole aggiuntive sconosciute all'assicurato che stabiliscono costi aggiuntivi ricaricati sul premio. Churning: l'assicuratore riferisce ingannevolmente al cliente, cagionandogli un danno, di poter acquistare un'assicurazione aggiuntiva a costo zero. In fase di sottoscrizione invece il costo della polizza aggiuntiva si riflette sul premio da corrispondere.

- *Falsa rappresentazione da cliente a assicurazione*

  Il cliente fornisce alla compagnia assicuratrice, cagionandole un danno, informazioni false per ottenere condizioni vantaggiose tra cui: i) False Informazioni mediche; ii) Falsa data di nascita; iii) Falso indirizzo di residenza per ottenere un premio più conveniente per la casa o l'assicurazione automobilistica; iv) Falsa "storia" assicurativa dell'individuo. La condotta può essere perpetrata anche attraverso una collusione tra cliente e broker/agente.
- *Polizze fittizie*

  Un terzo fa sottoscrivere al cliente, cagionandogli un danno, finte polizze al fine di appropriarsi del premio.
- *Twisting*

  L'assicuratore, con o senza il benestare del cliente, lo forza a rimpiazzare una vecchia polizza con una nuova garantendosi un guadagno maggiore per la sottoscrizione di nuove polizze.

Schemi r.c.a.

- *Past posting*

  Il past posting è uno schema in cui una persona viene coinvolta in un incidente automobilistico, ma non ha un'assicurazione. Dopo l'incidente, la persona ottiene l'assicurazione, attende un breve periodo di tempo e segnala che il veicolo è stato coinvolto in un incidente, ottenendo così il rimborso danni.

- *Sopravvalutazione danni*

  Lo schema prevede una sovrastima dell'entità di un danno occorso. Può verificarsi quando per una riparazione vengono utilizzati pezzi usati ma viene richiesto un rimborso per pezzi nuovi e può coinvolgere un perito assicurativo colluso.

- *Inscenare/indurre un incidente*

  Questo schema comporta un incidente automobilistico in realtà mai avvenuto o inscenato. Ciò avviene perché i costi di riparazione sono ridotti e molte compagnie di assicurazione non si preoccupano di inviare un investigatore per esaminare il veicolo.

Schemi assicurazione su beni

- *Richiesta rimborso per beni inesistenti*

  Si verifica ad esempio quando, a seguito di un incendio, viene stilato l'inventario dei beni andati perduti inserendo beni non esistenti.

  Oppure nel caso in cui venisse presentato un reclamo per una barca affondata, in realtà mai esistita. Il frodatore potrebbe aver in precedenza registrato una barca esibendo una falsa fattura di vendita e, successivamente, richiesto un rimborso per l'affondamento della stessa.

- *Sopravvalutazione danni*

  Sovrastimare, a danno dell'assicurazione, l'entità di un danno occorso o il valore dei beni distrutti/rubati.

Schemi assicurazione vita/infortuni

- *Falsa dichiarazione di decesso*

  Produrre o alterare, a danno dell'assicurazione, un certificato di decesso falso. In questi casi l'assicurato potrebbe essere vivo ma nascosto/disperso, o potrebbe essere morto in una data non coincidente con quella riportata nel certificato. Le richieste di rimborso a seguito di decesso vengono controllate meno rigidamente rispetto ad altri reclami.

- *Prestazioni sanitarie fraudolente*

  Dalla documentazione a supporto della somministrazione di cure mediche, risulta che le procedure sono state fraudolentemente frazionate a danno dell'assicurazione con l'obiettivo di aumentare l'onorario e quindi l'indennizzo. L'assicurato presenta, a danno dell'assicurazione, fatture e documentazione a supporto per prestazioni sanitarie: effettivamente non erogate; non necessarie.

- *Inscenare/indurre un incidente*

  Questo schema comporta la rappresentazione di un incidente in realtà mai avvenuto con l'obiettivo di ottenere fraudolentemente un indennizzo a danno della compagnia assicuratrice.

<u>Fase di Prevention</u>

La fase preventiva ha inizio con l'attività di background search. consiste in verifiche su terze parti riguardo criminal records, partecipazioni e cariche detenute in altre società, eventi negativi e solidità finanziaria. L'obiettivo consiste nella riduzione del rischio che la collaborazione con terze parti cagioni un danno alla società in termini reputazionali, anche con specifico riferimento a frodi. La selezione della controparte non può avvenire attraverso esclusivamente criteri di business. Successivamente si procede con la Reputational Search; divisa a sua volta in tre livelli.

- *Primo livello:*

1. Informazioni generali: dati anagrafici identificativi
2. Informazioni di compliance: sanzioni comminate a soggetti target attraverso verifiche su specifiche database
3. Informazioni reputazionali: notizie di adverse press su quotidiani, motori di ricerca
4. Informazioni legali: indagini e procedimenti a carico di soggetti target

Secondo livello:

1. Approfondimenti economico-finanziari e di *governance*: ricostruzione di intera catena proprietaria, se persone giuridiche, o di cariche ricoperte e partecipazioni detenute, se persone fisiche
2. Esami di fonti locali: ove applicabile, analisi descritte svolte su database locali nel caso in cui la terza parte sia estera

Terzo livello:

1. Ispezioni: verifiche in loco di procedure ed attività di soggetti *target*
2. Interviste: colloqui con soggetti *target*, anche attraverso somministrazione di questionari per omogenizzare l'approccio, per valutare competenza ed aderenza a principi modello 231

Fase di Detection

Gli obiettivi di questa fase consistono nel: individuare il potenziale/i attore/i; rilevare il luogo fisico dell'accadimento, i principali soggetti/funzioni coinvolti, i processi interessati; comprendere le motivazioni sottostanti; definire il periodo temporale degli eventi e degli effetti degli stessi; ricostruire gli eventi, comprendere le modalità (lo schema in caso di frode) e definire le eventuali responsabilità ed il potenziale danno. Le principali attività svolte in questa fase sono: Analisi delle transazioni a rischio frode Svolgimento di due diligence per individuare interessenze tra i soggetti potenzialmente coinvolti; Effettuazione di interviste ai soggetti potenzialmente coinvolti; Review di documentazione e comunicazioni riguardanti operazioni a rischio frode. Nella fase di Detection in campo assicurativo vengono poste in essere attività speciali in tema di:

1. *banche dati*: garantiscono la consultazione di informazioni in tempo reale; confronto dati tra fonti diversi per valutare la congruenza delle informazioni. Consentono verifiche approfondite e puntuali ed individuazione di anomalie ricorrenti.

2. *perizie accurate*: utilizzo di professionisti qualificati; distinzione tra danno intenzionale e fortuito;

3. *condivisione delle informazioni*: funzioni interne; compagnie assicurative; procure.

4. *adozione di tool di investigation:* diviso a sua volta in;

- Predictive tool: aggregazione su base storica di dati da diverse fonti (polizze, sinistri, anagrafiche); analisi statistica svolta in fase di apertura sinistro; individuale di probabilità che un sinistro sia fraudolenti.
- Investigative tool: ricostruzione relazioni tra soggetti coinvolti nel sinistro; geolocalizzazione mediante visualizzazione di mappa geografica; repository storico di indagini svolte.

4.3 Frodi informatiche

"...quelle cose che prima non mostrano li loro difetti sono più pericolose, però che di loro molte fiate prendere guardia non si può; sì come vedemo nel traditore, che né la faccia dinanzi si mostra amico, sì che fa di sé fede avere, e sotto pretesto d'amistade chiude il difetto de la inimistade" [90]

L'Information and Communication Technology è una componente imprescindibile delle attività quotidiane di ogni organizzazione strutturata, pertanto l'integrazione sempre più spinta dei processi aziendali con gli strumenti tecnologici introduce nuovi rischi significativi di cui è essenziale tenere conto, ovvero quelli relativi alle frodi di cui questo documento si occupa.

Il concetto di "frode ICT" - denominata anche, "computer fraud" o "technology fraud" - è complesso: fonti diverse ne danno definizioni parzialmente differenti, in funzione degli obiettivi specifici che perseguono o del contesto specifico a cui si riferiscono, come ad esempio:

- "qualsiasi falsificazione o appropriazione indebita compiuta attraverso la manomissione o l'uso malevolo di programmi informativi, file di dati, operazioni, attrezzature o mezzi di comunicazione, che comporti perdite all'organizzazione i cui i sistemi informativi sono stati violati, anche mediate 'assenza o l'abuso delle autorizzazione necessarie, con l'intenzione di commettere un atto fraudolento"[91]
- "l'immissione, l'alterazione, la cancellazione o la soppressione di dati o programmi informatici, o altre interferenze con il corretto trattamento dei dati, che influenzino il risultato della elaborazione causando perdite economiche [...] con l'intento di procurare un ingiusto profitto per sé o per un'altra persona" [92]

Definire con precisione il concetto di frode ICT consente inoltre di distinguerlo da altre tipologie di reato e di predisporre strategie di contrasto mirate, evitando così di incorrere nell'errore di identificare la frode ICT con qualsiasi atto criminale perpetrato utilizzando sistemi o servizi informatici.

[90] (Dante, Convivio, IV, XII, 3)
[91] Frauds_anatomy_Anatomia_della_frode
[92] Ministero della difesa_ LA CRIMINALITÀ INFORMATICA TRA IMPRESA, NUOVE TECNOLOGIE E CULTURA DIGITALICA

Spesso vengono associati tra loro, impropriamente, fenomeni assai diversi quali, a titolo di esempio: phishing, social engineering, furto di identità digitale, virus, hacking, mailbombing, spamming, contraffazione e dirottamento di nome di dominio, violazione di server, denial of service, distruzione o furto di dati, intercettazioni elettroniche.

Phishing

Il phishing è un tipo di truffa effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale.[93]

Il termine phishing è una variante di fishing, probabilmente influenzato da phreakinge [94]allude all'uso di tecniche sempre più sofisticate per "pescare" dati finanziari e password di un utente. La teoria popolare è che si tratti di un portmanteau di password harvesting, è un esempio di pseudoetimologica.

Si tratta di un'attività illegale che sfrutta una tecnica di ingegneria sociale: il malintenzionato effettua un invio massivo di messaggi che imitano, nell'aspetto e nel contenuto, messaggi legittimi di fornitori di servizi; tali messaggi fraudolenti richiedono di fornire informazioni riservate come, ad esempio, il numero della carta di credito o la password per accedere ad un determinato servizio.

Per la maggior parte è una truffa perpetrata usando messaggi di posta elettronica, ma non mancano casi simili che sfruttano altri mezzi, quali i messaggi SMS. Secondo un'indagine realizzata nel 2019, solo il 17,93 per cento degli intervistati sarebbe in grado di identificare tutti i diversi tipi di phishing (tra cui e-mail o sms contenenti link malevoli o siti web che replicano delle pagine legittime).[95]

[93] Ramzan, Zulfikar, Phishing attacks and countermeasures, in Stamp, Mark & Stavroulakis, Peter (a cura di), Handbook of Information and Communication Security, Springer, 2010, ISBN 978-3-642-04117-4.

[94] Phreakinge è un termine gergale inglese che indica l'attività di chi studia, sperimenta o sfrutta i telefoni, le compagnie e i sistemi telefonici per divertimento, vantaggio personale o curiosità, ricercando falle all'interno della tecnologia che permettano usi non previsti dal sistema.

[95] Phishing e cifratura: tra i buoni propositi per il 2020 mettiamo anche la sicurezza informatica, su lastampa.it.

Il social engineering è una tecnica di attacco cyber sempre più sofisticata, in grado di colpire direttamente i dipendenti di un azienda. La dizione italiana "ingegneria sociale" lascia ben intendere la natura di questa minaccia sempre più diffusa alla sicurezza informatica delle aziende: si tratta di un'arte, ancora prima che una scienza, che consiste nel manipolare le persone toccando leve psicologiche e comportamentali. Rispetto alle altre modalità di cybercrime, questa pratica si differenzia per una particolarità: il social engineering non sfrutta le falle dei sistemi informatici, bensì la debolezza e l'ingenuità delle persone.[96]

Il social engineering (o ingegneria sociale) è una tecnica di attacco cyber basata sullo studio del comportamento delle persone col fine di manipolarle e carpire informazioni confidenziali. Il procedimento si basa sulla psicologia umana e sfrutta la fiducia, la mancanza di conoscenza e, in generale, le vulnerabilità della vittima per ottenere dati confidenziali (password, informazioni su conti correnti, informazioni finanziarie), estorcere denaro o persino rubarne l'identità.[97]

Tema di stretta correlazione all'ingegneria sociale è quello che concerne il data breach *(violazione dei dati).* Una violazione dei dati è un incidente in cui le informazioni vengono rubate o sottratte da un sistema senza la conoscenza o l'autorizzazione del proprietario del sistema. Una piccola azienda o una grande organizzazione può subire una violazione dei dati. I dati rubati possono riguardare informazioni sensibili, proprietarie o riservate come numeri di carta di credito, dati dei clienti, segreti commerciali o questioni di sicurezza nazionale. Gli effetti derivanti da una violazione dei dati possono consistere in un danno alla reputazione della società target a causa di un percepito "tradimento della fiducia". Le vittime e i loro clienti possono anche subire perdite finanziarie nel caso in cui i relativi dati siano parte delle informazioni rubate.[98]

[96] Osservatori.net
[97] Osservatori.net
[98] Trend Micro.com

Tab.4.3.1. Metodologia generale di attacco/schema di attacco

Il processo standard delle metodologie di attacco di phishing può riassumersi nelle seguenti fasi:

1. l'utente malintenzionato (phisher) spedisce a un utente un messaggio e-mail che simula, nella grafica e nel contenuto, quello di una istituzione nota al destinatario (per esempio la sua banca, il suo provider web, un sito di aste online a cui è iscritto).

2. l'e-mail contiene quasi sempre avvisi di particolari situazioni o problemi verificatesi con il proprio conto corrente/account (ad esempio un addebito enorme, la scadenza dell'account, ecc.) oppure un'offerta di denaro.

3. l'e-mail invita il destinatario a seguire un link, presente nel messaggio, per evitare l'addebito e/o per regolarizzare la sua posizione con l'ente o la società di cui il messaggio simula la grafica e l'impostazione (Fake login).

4. il link fornito, tuttavia, non porta in realtà al sito web ufficiale, ma a una copia fittizia apparentemente simile al sito ufficiale, situata su un server controllato dal phisher, allo scopo di richiedere e ottenere dal destinatario dati personali particolari, normalmente con la scusa di una conferma o la necessità di effettuare una autenticazione al sistema; queste informazioni vengono memorizzate dal server gestito dal phisher e quindi finiscono nelle mani del malintenzionato.

5. il phisher utilizza questi dati per acquistare beni, trasferire somme di denaro o anche solo come "ponte" per ulteriori attacchi. Talora, l'e-mail contiene l'invito a cogliere una nuova "opportunità di lavoro" (quale operatore finanziario o financial manager), consistente nel fornire le coordinate bancarie del proprio conto online per ricevere l'accredito di somme che vanno poi ri-trasferite all'estero tramite sistemi di money trasfert (Western Union o Money Gram), trattenendo una percentuale dell'importo, che può arrivare a cifre molto alte. In realtà si tratta del denaro rubato con il phishing, per il quale il titolare del conto online beneficiario, spesso in buona fede, commette il reato di riciclaggio di denaro sporco. Quest'attività comporta per il phisher la perdita di una certa percentuale di quanto è riuscito a sottrarre, ma esiste comunque un interesse a disperdere il denaro sottratto in molti conti correnti e a fare ritrasferenti in differenti Paesi, perché così diviene più difficile risalire alla identità del criminale informatico e ricostruire compiutamente il meccanismo illecito. Peraltro, se i trasferimenti coinvolgono più Paesi, i tempi per la ricostruzione dei movimenti bancari si allungano, poiché spesso serve una rogatoria e l'apertura di un procedimento presso la magistratura locale di ogni Paese interessato[99].

[99] F. Cajani, G. Costabile, G. Mazzaraco, Phishing e furto d'identita digitale. Indagini informatiche e sicurezza bancaria, Milano, Giuffrè, 2008.

Tipologie di phishing:

1) *Spear phishing*

   Un attacco mirato verso un individuo o una compagnia è stato denominato spear phishing. Gli attaccanti potrebbero cercare informazioni sull'obbiettivo per poter incrementare le probabilità di successo. Questa tecnica è, alla lunga, la più diffusa su internet, con una quota del 91% degli attacchi.[100]

2) *Clone phishing*

   È un tipo di phishing in cui una mail legittima viene modificata negli allegati o nei link e rimandata ai riceventi, dichiarando di essere una versione aggiornata. Le parti modificate della mail sono volte a ingannare il ricevente. Questo attacco sfrutta la fiducia che si ha nel riconoscere una mail precedentemente ricevuta.

3) *Whaling*

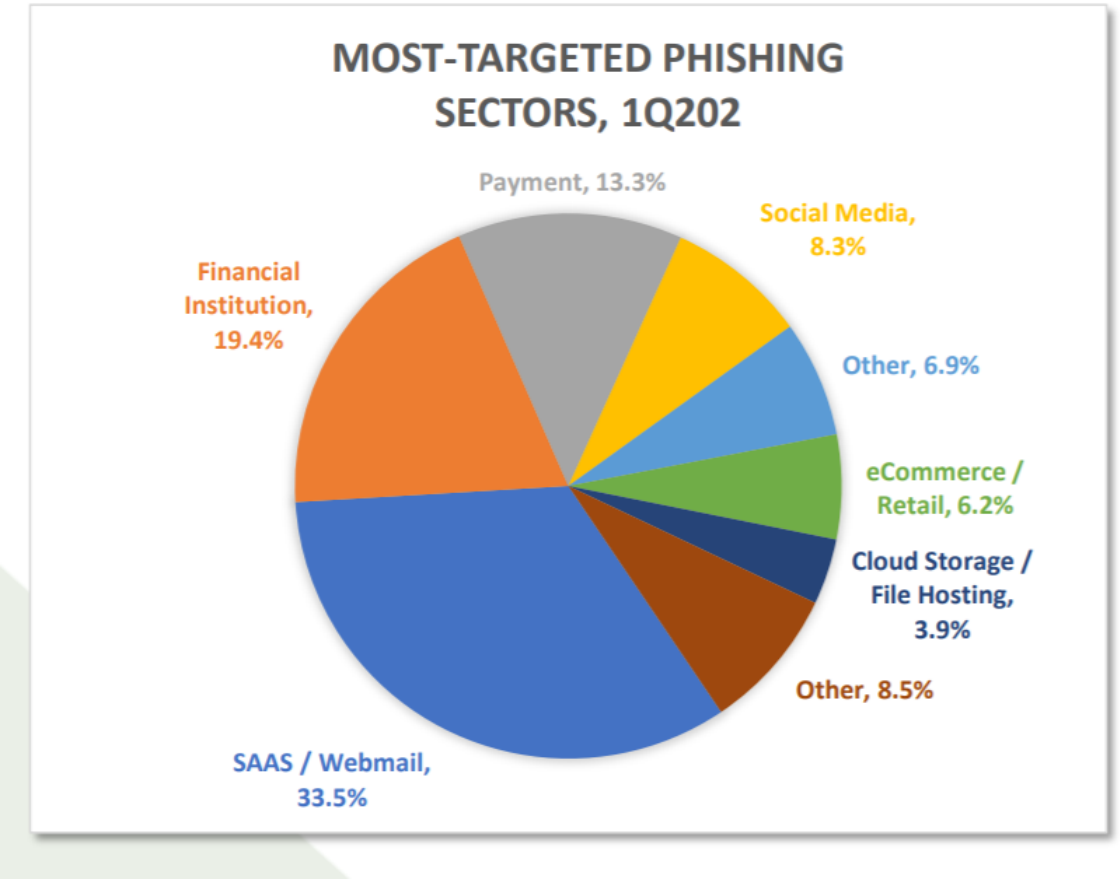
   Di recente molti attacchi di phishing sono stati indirizzati verso figure di spicco di aziende o enti e il termine whaling [101]è stato coniato per questi tipi di attacco. Viene mascherata una mail/ pagina web con lo scopo di ottenere delle credenziali di un manager. Il contenuto è creato su misura per l'obbiettivo, è spesso scritto come un subpoena legale, un problema amministrativo o una lamentela di un cliente. Sono state utilizzate anche mail identiche a quelle dell'FBI cercando di forzare il ricevente a scaricare e installare del software.[102]

Nel primo trimestre del 2020, il membro dell'APWG OpSec Security ha scoperto che i siti SaaS e di webmail sono rimasti i maggiori bersagli del phishing, con il 34% di tutti gli attacchi. *"A febbraio abbiamo rilevato un calo degli attacchi contro il settore dei pagamenti"*, ha osservato Stefanie Wood Ellis, responsabile prodotti e marketing antifrode di OpSec Online.

[100] Debbie Stephenson, Spear Phishing: Who's Getting Caught?, Firmex. URL consultato il 27 luglio 2014.
[101] "caccia alla balena"
[102] What Is 'Whaling'? Is Whaling Like 'Spear Phishing'?, About Tech. URL consultato il 28 marzo 2015 (archiviato il 28 marzo 2015).

"Questo ha fatto scendere i phish mirati ai pagamenti solo al 13 per cento di tutti gli obiettivi, quando nel Nei quattro trimestri precedenti il settore dei pagamenti era stato pari al 20% di tutto il phishing". OpSec (una fondazione Il membro dell'APWG precedentemente noto come MarkMonitor) offre soluzioni di protezione del marchio di classe mondiale.

Tab.4.3.2. Phishing 1Q20



103

La quantità di denaro che un aggressore può guadagnare ottenendo carte regalo è significativamente inferiore a quella che può ottenere con un bonifico bancario. Nel corso del primo trimestre del 2020, l'importo medio delle gift card richieste da un BEC l'aggressore era 1.000 dollari.

[103] APWG-2020

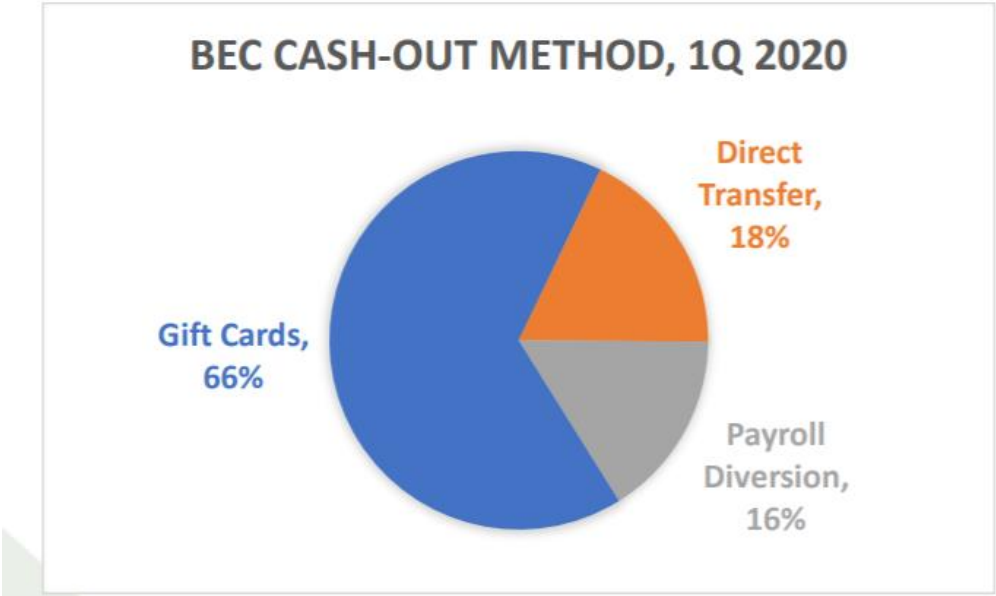
Tentativi di truffa intorno a questo importo di dollari possono avere una discreta possibilità di successo, perché possono essere approvati da più persone in un'azienda medio-grande, e l'importo è abbastanza piccolo da sfuggire ai controlli finanziari di alcune società.

4.3.1 Criminal use Covid 19 Business email compromise attacks

Il membro dell'APWG Agari segue la tecnica del furto di identità nota come *"business e-mail compromise"* o BEC. In un attacco BEC, un truffatore prende di mira i dipendenti che hanno accesso alle finanze dell'azienda, di solito inviando e-mail da account di posta elettronica falsi o compromessi (un attacco di "spear phishing"). Il truffatore si spaccia per un dipendente dell'azienda o per un'altra persona di fiducia e cerca di ingannare il dipendente per fargli inviare soldi. L'aggressore può prepararsi passando settimane all'interno della rete e dei conti dell'organizzazione, studiando i fornitori dell'organizzazione, il sistema di fatturazione e persino lo stile di comunicazione del CEO.

BEC Gli attacchi hanno causato perdite complessive per miliardi di dollari, sia alle grandi che alle piccole imprese. Agari ha esaminato migliaia di tentativi di attacco BEC osservati durante il primo trimestre. Agari conta la BEC come qualsiasi attacco di spear phishing basato sulla risposta che comporta l'impersonificazione di una persona di fiducia (una società esecutivo, venditore, ecc.) per ingannare una vittima a fare una transazione finanziaria o a inviare materiale sensibile. Agari protegge le organizzazioni dal phishing, dalle truffe BEC e da altre minacce avanzate via e-mail. Agari ha scoperto che i truffatori hanno richiesto fondi sotto forma di carte regalo nel 66% degli attacchi BEC, fino a 56 per cento nel terzo trimestre del 2019. Circa il 16 per cento degli attacchi ha richiesto una deviazione dei salari, dal 25% nel terzo trimestre. Circa il 18% ha richiesto bonifici bancari diretti

Tab 4.4.1. Cash Out Method; 1Q 20

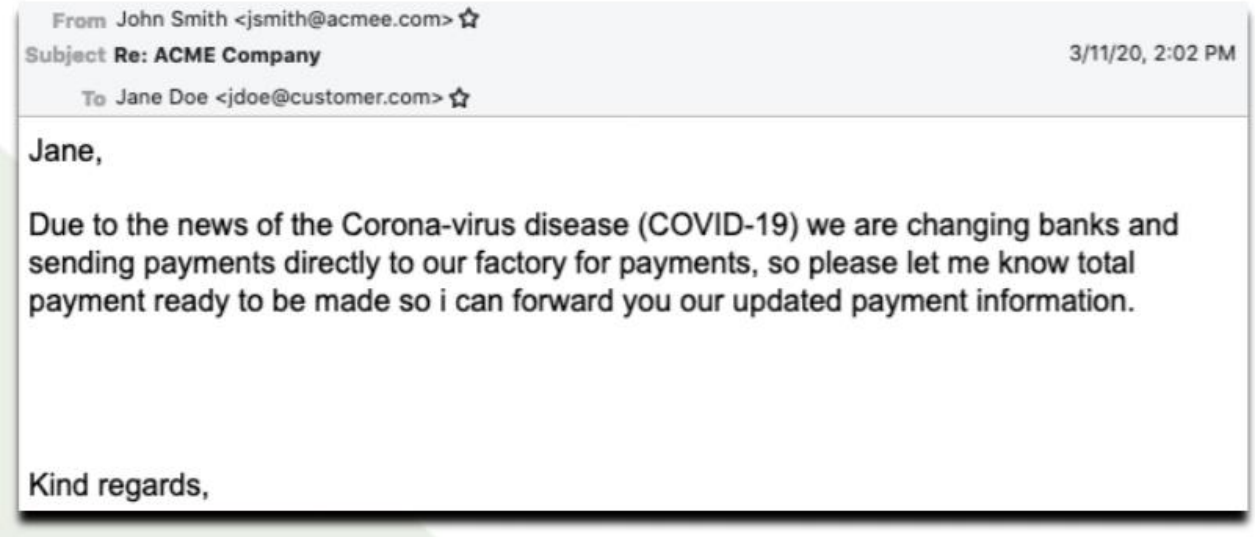


Agari, membro dell'APWG e collaboratore di Trends, ha anche seguito gli attacchi di phishing di COVID-19. *"Il nostro I dati indicano che gli attacchi di phishing di COVID-19 hanno iniziato ad aumentare la settimana dell'8 marzo. È stato lo stesso periodo in cui COVID-19 ha cominciato ad aumentare come argomento di interesse pubblico generale secondo Google Trends,"* ha detto Crane.Hassold, direttore senior della ricerca sulle minacce di Agari.

Hanno identificato quello che potrebbe essere stato il primo uso documentato della pandemia come esca in un "*Business Compromesso e-mail*" o attacco BEC. In un attacco BEC, un truffatore prende di mira i dipendenti che hanno accesso a finanze dell'azienda, di solito inviando loro e-mail da un account di posta elettronica falso o compromesso (una "lancia attacco "phishing"). Il truffatore si spaccia per un dipendente dell'azienda o per un'altra persona di fiducia e cerca di ingannare l'impiegato a mandare soldi.

L'11 marzo, un gruppo criminale che Agari chiama " *"Ancient Tortoise*" ha contattato un'azienda e si è spacciato per uno dei veri fornitori dell'azienda.

Il criminale ha chiesto alla società di pagare le fatture scadute, e ha usato il coronavirus come pretesto per fornire nuovi dettagli di pagamento alla vittima. Il criminale ha spiegato che l'epidemia aveva costretto il fornitore a cambiare la banca che utilizzava per ricevere i pagamenti. Il nuovo Il conto si è rivelato essere a Hong Kong, da cui il criminale poteva recuperare i fondi tramite i money mules.



Sopra: l'aggressore ha usato un dominio simile a quello dell'azienda bersaglio.

Nota: i nomi e i domini utilizzati sono stati modificati in precedenza per proteggere la vittima[104]

[104] Agari; https://docs.apwg.org/reports/apwg_trends_report_q1_2020.pdf

4.3.2 Toll fraud

L' *International revenue sharing fraud* (IRSF), nota anche come frode del pedaggio, è uno schema in cui i truffatori generano artificialmente un alto volume di chiamate internazionali su rotte costose. I truffatori effettuano chiamate verso i cosiddetti numeri a tariffa maggiorata e si prendono una parte delle entrate generate da queste chiamate. Anche se ci sono molti altri schemi nelle frodi di telecomunicazione, l'IRSF è il più diffuso ed è cresciuto di sei volte dal 2013. In tutto il settore delle telecomunicazioni, le perdite totali derivanti dalle frodi sui pedaggi sono stimate in 10 miliardi di dollari all'anno. Questo numero è aumentato solo negli ultimi anni con l'adozione di VOIP[105] e API[106] di comunicazione che rendono facile effettuare chiamate internazionali.

Qualsiasi applicazione che può effettuare una chiamata alla rete telefonica pubblica è vulnerabile all'IRSF. Vediamo più comunemente l'IRSF in tre modi:

1) *Hacking del PBX*: Prima dell'introduzione delle API di comunicazione, i truffatori dell'IRSF predavano principalmente i PBX[107] scansionando gli intervalli IP[108] per una porta 5060 aperta. I truffatori costringevano poi brutamente l'autenticazione del server, ottenevano l'accesso, quindi creavano traffico di frodi a pedaggio. Questa tecnica è ancora molto diffusa. Se siete clienti SIP Trunking, assicuratevi di seguire le migliori pratiche per proteggere il vostro PBX.

[105] Voice over IP (in italiano "Voce tramite protocollo Internet", in acronimo VoIP), in telecomunicazioni e informatica, indica una tecnologia che rende possibile effettuare una conversazione, analoga a quella che si potrebbe ottenere con una rete telefonica, sfruttando una connessione Internet o una qualsiasi altra rete di telecomunicazioni dedicata a commutazione di pacchetto, che utilizzi il protocollo IP senza connessione per il trasporto dati.
[106] In un programma informatico, con application programming interface si indica un insieme di procedure atte all'espletamento di un dato compito; spesso tale termine designa le librerie software di un linguaggio di programmazione.
[107] Un private branch exchange o PBX, nelle telecomunicazioni, è una centrale telefonica per uso privato, principalmente usata nelle aziende, enti, organizzazioni, per fornire una rete telefonica interna, tipicamente allacciandola alla rete telefonica generale esterna.
[108] Un indirizzo IP (dall'inglese Internet Protocol address) – in informatica e nelle telecomunicazioni – è un'etichetta numerica che identifica univocamente un dispositivo detto host collegato a una rete informatica che utilizza l'Internet Protocol come protocollo di rete.

2) *Abuso dell'account:* Qualsiasi servizio che offre agli utenti, in particolare se offri una sorta di esperienza di prova gratuita, è a rischio di frodi a pagamento. Questi truffatori creeranno un gran numero di conti falsi per generare traffico di chiamate verso numeri a tariffa maggiorata.

3) *Spamming [109]con codice di verifica vocale:* Quando si implementa l'SMS 2FA, è buona prassi fornire la possibilità di inviare un codice tramite una telefonata nel caso in cui l'utente sia su un telefono fisso o abbia problemi a ricevere SMS. I truffatori dell'IRSF sono attivamente alla ricerca di questi flussi, che spesso consentono di chiamare verso qualsiasi parte del mondo. I truffatori lanciano attacchi script per generare un elevato volume di chiamate attraverso questa funzione di verifica vocale.

Fase di Prevention

La migliore strategia di prevenzione è una combinazione di misure per limitare l'accesso di un truffatore alla vostra capacità di chiamata, oltre a stabilire limiti e restrizioni. Assicuratevi di aver considerato ciascuno dei seguenti aspetti della vostra applicazione:

i) *Sicurezza dell'account*: Utilizzare un numero di telefono e un processo di verifica via e-mail per ottenere la certezza che si tratti di una persona reale. Inoltre, qualsiasi altra valutazione delle frodi o integrazione di servizi antifrode di terzi può essere molto utile per garantire che i cattivi attori non passino dalla porta di casa vostra.

ii) *Autorizzazioni Geo:* Limitare il più possibile le chiamate verso destinazioni internazionali. Poiché le frodi a pedaggio terminano nei paesi con tariffe telefoniche costose, potete limitare la vostra esposizione permettendovi di chiamare solo verso i paesi più importanti. Se non c'è un motivo legittimo per cui voi o uno dei vostri utenti finali debba chiamare un paese, allora disattivate quella destinazione.

[109] Lo spam (o spamming) indica l'invio anche verso indirizzi generici, non verificati o sconosciuti, di messaggi ripetuti ad alta frequenza o a carattere di monotematicità tale da renderli indesiderati (generalmente commerciali o offensivi).

iii) *Limiti tariffari*: Ai truffatori piace attaccare duramente e velocemente gli account appena creati. Limitando le chiamate al minuto, le chiamate per 60 minuti e le chiamate per 24 ore, la durata delle chiamate e le chiamate contemporanee, si riduce la capacità dei truffatori di creare un elevato volume di traffico in un breve periodo di tempo. I limiti esatti dipendono dal rischio che si è disposti a correre relativamente alla fornitura di un'esperienza a basso attrito per i clienti legittimi. Vi consigliamo di aprire i vostri servizi solo dopo aver verificato sufficientemente il vostro cliente.

Oltre alle misure di cui sopra, consultate anche la nostra Guida per gli Sviluppatori Antifrode, una panoramica di altri tipi di frode che potreste dover affrontare.[110]

Fase di detection

Nel corso della commercializzazione dei servizi, la detection viene garantita con il monitoring di parametri che consentono, da parte di esperti analisti frodi, l'individuazione dei più rilevanti rischi emergenti. In caso di anomalie, gli analisti provvedono ad effettuare approfondimenti ed eventualmente a confermare la presenza di un incidente. Nel mercato delle telecomunicazioni, in particolare, per effettuare una efficace attività di detection, è di basilare importanza innanzitutto mantenere la mappatura aggiornata della molteplicità dei servizi offerti, in modo da poter intercettare anche i più deboli segnali di una frode emergente e di garantire una costante valutazione del rischio commerciale. I Fraud Management System, che monitorano il traffico telefonico e consentono la gestione dei casi, rivestono un ruolo fondamentale in questa attività.

[110] https://www.twilio.com/learn/voice-and-video/toll-fraud

Tali sistemi elaborano il traffico generato dai clienti e, sulla base di regole e parametri definiti dagli analisti frodi, generando i cosiddetti "casi". I parametri e le regole utilizzate dai Fraud Management System per il traffico telefonico sono molteplici (per direttrice chiamata, controlli su black list, ecc.), sono definiti dinamicamente e si basano tipicamente sul superamento di soglie di traffico. Dal momento che i fenomeni fraudolenti sono soggetti a rapide mutazioni e ad una notevole variabilità, i sistemi tradizionali di controllo basati esclusivamente sul superamento di soglie di traffico sono affiancati da moduli a tecnologia più evoluta come le reti neurali, con una intrinseca capacità di apprendimento dai casi di analisi pregressa. Naturalmente i sistemi di controllo, anche i più evoluti, devono essere costantemente aggiornati, corredandoli di nuove features messe a disposizione dai fornitori.

I sistemi aziendali per l'attività antifrode non sono tuttavia in grado di individuare, da soli, i fenomeni fraudolenti nel caso in cui la frode venga perpetrata sfruttando problemi tecnici che hanno come effetto la mancata produzione di dati utili al monitoraggio; anche l'utilizzo di tecniche di controllo basate sull'analisi economica dei servizi sarà quindi utile per evidenziare la generazione di costi anomali per l'azienda sfuggiti ai metodi di detection tradizionale.

Infine, tra le attività svolte in fase di detection, dopo l'acquisizione di un cliente, segnaliamo i controlli antifrode, effettuati in automatico, sull'eventuale presenza del cliente in blacklist e su altri tipi di informazioni sociodemografiche e comportamentali, allo scopo di definire un indice di rischio ed eventualmente attivare il fraud Analyst per ulteriori approfondimenti o per il passaggio ad una fase di reaction. Risultano quindi molto utili le verifiche documentali, che sono anche finalizzate ad individuare false identità, complete o parziali. Il progetto UCAMP2, già citato in precedenza, potrebbe risultare molto utile per facilitare l'accesso agli archivi di Stato e quindi permettere la verifica della congruità dei dati dell'utente. [111]

[111][111] https://frodi.clusit.it/_files/le_frodi_nella_rete.pdf

Reaction

La fase di reaction comporta l'applicazione di procedure per la gestione dei fenomeni di frode e l'eventuale escalation dei casi più rilevanti al Management. Nel caso di frode accertata dall'analisi, la reaction consiste tipicamente nella sospensione o blocco immediato dei servizi oggetto di frode, nella sospensione o blocco di SIM e IMEI, con una richiesta di supporto alle Tecnologie per eventuali interventi sulla Rete o all'area Legal, nel caso in cui si debbano bloccare dei pagamenti ad altre entità coinvolte (ad es. altro operatore). Successivamente, la gestione dell'incidente prevede l'individuazione dei meccanismi che hanno originato la frode e, se necessario, la denuncia alle Autorità competenti. Ciò avviene attraverso un processo di condivisione all'interno di un Gruppo di Lavoro che coinvolgerà diverse funzioni aziendali, di volta in volta interessate all'incidente, tra cui Finance, Marketing, Legal, Customer Care, Technology, allo scopo di approntare in breve tempo un piano di azioni da condividere con il Management.[112]

[112] https://frodi.clusit.it/_files/le_frodi_nella_rete.pdf

4.3.3 Malware & Ransomwhere

Un ransomware è un tipo di malware che limita l'accesso del dispositivo che infetta, richiedendo un riscatto (ransom in inglese) da pagare per rimuovere la limitazione. Ad esempio, alcune forme di ransomware bloccano il sistema e intimano l'utente a pagare per sbloccare il sistema, altri invece cifrano i file dell'utente chiedendo di pagare per riportare i file cifrati in chiaro. Inizialmente diffusi in Russia, gli attacchi con ransomware sono ora perpetrati in tutto il mondo.[113]

I ransomware tipicamente si diffondono come i trojan[114], dei malware worm, penetrando nel sistema attraverso, ad esempio, un file scaricato o una vulnerabilità nel servizio di rete. Il software eseguirà poi un payload[115], che ad esempio cripterà i file personali sull'hard disk.[116] I ransomware più sofisticati utilizzano sistemi ibridi di criptazione (che non necessitano di condivisione di chiavi fra i due utenti) sui documenti della vittima, adottando una chiave privata casuale e una chiave pubblica fissa. L'autore del malware è l'unico a conoscere la chiave di decriptazione privata. Alcuni ransomware eseguono un payload che non cripta, ma è semplicemente un'applicazione che limita l'interazione col sistema, agendo sulla shell di Windows e rendendola non operativa e controllata dal malware stesso,[117]o addirittura modificando il master boot record e/o la tabella di partizione (il che impedisce l'avvio del sistema operativo finché non viene riparata).

[113] Dunn John E., Ransom Trojans spreading beyond Russian heartland, TechWorld, 9 marzo 2012. URL consultato il 25 maggio 2015 (archiviato dall'url originale il 2 luglio 2014).
[114] Un trojan o trojan horse, nell'ambito della sicurezza informatica, indica un tipo di malware. Il trojan nasconde il suo funzionamento all'interno di un altro programma apparentemente utile e innocuo: l'utente, eseguendo o installando quest'ultimo programma, in effetti attiva anche il codice del trojan nascosto
[115] Il carico utile, in informatica, è un termine utilizzato per indicare la parte di dati trasmessi effettiva che è destinata all'utilizzatore, in contrasto con i metadati e con gli header che servono esclusivamente a far funzionare il protocollo di comunicazione.
[116] Adam Young, Building a Cryptovirus Using Microsoft's Cryptographic API, in Jianying Zhou e Javier Lopez (a cura di), Information Security: 8th International Conference, ISC 2005, Springer-Verlag, 2005, pp. 389–401.
[117] Ransomware: Fake Federal German Police (BKA) notice, SecureList (Kaspersky Lab). URL consultato il 10 marzo 2012 (archiviato dall'url originale il 5 febbraio 2012).

Il payload potrebbe ad esempio mostrare notifiche che credibilmente potrebbero essere state inviate dalla polizia federale o da varie compagnie, le quali affermano falsamente che il sistema sia stato usato per attività illegali o che contenga materiale illegale, pornografico o piratato.[118] Altri payload imitano le notifiche di attivazione prodotto di Windows XP, affermando che il computer potrebbe montare una distribuzione di Windows contraffatta, che va quindi riattivata. Queste tattiche forzano l'utente a pagare l'autore del malware per rimuovere il ransomware, sia con un programma che decritti i file criptati, sia con un codice di sblocco che elimini le modifiche fatte dal ransomware. Questi pagamenti di solito vengono effettuati tramite bonifico, con sottoscrizione via SMS, con un pagamento online attraverso un servizio voucher come Ukash o Paysafecard, o, più recentemente, tramite Bitcoin (la valuta digitale).

Per proteggere i computer dagli attacchi portati da temibili programmi malevoli ed evitare che gli utenti rimangano vittima di insidiose frodi informatiche si ricorre all'utilizzo di *vari metodi, di natura giuridica (cyberpolizia), educativa e tecnica*.

Il secondo importante metodo per proteggere gli utenti dai cybercriminali e dal malware è rappresentato dal *fattore educativo*; ciò si realizza informando adeguatamente gli utenti riguardo alla necessità di seguire scrupolosamente certe regole e adottare determinati comportamenti durante la navigazione in Rete e nello svolgimento delle attività digitali. Vi sono, di fatto, tre regole principali da seguire, sia per gli utenti domestici che per gli utenti corporate:

1. Utilizzo obbligatorio di un'adeguata protezione antivirus.
2. Non considerare affidabili le informazioni che giungono sul computer attraverso fonti non verificate

[118] Police warn of extortion messages sent in their name, Helsingin Sanomat. URL consultato il 9 marzo 2012 (archiviato dall'url originale il 14 marzo 2012).

Il rischio di infezioni informatiche può essere ugualmente ridotto attraverso quelle che vengono normalmente definite "*misure organizzative*". Si tratta, più precisamente, di misure riguardanti restrizioni di vario genere, valide sia per gli utenti domestici che per gli utenti corporate:

- applicare dei limiti all'utilizzo dei client di messaggistica istantanea;
- consentire l'accesso soltanto ad un numero limitato di siti web;
- attribuire solo a determinati computer del network aziendale la facoltà di accedere ad Internet, e così via.

Purtroppo, per quanto gli intenti siano più che apprezzabili e giustificati, restrizioni del genere possono talvolta produrre un impatto negativo sulle aspettative del singolo utente e sui processi di business dell'impresa. In tal caso è necessario trovare un giusto equilibrio tra le necessità delle due parti, considerando anche il fatto che ogni situazione può presentare aspetti specifici, da valutare con attenzione.

Non trascurare le informazioni messe costantemente a disposizione dalle società produttrici di soluzione antivirus e dagli esperti di sicurezza IT. Entrambi forniscono tempestivamente informazioni riguardo alle nuove tipologie di frodi informatiche, alle minacce IT più recenti, alle epidemie in corso, etc.; dedicate pertanto la necessaria attenzione a simili informazioni.

La storia del worm di posta elettronica LoveLetter e dei suoi numerosi cloni illustra perfettamente come possono essere respinti con successo gli attacchi portati dai malintenzionati. In pratica, immediatamente dopo la diffusione iniziale dell'epidemia generata dal worm, quasi tutte le società produttrici di antivirus hanno pubblicato, per gli utenti, precise raccomandazioni e linee guida riguardo alle precauzioni da adottare per proteggersi nei confronti di questo genere di e-mail worm.

A volte, tuttavia, vi sono dei casi in cui le informazioni diffuse riguardo ai nuovi incidenti generati da virus e altri tipi di malware non corrispondono esattamente alla reale portata di tali minacce IT. Abbastanza spesso, in effetti, dei semplici worm di posta elettronica, mascherati all'interno di e-mail relative ai temi caldi del momento – ad esempio un campionato del mondo di calcio, un disastro naturale, una catastrofe tecnologica o l'arresto del terrorista numero uno al mondo – vengono presentati da alcune società antivirus come fossero il tema in assoluto più importante e irrinunciabile del momento.

Le tre regole fondamentali di "igiene informatica", qui sopra descritte, possono essere così riassunte: la protezione è un "must"; non credere a nessuno, se non alle società antivirus (fatte le debite riserve); assicuratevi di disporre di un'efficace protezione anti-malware![119]

Nel 2012, circa 30.000 clienti bancari europei sono stati derubati di circa 36 milioni di euro - cioè circa 47 milioni di dollari - in una truffa bancaria online che ha funzionato sfruttando i dispositivi mobili, secondo le società di sicurezza che si sono imbattute nell'operazione. La truffa è stata soprannominata *Eurograbber* da Check Point Software Technologies[120] e Versafe, che dicono di aver scoperto l'operazione attraverso istituzioni finanziarie che conoscono dopo che i loro clienti di online banking sono stati colpiti.

Eurograbber di solito lavorava ingannando le vittime per fargli scaricare una variante personalizzata del Trojan Zeus, che poi prendeva il controllo dei loro computer e intercettava le sessioni di online banking. L'infezione del Trojan di Eurograbber può avvenire durante la navigazione in Internet o quando si cade in una e-mail di phishing, ha detto Darrell Burkey, direttore dei prodotti IPS di Check Point Software Technologies, che ha lavorato con l'israeliana Versafe per aiutare a indagare su Eurograbber.

[119] encyclopedia

[120] La Check Point Software Technologies Ltd. è un'azienda israeliana produttrice di dispositivi di rete e software, specializzata in prodotti relativi alla sicurezza quali firewall e VPN.

"*Si tratta fondamentalmente di un attacco man-in-the-middle contro un sito di una banca*", ha detto Burkey, aggiungendo che si ritiene che la truffa sia un'operazione criminale fuori dall'Ucraina, i cui server di comando e controllo sono stati recentemente interrotti dalle forze dell'ordine europee con la cooperazione degli ISP.

Eurograbber è stato scoperto prima in Italia, poi diffuso in Germania, Olanda e Spagna, e ha colpito sia i conti commerciali che quelli dei singoli consumatori di circa 30 banche, secondo Check Point e Versafe, che oggi ha pubblicato un rapporto sul funzionamento di Eurograbber. Eurograbber è stato in grado di trasferire illegalmente fondi dai conti dei clienti per importi che andavano dai 500 ai 250.000 euro.

Gli importi sottratti dai conti delle vittime erano relativamente bassi rispetto al conto stesso, dando così modo alla vittima di non accorgersi in breve tempo dell'importo ingiustamente sottratto dal proprio account. Molto spesso gli importi ingiustamente trasferiti erano così bassi da non far scattare i "*red flag*" della banca vittima; permettendo così ai truffatori grazie all'economia di scala di vedersi trasferire grandi importi nei propri conti.

E anche se ci sono state molte frodi bancarie negli ultimi anni, Eurograbber ha colpito le società di sicurezza come notevole nel modo in cui ha superato le misure di sicurezza delle banche basate sull'invio di un cosiddetto numero di autenticazione della transazione (TAN) via SMS al dispositivo mobile del cliente. Il TAN è una misura di sicurezza via SMS che consente al cliente della banca di verificare che la transazione bancaria online sia effettivamente autorizzata - ma Eurograbber compromette anche questo.

Durante la prima sessione bancaria del cliente dopo che il suo computer è stato infettato, il malware di Eurograbber inietta nella sessione istruzioni che invitano il cliente a inserire il suo numero di cellulare.

A quel punto, alla vittima viene detto di completare un falso "aggiornamento di sicurezza del software bancario" seguendo le istruzioni inviate al suo dispositivo mobile via SMS. Le istruzioni dell'aggressore via SMS invitano la vittima a cliccare su un link per completare un "aggiornamento di sicurezza" sul proprio cellulare. Tuttavia, "cliccando sul link si scarica effettivamente una variante di "Zeus in the mobile" (ZITMO) Trojan", si legge nel rapporto. La variante ZITMO è stata specificamente progettata per intercettare l'SMS della banca contenente l'importante "numero di autorizzazione della transazione".[121]

4.4 Gaming fraud

Truffa per il pagamento del gioco d'azzardo online

Mentre le cifre esatte sono quasi impossibili da individuare, il gioco online è come minimo un'industria multimiliardaria all'anno. Con tutto quel denaro che scorre in ogni settore, diventa altamente suscettibile a frodi o furti. Le frodi nei pagamenti sono un tipo di furto e rappresentano una significativa minaccia finanziaria per gli istituti di gioco online. Ecco una panoramica delle frodi di pagamento del gioco online, inclusi alcuni dei diversi tipi di frodi a cui sono vulnerabili le strutture di gioco online e cosa si può fare al riguardo.[122]

Che cos'è la frode dei pagamenti per il pagamento dei giochi online?

Ci sono due tipi principali di frodi nei pagamenti nell'industria del gioco, sebbene ci sia una serie di modi per commettere diversi tipi di frodi nei pagamenti. Le frodi "amichevoli" sono commesse dal legittimo titolare della carta di credito e la maggior parte degli altri tipi di frode sono una forma di furto d'identità. Ecco alcuni dei diversi modi in cui i giocatori possono commettere frodi nei pagamenti.[123]

[121] Senior Editor, Network World, Network World
[122] TransUnion_Formerly iovation
[123] TransUnion_Formerly iovation

Frode amichevole

A un livello più piccolo, l'industria del gioco d'azzardo si trova ad affrontare una quantità decente di frodi di chargeback. Analogamente all'industria dell'e-commerce, il chargeback si riferisce alle procedure relative all'autenticità degli acquisti. Un chargeback si verifica quando un acquisto digitale viene effettuato per acquistare un prodotto, fisico o online, e per qualche ragione non viene soddisfatto. Ciò significa che il prodotto non raggiunge mai l'acquirente, o è danneggiato o non mantiene la promessa fatta dal venditore.

L'addebito che viene restituito su una carta di pagamento dopo che un cliente contesta con successo un articolo sull'estratto conto o sul rapporto delle transazioni è chiamato chargeback. Ci possono essere due ragioni per cui ciò si verifica.

- Il primo motivo è dovuto ad una vera e propria confusione del titolare della carta di credito, quando il pagamento viene fatturato da una fonte sconosciuta. Questo può essere facilmente corretto assicurando che l'estratto conto della carta di credito rifletta un gioco specifico piuttosto che la sua società madre.

- Il secondo motivo è un po' più complicato. Questo avviene quando un chargeback viene utilizzato in modo improprio dal cliente per motivi malevoli. In questo caso, il giocatore si rifiuta di pagare le spese legittime in base a false richieste.

Poiché l'industria del gioco si occupa di un caso predominante di transazioni "veloci" di basso valore, rende difficile per l'azienda dimostrare che ogni transazione è avvenuta. Questo tipo di frode può mettere a dura prova il tempo e le risorse dell'azienda.[124]

[124] https://razorpay.com/learn/everything-you-need-to-know-about-tackling-gaming-fraud/

Acquisizione del conto

L'acquisizione di un conto o ATO può avvenire in diversi modi. In alcuni casi, i criminali informatici cercheranno di ottenere le credenziali di accesso di un utente attraverso una truffa di phishing. In questo tipo di truffa, un cybercriminale invierà all'utente un'e-mail con un qualche tipo di avviso, invitandolo ad accedere al sito per controllare il proprio account. L'e-mail conterrà un utile link che li porterà effettivamente a un sito controllato dal phisher, dove potranno acquisire le credenziali di accesso dell'utente. Il cybercriminale può quindi utilizzare le credenziali di accesso dell'utente per accedere al suo account sul sito legittimo e prosciugare il suo account criminali informatici possono anche percorrere la strada opposta, pagando per le attività di gioco con conti di credito che hanno rilevato.[125]

Attacco BIN

Un attacco BIN è anche un tipo di acquisizione di account, ma è molto più difficile da rilevare o scoraggiare per qualsiasi tipo di software di rilevamento delle frodi. La maggior parte delle banche produce carte di pagamento con una certa porzione di numeri che appaiono in ordine sequenziale, noti come BIN o Bank Identification Numbers. I criminali informatici hanno appreso che la maggior parte delle carte con lo stesso codice BIN hanno anche la stessa data di scadenza.

Ciò che manca loro è un codice CVV valido, ma ci sono ancora molti commercianti online che non richiedono il CVV per effettuare un acquisto. Trovando un codice BIN e una data validi, i criminali informatici possono giocare con i numeri rimanenti fino a quando non ne trovano uno che funziona. Una volta che sanno di avere un numero di carta di credito valido e la data di scadenza, possono poi utilizzare la carta per effettuare una singola grande transazione.

[125] TransUnion_Formerly iovation

I siti di gioco sono spesso l'obiettivo principale per questi acquisti e anche per trovare un numero valido. Poiché la maggior parte dei software di rilevamento delle frodi è alla ricerca di modelli di spesa insoliti, è improbabile che un piccolo acquisto e un acquisto di grandi dimensioni sollevino allarmi, il che consente di non rilevare la spesa fino a quando il titolare della carta autorizzato non controlla il loro estratto conto.[126]

Come prevenire le frodi nei pagamenti

L'autenticazione degli utenti e la fornitura di un'esperienza di qualità per i clienti è fondamentale per prevenire frodi e abusi di chargeback. Ma è più facile a dirsi che a farsi. La situazione attuale mette le agenzie di scommesse online in una posizione difficile. Un certo grado di attrito nell'esperienza del cliente è necessario per scoraggiare le frodi, ma troppo attrito può allontanare gli utenti legittimi.

Un rapporto pubblicato da Jumio [127]ha rilevato che più del 25% dei potenziali clienti del gioco d'azzardo online ha abbandonato il processo di apertura del conto prima del completamento, sostenendo che il processo era troppo lungo o complesso. I commercianti devono bilanciare la necessità di autenticazione con le esigenze dell'esperienza del cliente. L'unico modo per ottenere questo risultato è quello di separare i punti di attrito positivi da quelli negativi.

[126] TransUnion_Formerly iovation

[127] Jumio è una società di pagamenti mobili online e verifica dell'identità che fornisce prodotti per la scansione e la convalida di carte e ID per transazioni mobili e Web, che vendono come "Netverify Trusted Identity as a Service"

Un punto di attrito "positivo" è un punto che presenta un ragionevole e minimo grado di attrito che è in definitiva trascurabile rispetto alla protezione che fornisce. Alcuni esempi di attrito positivo includono:

- Verifica del CVV della carta quando la si collega al conto dell'utente.
- Chiedere agli utenti di verificare ogni aggiunta di fondi prima di finalizzare.
- Richiedere password complesse e uniche per tutti i nuovi conti.
- Offrire 3-D Secure 2.0 per gli utenti che optano per il servizio.
- Impiegando strumenti di frode backend (geolocalizzazione, verifica dell'IP, punteggio delle frodi, ecc.)
- Offerta di pagamenti mobili con autenticazione a due fattori.
- Verifica dell'età dei singoli utenti per prevenire l'abuso del gioco d'azzardo online da parte dei minorenni.

Al contrario, l'attrito "negativo" rallenta le transazioni e influisce sull'esperienza del cliente, fornendo al tempo stesso una scarsa protezione reale contro le frodi e i chargeback. Alcuni esempi di questo possono includere:

- Navigazione del sito troppo complicata (o interrotta).
- Campi eccessivi o ridondanti durante la creazione del conto e il finanziamento.
- Limitazione dei metodi di pagamento accettati.
- Implementazione di metodi di verifica obsoleti o inefficaci.
- Nessuna strategia sarà mai perfetta
- Anche dopo aver adottato punti di attrito positivi e aver eliminato quelli negativi, non si è ancora completamente protetti.

La natura dell'industria richiede di stare al passo con il progresso tecnologico, così come i regolamenti del settore, le regole degli schemi di carte, il diritto internazionale... e altro ancora. Questo può sembrare intimidatorio, ma collaborare con gli esperti del settore per gestire i diversi aspetti della vostra strategia di business può rendere tutto molto più facile.[128]

La funzione Antiriciclaggio→ Strumenti di prevenzione adottati da Sisal

Dal 2013 Sisal ha formalizzato il presidio delle attività di antiriciclaggio e ha creato una funzione organizzativa dedicata. I principali compiti della funzione Antiriciclaggio sono:

- identificare e verificare adeguatamente il profilo della clientela attraverso procedure particolarmente rigorose (in particolare per le transazioni superiori a € 1.000);
- istituire l'Archivio Unico Informatico (AUI) nel quale registrare e conservare i dati identificativi e le altre informazioni relative ai rapporti e alle operazioni;
- inviare i dati aggregati all'Unità di Informazione Finanziaria e segnalare le eventuali operazioni sospette;
- istituire misure di controllo interno e assicurare un'adeguata formazione dei dipendenti.

In funzione dello sviluppo della normativa antiriciclaggio si è aggiunto un ulteriore importante Stakeholder istituzionale, Banca d'Italia, e nello specifico l'unità di Informazione Finanziaria (UIF), struttura incaricata di prevenire e contrastare il riciclaggio del denaro e il finanziamento al terrorismo.

[128] Chargebacks911

Principali attività nel settore giochi 2018

- Prosecuzione delle attività di analisi delle evidenze generate dagli indicatori di rischio e dall'attività di name detection;
- Erogazione, tramite una piattaforma di e-learning, della formazione antiriciclaggio per tutti i punti vendita e per il personale interno Sisal;
- Gestione delle richieste di informazioni da parte delle autorità esterne in ambito antiriciclaggio.

Principali attività nei servizi di pagamento 2018

- Revisione e aggiornamento delle procedure antiriciclaggio in relazione al mutato quadro normativo;
- Erogazione, tramite una piattaforma di e-learning, della formazione antiriciclaggio per la rete distributiva e per il personale di sede direttamente coinvolto nell'attività dell'Istituto di Pagamento;
- Individuazione di nuovi indicatori di anomalia;
- Svolgimento di visite ispettive in ambito antiriciclaggio per i punti di pagamento;
- Gestione delle richieste di informazioni da parte delle autorità esterne in ambito antiriciclaggio. Ulteriori tutele per il giocatore online

Ulteriori tutele per il giocatore online

- Sisal verifica l'identità dei suoi clienti al momento della registrazione iniziale (compilazione form d'iscrizione) e a registrazione ultimata;
- Ogni giocatore deve inviare entro 30 giorni una copia fronte/retro di un documento di identità;
- I Conti Gioco di cui entro 30 giorni non è pervenuta la documentazione vengono sospesi;
- Non sono consentite registrazioni replicate. Il sistema verifica sempre l'univocità di codice fiscale e anagrafica.[129]

[129] Sisal_ https://www.sisal.com/iniziative/tutela-consumatore/sicurezza/prevenire-riciclaggio

Rischi di riciclaggio nell'e-gaming & Casi Reali

Nella letteratura scientifica internazionale i rischi di reale utilizzo dell'e-gaming, quale strumento per la commissione del reato di cui all'art. 648-bis c.p., vengono considerati molto contenuti per i Paesi che hanno adottato sistemi regolati, ed al contrario marcati ed evidenti per quelli deregolamentati.[130]

Il riciclaggio di denaro con l'evoluzione delle tecnologie e dei giochi online colpisce anche le piattaforme di gaming per adolescenti. Fortnite, World of Warcraft rientrano tra I giochi in streaming più gettonai per il riciclo di denaro sporco.

Il settore è scarsamente regolamentato e pertanto diventa luogo ideale per ripulire i profitti illeciti derivanti da droga ed armi. I riciclatori di denaro non difettano certo di fantasia: merito dell'esperienza, certo, così come dell'evoluzione tecnologica che, senza che sua intenzione, offre spesso nuove opportunità inedite per i criminali. Lo dimostra il settore degli MMORPG[131].

Fortnite è un gioco online molto famoso, sviluppato nel 2017 dalla società USA Epic Games. Nel settembre del 2018 ha raggiunto l'impressionante quota 200 milioni di utenti registrati con una crescita di oltre il 65% in appena cinque mesi. A gennaio, il quotidiano The Independent[132], in partnership con la società di sicurezza informatica Sixgill[133], ha rivelato come la piattaforma sia stata mezzo (ovviamente involontario) di varie operazioni di riciclaggio realizzate attraverso i cosiddetti V-bucks, la valuta utilizzata nel videogioco.

[130] Rischi di riciclaggio nell e gaming Avv. Maurizio Arena,Avv. Marcello Presilla

[131] Un MMORPG (cioè Massive[ly] Multiplayer Online Role-Playing Game, ovvero gioco di ruolo in rete multigiocatore di massa) è un gioco di ruolo per computer o console che viene svolto tramite Internet contemporaneamente da più persone reali, perciò si chiamano giochi "online".

[132] The Independent è un quotidiano britannico online. Fondato nel 1986 come giornale cartaceo, dall'aprile 2016 esce esclusivamente in edizione digitale

[133] Sixgill è una società israeliana di cyber intelligence informatica che analizza e monitora il deep web e il dark web per individuare informazioni sulle minacce. La società è stata fondata nel 2014 e ha sede a Netanya, in Israele.

Utilizzando carte di credito rubate e/o clonate, i "riciclatori" avrebbero acquistato ingenti quantità di moneta digitale da rivendere a prezzo scontato sul dark web. Per far sparire ogni eventuale traccia gli acquisti effettuati sullo store ufficiale del gioco sarebbero stati realizzati in bitcoin rendendo di fatto le transazioni ancora più difficili (se non impossibili) da tracciare. I numeri assoluti dell'operazione criminale non sono comunque noti con certezza.[134]

Per i criminali del riciclaggio di denaro, sostiene un'indagine della società informatica canadese Trulioo, i metodi tradizionali si scontrano con le stringenti regolamentazioni sperimentata negli ultimi anni da molti stati. Iniziative come l'Anti-Money Laundering Directive della UE relative alla Beneficial Ownership (NDG: le operazioni trasparenza sulle compagnie di facciata registrate nei paradisi fiscali) rendono il riciclaggio sempre più complicato e soprattutto rischioso.

Proprio per queste ragioni la ricerca dell'anonimato conduce i criminali in territori più o meno vergini dove i margini di manovra sono decisamente più larghi. Secondo le stime più recenti il gaming online fattura oggi oltre 170 miliardi di dollari a livello globale e per le organizzazioni criminali rischia di apparire ancor più attraente di un comparto tradizionalmente profittevole come il gioco d'azzardo.[135]

[134] https://www.gdr-online.com/articoli-giochi-online-riciclaggio-di-denaro.asp
[135] https://www.gdr-online.com/articoli-giochi-online-riciclaggio-di-denaro.asp

CONCLUSIONE

Le frodi aziendali sono sempre state oggetto di attenzione da parte di studiosi e giuristi: inizialmente non si indagava a fondo sulle cause relativi a tali fatti, che tuttora continuano ad interferire sul mercato e le sue regole, perché si pensava che la motivazione che spingesse a commettere illeciti fosse un'esigenza di tipo fiscale. Successivamente è stato riscontrato che alla diffusa pratica delle manipolazioni contabili non vi ricorrevano solo quelle aziende o gruppi che volevano coprire temporanee situazioni di difficoltà. Al contrario, ad esse hanno fatto ricorso proprio gruppi industriali che presentavano apparentemente un buon andamento economico finanziario e una solida struttura patrimoniale.

È ormai indiscutibile che il mondo in cui viviamo stia attraversando un periodo di crisi e, come sottolineano spesso i media o vari analisti o pensatori, essa riguarda vari aspetti della vita. Ma analizzando la situazione con più attenzione, si può individuare un denominatore comune, un fattore che, come ha ben evidenziato Ervin Làszlò[136] , si situa per così dire alla fonte, e cioè il fatto che tutte le crisi discendono a cascata dalla vera e unica crisi: la *crisi dei valori*. La crisi di valori porta sì ad uno smarrimento di quelli che sono i punti cardine di una condotta di vita integra ed etica basata su capisaldi solidi in tema di integrità morale.

Vi è la consapevolezza che con il trascorrersi del tempo l'evoluzione tecnologica affini e migliori quelli che sono gli strumenti adottati dai fraudatori per portare al termine il proprio obiettivo. Allo stesso tempo l'evoluzione stessa affina da un lato quelli che sono gli impianti normativi e dall'altro quelli che sono le best practices in termini di prevention e detection che le imprese adottano, con i dovuti adattamenti alla singola realtà e market segment. Seguendo un processo logico semplice, al compiersi di una nuova manovra fraudolenta, gli enti predisposti alla mitigazione del rischio di frode studiano e mettono in atto strumenti mirati a cauterizzare quelli che sono i danni emersi con il fine ultimo di prevenirli.

[136] esperto in filosofia della scienza e della teoria dei sistemi

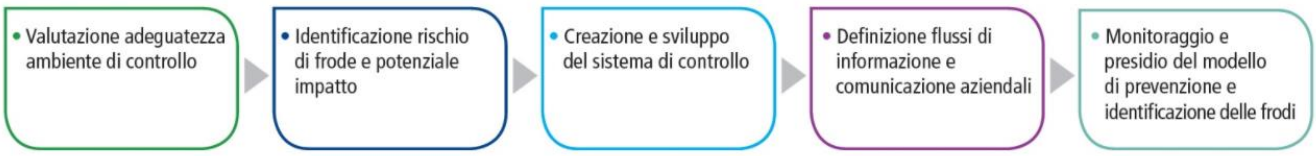
In quest'ottica la sfida al contrasto delle frodi risulta avvincente in quanto occorre un continuo adattamento ai nuovi schemi di frode a cui le imprese sono esposte.

L'esatta dimensione del fenomeno delle frodi all'interno delle imprese è tuttavia di difficile determinazione in primo luogo a causa del timore di danneggiare l'immagine aziendale, che induce le organizzazioni a non rendere pubbliche le malpractices individuate e a non palesare pertanto l'inadeguatezza e/o l'inefficacia dei propri meccanismi di controllo e, in secondo luogo, per la difficoltà sempre maggiore di individuarle.

Bisogna tenere conto che è quasi impossibile stimare con certezza il numero di frodi che realmente accadono nei diversi settori economici.

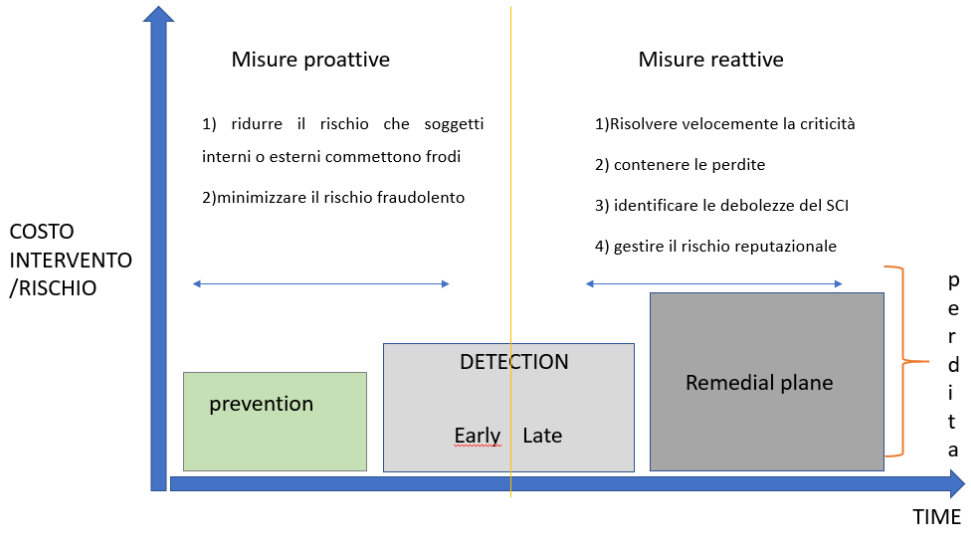
In un sistema perfetto dove il Sistema di Controllo Interno opera a pieno regime, il processo di *prevention*, *detection* e *investigation* operano come ingranaggi di un sistema ben lubrificato.

Tab 5.1 Sintesi del SCI



Riteniamo infatti che investimenti mirati che operino nella fase preventiva possano rappresentare il miglior strumento per ammortizzare se non prevenire atti illeciti poi difficilmente sanabili; : sebbene infatti non causino un beneficio diretto e tangibile per la società, in quanto l'obiettivo è evitare che la frode venga commessa, il valore aggiunto, in ottica costi-benefici, è rappresentato proprio dal risparmio di costo ottenuto dalla mancata concretizzazione della perdita dovuta a frodi e, seppur difficilmente quantificabile, dal danno reputazionale non manifestato.

Tab 5.2 Fraud Prevention & Detection



Investire nella prevenzione è fondamentale per minimizzare l'esposizione al rischio reputazionale & ridurre il rischio di atti fraudolenti commessi da soggetti interni o esterni. I benefici reali si hanno nel lungo termine in quanto si saranno sviluppate strategie efficaci a limitare il verificarsi di frodi e conseguentemente la perdita economica ad essa collegata. Conseguentemente nel lungo termine si avrà la capacità di risolvere velocemente situazioni critiche; contenere le perdite; identificare le debolezze del sistema di controllo interno e gestire il rischio reputazione.

La tecnologia in questo rappresenta un fedele alleato, grazie ai molteplici strumenti che offre. L'utilizzo delle tecniche più avanzate di data analytics e intelligenza artificiale rappresentato strumenti in grado di incrociare una grande quantità di dati e conseguentemente di indicarti i punti di debolezza del proprio sistema rendendo di fatto le analisi contemporaneamente sia più efficaci che efficienti.

Per prevenire reati le società dettano una serie di comportamenti da far adottare a tutti i soggetti che operano per le società o nelle società. La violazione di tali regole comporta l'applicazione di sanzioni più o meno gravi per garantire l'efficace attuazione dei modelli stessi e consentire alle società di beneficiare dell'esimente dalle responsabilità amministrative.

La progettazione e l'applicazione dei diversi sistemi di controllo analizzati precedentemente e dei modelli organizzativi, tagliati su misura sull'impresa e ben integrati tra di loro, rappresentano una soluzione efficace a contrasto delle frodi. Tuttavia, rivestono un ruolo cruciale la (i) necessità di aggiornamento continuo di tali strumenti per rispondere in maniera sempre più puntuale ai rischi di frode in costante mutamento ed (ii) il bilanciamento tra sistema di controllo ed operatività del business: per garantire una piena sostenibilità dell'attività d'impresa nel lungo periodo: il primo non deve ingessare la seconda e quest'ultima non può operare al di fuori dei paletti disegnati dal primo.

BREVE RIASSUNTO DELL'ELABORATO

CAPITOLO 1

LA FRODE: FATTISPECIE, FATTORI CHE NE FAVORISCONO IL REALIZZO

L'obiettivo del presente elaborato risiede nel tentativo di ripercorrere e ricostruire quelli che sono gli schemi tipici e non di generali schemi di frode ed in parallelo considerare ed argomentare quelli che sono gli strumenti principali nati ed in continua evoluzione che mirano a contrastare la diffusione delle frodi societarie in diversi settori e canali del panorama moderno. Particolare attenzione verrà data al mondo delle frodi informatiche, assicurative e bancarie, che rappresentano un tema topico del sistema fraudolento moderno; punto centrale e fondamentale di questo elaborato ruota nel percorrere l'evoluzione in corso delle tecniche fraudolente moderne e non. Una delle teorie che spiega al meglio il perché vengano attuale azioni fraudolente prende il nome di *Fraud Triangle.* Tale teoria sancisce che ogni frode presenta tre elementi caratterizzanti: 1) Incentivi e pressioni; 2) Opportunità.

Tenendo fede a quello che è lo scenario mondiale nel corso di questo 2020 non possiamo non riportare di seguito alcune considerazioni che enucleano tali aspetti con riferimento specifico al rischio di frode correlato alla vicenda COVID-19. Nel corso di questa fase dell'emergenza da COVID-19 si riscontrano perlomeno due fattori standard che fisiologicamente aumentano il rischio di frode all'interno di una società; l'obiettivo immediato del management riguarda il contenimento dell'impatto economico-patrimoniale degli effetti dell'emergenza sul business per salvaguardare la continuità della propria impresa nel breve periodo ed lo scenario in cui l'impresa opera è costantemente mutevole e si adatta agli sviluppi dell'emergenza, dettati ad esempio da provvedimenti d'urgenza emanati dal Legislatore per contenere gli impatti negativi legati alla vicenda.

I principiali rischi sono dettati da:

1) La mancanza di un framework di controllo che garantisca livelli di performance dei dipendenti assimilabili alla situazione pre-COVID-19 e prevenga comportamenti non etici messi in atto dagli stessi;
2) L'impossibilità di svolgere alcuni controlli da remoto in quanto non è prevista la versione, ove possibile, automatizzata degli stessi;
3) Il proliferare di schemi di frode che basano la propria riuscita sulla difficoltà di comunicazione tra soggetti fisicamente distanti.

Si pensi ad esempio alla cd. "CEO Fraud", in cui il frodatore inoltra ad un dipendente del dipartimento amministrativo una e-mail fake in cui, spacciandosi per l'AD, richiede, in deroga alle procedure in vigore, la disposizione urgente di un pagamento a favore di un beneficiario a lui riconducibile. In un contesto di crisi ed incertezza come quello provocato dal COVID-19, comportamenti comunque giudicati fraudolenti tendono ad essere giustificati più facilmente dal soggetto che commette o tenta di commettere l'illecito perché messi in atto al fine salvaguardare un interesse reputato più meritevole di tutela.

Schematizzare gli elementi che portano un soggetto a compiere atti fraudolenti, tenendo conto del fatto che le fonti delle frodi sono differenti anche a seconda del ruolo ricoperto dal perpetratore; rende quasi impossibile riscostruire un modello unico in grado di delineare un meccanismo univoco. Se prendiamo come esempio i *white collar crime* e li mettiamo a confronto con le *corporate fraud* possiamo con semplicità identificare leve e ragioni diverse pur avendo come risultato il compiersi di una frode. Secondo Bologna gli elementi che danno luogo a queste reazioni fraudolente sono le seguenti: 1) ideologico, 2) economico; 3) psicologico.

Nel valutare questi elementi bisogna tenere costo che oltre a fattori di natura personale, esistono un insieme di fattispecie esterne collegate all'ambiente di lavoro ed al collocamento dell'impresa che influenzano le scelte decisionali fraudolente del soggetto. Possiamo riconoscere qua sotto alcuni degli elementi interni che possono influire sul livello di qualità del sistema di controllo interno:

1) il grado di separazione dei compiti;
2) le modalità di effettuazione delle pianificazioni e dei controlli su di esse;
3) le vie intraprese per la gestione dei rapporti con il personale;
4)lo stile di direzione e le deleghe di responsabilità.

Un'altra distinzione in merito alla generale distinzione delle frodi riguarda le frodi interne e quelle esterne. Le prime sono attuate da soggetti che hanno legittimo accesso agli edifici, agli asset e ai documenti contabili aziendali (manager, impiegati e collaboratori a tutti i livelli). Le seconde invece sono commesse da soggetti esterni, oppure che entrano in contatto con l'azienda in virtù di relazioni legittime (clienti, fornitori, equiparati a soggetti interni). Con l'obiettivo ultimo di combattere e limitare la diffusione delle frodi, il primo passo che deve essere fatto è quello di classificare e riconoscere gli schemi di frode potenzialmente attuabili dentro l'impresa; a tale scopo interviene l'*Association of Certified Fraud Examiners* (AFCE). L'ACFE istituisce poi un'ulteriore classificazione, considerata universalmente come la più autorevole, relativamente alle occupational fraud. In tale ambito, secondo l'ente, i comportamenti fraudolenti possono essere suddivisi in:

1) le frodi di falsa informativa finanziaria (financial statement fraud);
2) l'appropriazione indebita di beni (asset misappropriation);
3) la corruzione (corruption).

Al livello più alto del *Fraud Tree*, ci sono le tre categorie principali di frodi professionali. Malversazione di beni (*Asset Misappropriation*), riguardante un dipendente che ruba o utilizza in modo improprio le risorse dell'organizzazione che lo impiega, si verifica nella maggioranza delle casistiche (86% dei casi). Al contrario, la frode a livello di bilancio (*Financial Stament Fraud*), in cui l'autore del reato provoca intenzionalmente un'inesattezza o un'omissione materiale nella gestione finanziaria dell'organizzazione, sono i meno comuni (10% degli schemi), ma la categoria di frode professionale più costosa. La terza categoria, la corruzione - che comprende reati come la corruzione, i conflitti di interesse e l'estorsione - cade nel mezzo in termini di sia la frequenza che i danni finanziari. Questi schemi si verificano nel 43% dei casi e causano una perdita mediana di 200.000 dollari.

Negli ultimi anni, complice anche la crisi economica, il rischio di alternazione dolosa della rappresentazione della situazione economico-patrimoniale-finanziaria nel bilancio delle società è aumentato. Le ragioni che portano ad una manipolazione di quanto rappresentato in bilancio può avvenire per diverse ragioni, tra queste riconosciamo:

1) Incoraggiare gli investimenti attraverso la vendita di azioni;

2)Per dimostrare l'aumento dell'utile per azione o dell'interesse sui profitti della società,

3)quindi permettendo di aumentare i pagamenti di dividendi/distribuzione;

4)Per coprire l'incapacità di generare flussi di cassa;

5)Per evitare percezioni negative del mercato. In questo contesto il legislatore con l'intento di sanzionare le condotte di falso in bilancio e ridurre il rischio di frode è intervenuta andando a modificare la fattispecie di reato di *'false comunicazioni sociali*, di cui agli articoli 2621 e 2622 del Codice civile.

Spesso errori significativi di una falsa informativa economico-finanziaria riguardano la sopravvalutazione dei ricavi (ad esempio, attraverso la loro rilevazione anticipata o la registrazione di ricavi fittizi) o la loro sottovalutazione (per esempio, attraverso il loro non corretto rinvio ad un esercizio successivo).

Le ragioni che portano ad una manipolazione di quanto rappresentato in bilancio può avvenire per diverse ragioni, tra queste riconosciamo:

1)Attività o ricavi sopravvalutati, costi delle attività o ricavi artificiali;
2)Passività e spese sottovalutate.

Nella redazione del bilancio, la direzione ha la responsabilità di effettuare numerose valutazioni e assunzioni che riguardano le stime contabili significative ed ha la responsabilità di controllare la ragionevolezza di tali stime su base ricorrente. Una falsa informativa economico-finanziaria è spesso realizzata con stime contabili intenzionalmente non corrette. In caso di operazioni significative bisogna considerare se la motivazione economica sottostante alle operazioni (o la sua eventuale assenza) suggerisce che le operazioni siano state poste in essere per realizzare una falsa informativa economico-finanziaria o per nascondere appropriazioni illecite di beni e attività dell'impresa.

Tra le voci di bilancio sensibili ad azioni fraudolente riconosciamo anche i le consulenze e le intermediazioni fittizie; la tecnica, piuttosto semplice, è quella di utilizzare fatture per prestazioni di consulenza inesistenti o di valore nettamente inferiore allo scopo di creare indebite disponibilità per gli amministratori. Al fine di individuare e prevenire questo tipo di frode è opportuno andare a verificare tutti i costi per servizi più significativi, ed anche i costi legati alle intermediazioni, controllando che siano sottoposti a procedure rigide sia nella fase di creazione del rapporto, che nella fase di pagamento.

CAPITOLO 2

IDENTIFICAZIONE E GESTIONE DEL RISCHIO DI FRODE E LE PRINCIPALI NORMATIVE ITALIANE E STATUNITENSI

La gestione del rischio di frode e di cattiva condotta è una preoccupazione crescente per il management e per le parti interessate nell'ambiente aziendale odierno. Secondo un recente studio dell'Association of Certified Fraud Examiners, una tipica organizzazione perde circa il 7% dei suoi ricavi annuali a causa delle frodi. Un'organizzazione deve riconoscere i rischi specifici di frode che potrebbero minacciare la sua stabilità finanziaria, operativa e del marchio.

La valutazione del rischio di frode è composta da 15 moduli, ognuno dei quali contiene una serie di domande destinate ad aiutare le organizzazioni a fare uno zoom sulle aree di rischio. Il professionista della frode e il cliente o il datore di lavoro dovrebbero iniziare il processo di valutazione del rischio lavorando insieme per rispondere alle domande di ogni modulo. Una volta completate tutte le domande, il professionista della frode dovrebbe esaminare i risultati della valutazione con il cliente o il datore di lavoro. La Valutazione del Rischio di Frode può rivelare alcuni rischi residui di frode che non sono stati adeguatamente mitigati a causa della mancanza o della non conformità con gli appropriati controlli preventivi e investigativi. Il professionista della frode dovrebbe lavorare con il cliente per sviluppare strategie di mitigazione di eventuali rischi residui con una probabilità o una significatività di accadimento inaccettabilmente alta.

La prevenzione delle frodi aziendali è diventato un tema importante da quando l'approvazione negli USA del Sarbanes-Oxley Act del 2012 ha imposto nuovi obblighi alle aziende. Lo scopo è quello di garantire una sistematica azione preventiva delle frodi aziendali in modo da incrementare la fiducia degli investitori. L'analisi degli obiettivi aziendali e il monitoraggio dei sistemi incentivanti intendono attenuare le situazioni di tensione da cui ha origine il processo fraudolento.

Già da diversi anni si ritiene che la prevenzione delle frodi aziendali debba essere messa in atto tramite un'adeguata implementazione del sistema di controllo interno. In Italia lo sviluppo di adeguati sistemi di controllo interno e di auditing è stato stimolato dall'adozione del Decreto Legislativo n. 231/2001 dell'8 giugno del 2001, intitolato "Disciplina della responsabilità amministrativa delle persone giuridiche", a norma dell'art. 11 della legge 29 settembre 2000, n.300, ha introdotto nel nostro ordinamento la responsabilità penale degli enti, aggiungendola a quella della persona che materialmente ha commesso il fatto.

Una conseguenza fondamentale di una simile innovazione è stata, ovviamente, l'inserimento del controllo della legalità e della regolarità dell'operato sociale fra il novero degli interessi di tutti i soggetti che partecipano a vario titolo alle vicende patrimoniali dell'ente. Inizialmente gli studiosi hanno avuto delle perplessità, essi si sono domandati se la società potesse veramente compiere un reato, in realtà la risposta appare semplice: l'azienda non è solo un complesso di beni, ma è caratterizzata da un elemento umano.

L'ambito di applicazione della norma è stabilito all'art.1, per ciò che concerne il lato oggettivo ci si riferisce alla "responsabilità degli enti per gli illeciti amministrativi dipendenti da reato", dal lato soggettivo è previsto che il decreto si applichi agli enti forniti di personalità giuridica e alle società e associazioni anche se prive di questo requisito, rimangono quindi esclusi lo Stato, gli enti pubblici territoriali ed infine quelli non economici che svolgono funzioni di rilievo costituzionale.

Le conseguenze per l'organizzazione cambiano a seconda del soggetto che ha commesso il reato: in caso di soggetti apicali, in base art.6, la società non è responsabile se dimostra che:

a) L'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi

b) Il compito di vigilare sul funzionamento e l'osservanza dei modelli e di curare il loro aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo;

c) Le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione;

d) Non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla lettera b).

La sanzione pecuniaria, sempre applicata, viene irrogata per quote, il cui numero, non inferiore a 100 e non superiore a 1000, è determinato dal giudice tenendo conto della gravità del fatto, del grado di responsabilità dell'ente, nonché dell'attività svolta per eliminare od attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti.

CAPITOLO 3

UN VALIDO STRUMENTO DI PREVENZIONE DELLE FRODI: IL SISTEMA DI CONTROLLO INTERNO

L'espressione "controllo interno" assume, significati diversi a seconda dell'ambito a cui ci si riferisce. Nel settore pubblico il controllo interno consiste principalmente in attività di verifica effettuate da un soggetto che, nonostante non sia parte dell'ente monitorato, opera comunque nei confini dello stesso. In genere le best practices internazionali si rifanno al Coso Report ed in seguito le autorità di vigilanza nazionali operano per meglio amalgamare il Coso con il sistema di vigilanza per esistente.

Negli Stati Uniti, il concetto di sistema di controllo interno è già stato trattato e definito da tempo dal Committee of Sponsoring Organizations of the Treadway Commission (CoSO) che nel 1992, dopo diversi significativi scandali avvenuti negli anni "80, ha pubblicato il CoSO Report: Internal Control – An Integrated Framework, un documento avente l'obiettivo di fornire sia una definizione comune di controllo interno, sia uno standard di riferimento attraverso il quale le società e ogni altra forma di organizzazione possano valutare ed implementare i loro sistemi di controllo. Prima di trattare però più nello specifico il modello presentato dal CoSO Report, è doveroso fornire una definizione avente valenza generale del concetto di sistema di controllo interno.

Poiché gli obiettivi riguardanti l'affidabilità del reporting e la conformità alle leggi e ai regolamenti sono sotto il diretto controllo dell'azienda, l'ERM è in grado di fornire una ragionevole sicurezza per il conseguimento di questa tipologia di obiettivi. Il conseguimento degli obiettivi strategici e operativi è soggetto a eventi esterni che non sempre rientrano nella sfera di controllo dell'azienda; di conseguenza, la gestione del rischio può solo fornire una ragionevole sicurezza che il management e il consiglio di amministrazione, nel suo ruolo di vigilanza, siano tempestivamente informati della misura in cui si stanno realizzando detti obiettivi.

L'ERM è costituito da otto componenti interconnessi. Essi derivano dal modo in cui il management gestisce l'azienda e sono integrati con i processi operativi. Questi componenti sono:

• *Ambiente interno* - L'ambiente interno, che costituisce l'identità essenziale di un'organizzazione, determina i modi in cui il rischio è considerato e affrontato dalle persone che operano in azienda.

• *Definizione degli obiettivi* - Gli obiettivi devono essere fissati prima di procedere all'identificazione degli eventi che possono potenzialmente pregiudicare il loro conseguimento.

• *Identificazione degli eventi* - Gli eventi esterni e interni, che influiscono sul conseguimento degli obiettivi aziendali, devono essere identificati distinguendoli tra "rischi" e "opportunità".

• *Valutazione del rischio* - I rischi sono analizzati, determinando la probabilità che si verifichino in futuro e il loro impatto, al fine di stabilire come devono essere gestiti.

• *Risposta al rischio* - Il management seleziona le risposte al rischio emerso (evitarlo, accettarlo, ridurlo, comparteciparlo) sviluppando interventi per allineare i rischi emersi con i livelli di tolleranza al rischio e di rischio accettabile.

• *Attività di controllo* - Devono essere definite e realizzate politiche e procedure per assicurare che le risposte al rischio siano efficacemente eseguite.

• *Informazioni e comunicazione* - Le informazioni pertinenti devono essere identificate, raccolte e diffuse nella forma e nei tempi che consentano alle persone di adempiere correttamente le proprie responsabilità.

• *Monitoraggio* - L'intero processo dell'ERM deve essere monitorato e modificato ove necessario.

Esiste un rapporto diretto tra obiettivi, ossia ciò che un'azienda si sforza di conseguire, e i componenti dell'ERM, ovvero ciò che occorre per conseguire gli obiettivi. Questo rapporto è schematizzato in una matrice tridimensionale a forma di cubo. Le quattro categorie di obiettivi – strategici, operativi, di reporting e di conformità – sono rappresentate nelle colonne verticali del cubo, gli otto componenti sono invece rappresentati nelle righe orizzontali del cubo, e le unità operative dell'organizzazione sono rappresentate dalla terza dimensione della matrice. La valutazione dell'efficacia del processo di gestione del rischio aziendale è un giudizio soggettivo, fondato sulla presenza degli otto componenti e sul loro corretto funzionamento. Pertanto, i componenti costituiscono anche dei criteri di efficacia. Così, se in un processo tutti gli otto componenti sono presenti e funzionano correttamente, ciò rappresenta una prova dell'assenza di debolezze significative e che i rischi che si vogliono affrontare sono al di sotto del livello di rischio ritenuto accettabile.

CAPITOLO 4

TIPOLOGIE DI FRODE E RELATIVI STRUMENTI DI PREVENZIONE

Frodi bancarie

Gli istituti finanziari, a fronte dello sviluppo tecnologico in cui stanno investendo, sono chiamati a fronteggiare nuovi rischi di frode dettati principalmente dall'introduzione di nuovi strumenti di pagamento digitali e dall'utilizzo dell'home & open banking da parte della propria clientela.

La prevenzione di frodi con carte di pagamento avviene generalmente attraverso: 1) Tools di machine learning e intelligenza artificiale; 2) L'implementazione di sistemi di conferma della transazione da parte del pagatore attraverso solamente device preregistrati; 3) L'introduzione di alert atti ad individuare anomalie comportamentali; 4) L'applicazione di limiti ad ammontare e frequenza di operazioni; 5) La fornitura del servizio di SMS alert per transazioni con carte e prelievi

La detection riguarda un approfondimento sulle transazioni che, a seguito del processo di monitoring, presentano indici di anomalia. L'attività consiste generalmente di: 1) Contatto con il cliente per verificare la legittimità dell'operazione; 2) Individuazione di eventuali IP di accesso usato per effettuare le transazioni (verifica con le aspettative di comportamento del cliente e la lista di device preregistrati), frequenza e geolocalizzazione delle transazioni per delimitare il perimetro della frode; 3) Quantificazione degli importi oggetto di transazioni anomale; 4) Identificazione di ATM e merchant compromessi; 5) Exit dei clienti coinvolti della frode.

Frodi assicurative

Per "*Frode assicurativa*[137]" si intende qualsiasi comportamento intenzionale posto in essere con l'inganno e in generale disonestamente da uno o più soggetti con l'obiettivo di ottenere un vantaggio personale o di terzi, causando un danno diretto o indiretto alla compagnia assicuratrice, un agente o broker o un cliente. La frode può avvenire in tutte le fasi tra la sottoscrizione della polizza ed il pagamento dell'indennizzo. I principiali fattori di rischio del settore sono i seguenti: 1) Intermediazione; 2) Asimmetria informativa; 3) Moral Hazard; 4) Adverse selection; 5) Elevata liquidità; 6) Competitività del mercato; 7) Nuovi canali di vendita; 8) Frazionamento del rischio. La frode nel business delle assicurazione alimenta un circolo vizioso. L'evento fraudolento provoca una perdita economica per l'assicurazione che risponde attraverso un aumento delle tariffe delle polizze. Dall'aumento del premio derivano un aumento della liquidità disponibile e del possibile indennizzo, fattori che rendono più probabile l'accadimento di un ulteriore caso di frode. I principali schemi di frode assicurative si suddividono in 5 tipologie differenti: 1) Frodi perpetrate da Agenti/Brokers; 2) Sottoscrizioni fraudolente; 3) Schemi r.c.a.; 4) Schemi assicurazione su beni; 5) Schemi assicurazione vita/infortuni. La frode più diffusa in ambito assicurativo è l'appropriazione indebita [138](48% dei casi). Generalmente è compiuta da soggetti esterni (65% dei casi) e riguarda il ramo danni [139]– RC auto (70% dei casi). La fase preventiva ha inizio con l'attività di background search. consiste in verifiche su terze parti riguardo criminal records, partecipazioni e cariche detenute in altre società, eventi negativi e solidità finanziaria. Successivamente si procede con la Reputational Search.

[137] Assicurazioni.Blog

[138] L'appropriazione indebita, secondo l'art. 646 del codice penale, si ha quando qualcuno si appropria del denaro o di una cosa mobile di un'altra persona, procurandosi di conseguenza un ingiusto profitto. Come nel furto, si ha il reato appena descritto quando il vantaggio è esclusivamente patrimoniale. L'appropriazione si ha ogni volta che il soggetto tratta la cosa altrui come fosse propria.

[139] Le polizze del "ramo danni" tutelano l'assicurato da eventi che possono danneggiare singoli beni del suo patrimonio (ad esempio la casa o l'auto), le sue possibilità di guadagno, il patrimonio nel suo complesso o la sua persona.

Frodi informatiche

L'Information and Communication Technology è una componente imprescindibile delle attività quotidiane di ogni organizzazione strutturata, pertanto l'integrazione sempre più spinta dei processi aziendali con gli strumenti tecnologici introduce nuovi rischi significativi di cui è essenziale tenere conto, ovvero quelli relativi alle frodi di cui questo documento si occupa. Definire con precisione il concetto di frode ICT consente inoltre di distinguerlo da altre tipologie di reato e di predisporre strategie di contrasto mirate, evitando così di incorrere nell'errore di identificare la frode ICT con qualsiasi atto criminale perpetrato utilizzando sistemi o servizi informatici.

Phishing

Il phishing è un tipo di truffa effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale.

Business e-mail compromise Attacks

In un attacco BEC, un truffatore prende di mira i dipendenti che hanno accesso alle finanze dell'azienda, di solito inviando e-mail da account di posta elettronica falsi o compromessi (un attacco di "spear phishing"). Il truffatore si spaccia per un dipendente dell'azienda o per un'altra persona di fiducia e cerca di ingannare il dipendente per fargli inviare soldi.

Toll fraud

Gli abusi e gli arbitraggi non sono classificabili come vere e proprie frodi, piuttosto come forme illecite di utilizzo di servizi senza che i comportamenti che li caratterizzano possano essere considerati illegali. Abusi e arbitraggi consistono infatti nell'utilizzo e nello sfruttamento in maniera impropria di servizi, tariffe e promozioni che l'operatore mette sul mercato, violando termini contrattuali o sfruttando a proprio vantaggio delle vulnerabilità, anche temporanee, legate a

lacune tecnologiche, errori di programmazione del software o bug dei sistemi informatici.

Malware & Ransomwhere

Un ransomware è un tipo di malware che limita l'accesso del dispositivo che infetta, richiedendo un riscatto (ransom in inglese) da pagare per rimuovere la limitazione. Ad esempio, alcune forme di ransomware bloccano il sistema e intimano l'utente a pagare per sbloccare il sistema, altri invece cifrano i file dell'utente chiedendo di pagare per riportare i file cifrati in chiaro. Inizialmente diffusi in Russia, gli attacchi con ransomware sono ora perpetrati in tutto il mondo.

Gaming fraud

Mentre le cifre esatte sono quasi impossibili da individuare, il gioco online è come minimo un'industria multimiliardaria all'anno. Con tutto quel denaro che scorre in ogni settore, diventa altamente suscettibile a frodi o furti. Ci sono due tipi principali di frodi nei pagamenti nell'industria del gioco, sebbene ci sia una serie di modi per commettere diversi tipi di frodi nei pagamenti. Le frodi "amichevoli" sono commesse dal legittimo titolare della carta di credito e la maggior parte degli altri tipi di frode sono una forma di furto d'identità.

CONCLUSIONE

Investire nella prevenzione è fondamentale per minimizzare l'esposizione al rischio reputazionale & ridurre il rischio di atti fraudolenti commessi da soggetti interni o esterni. I benefici reali si hanno nel lungo termine in quanto si saranno sviluppate strategie efficaci a limitare il verificarsi di frodi e conseguentemente la perdita economica ad essa collegata. Conseguentemente nel lungo termine si avrà la capacità di risolvere velocemente situazioni critiche; contenere le perdite; identificare le debolezze del sistema di controllo interno e gestire il rischio reputazione

INDICE DELLE TABBELLE

INDICE DELLE FONTI

1. *De Bello Gallico. B.C.2,14,1i*
2. *Allegrini M., et al., 2003*
3. *Report of the Nation*
4. *"Le Frodi Aziendali: frodi amministrative, alterazione di bilancio e computer crime. Marco Allegrini, Giuseppe D'Onza, Daniele Mancini, Stefano Garzella- Franco Angeli, 2003.*
5. "Il rischio di frode ai tempi del COVID-19", Fabrizio Santaloia e Stefano Mango, LinkedIn (https://www.linkedin.com/pulse/il-rischio-di-frode-ai-tempi-del-covid-19-fraud-risk-santaloia/?trackingId=BEKqPYcqI5546BY98x7%2FxA%3D%3D), marzo 2020*Laganà G., Gallo Riva P., Mastromarchi D., 1995*
6. Tratto da: "Frodi aziendali" Ed. Egea (2012) - Giuseppe Pogliani, Nicola Pecchiari, Marco Mariani
7. *AFCE Web Site_Missionsito dell'ACFSE "Report to the Nations" (2020).*
8. *"The Fraud Tree, occupational fraud and abuse classification system"; ACF*
9. *"Le Frodi Aziendali: frodi amministrative, alterazione di bilancio e computer crime". Marco Allegrini, Giuseppe D'Onza, Daniele Mancini, Stefano Garzella- Franco Angeli, 2003*
10. Secondo un recente studio dell'Association of Certified Fraud Examiners, una tipica organizzazione perde circa il 7% dei suoi ricavi annuali a causa delle frodi. *Tratto da: "La responsabilità amministrativa per reati penali posta a carico di società ed associazioni secondo il D. Lgs.231/01", in "Revisione Contabile" n.42/2001.*
11. *"Valutazione dei rischi e controllo interno" - S. Beretta, Milano (2004), pag. 167*
12. *"Fondamenti aziendalistici della responsabilità degli enti ai sensi del D.lgs. n. 231 del 2001" - G.B. Alberti, in Le Società, Milano (2002), Fasc.5*
13. *"La responsabilità amministrativa per reati penali posta a carico di società ed associazioni secondo il D. Lgs.231/01", in "Revisione Contabile" n.42/2001.*
14. *Sarbanes-Oxley Act*
15. Olson D. L., Wu D. D., 2008
16. PricewaterhouseCoopers, 2006
17. *Modello di organizzazione gestione e controllo ai sensi del D.LGS 231/2001*
18. PricewaterhouseCoopers, 2002
19. *Le frodi commesse attraverso carte di pagamento*-Andrea D'Andrea - Associate Partner e Stefano Mango - Senior Consultant | EY Forensics – FSO
20. Fonte: Osservatorio Crif, dicembre 2018.
21. Assicurazioni.Blog
22. Fonte: MEF, Rapporto statistico sulle frodi con carte di pagamento no. 7/2017, 2017.
23. Broccardi
24. Art. 642 c.p.
25. Banche dati (Regolamento n. 23 del 1° giugno 2016)
26. Referente antifrode (Lettera al mercato del 21 maggio 2014)
27. Indicatori e livelli di anomalia (Provvedimento n. 47 del 1° giugno 2016)
28. (Dante, Convivio, IV, XII, 3)
29. Frauds_anatomy_Anatomia_della_frode

30. Ministero della difesa_ LA CRIMINALITÀ INFORMATICA TRA IMPRESA, NUOVE TECNOLOGIE E CULTURA DIGITALICA
31. Ramzan, Zulfikar, Phishing attacks and countermeasures, in Stamp, Mark & Stavroulakis, Peter (a cura di), Handbook of Information and Communication Security, Springer, 2010, ISBN 978-3-642-04117-4.
32. Osservatori.net
33. Trend Micro.com
34. F. Cajani, G. Costabile, G. Mazzaraco, Phishing e furto d'identita digitale. Indagini informatiche e sicurezza bancaria, Milano, Giuffrè, 2008.
35. Debbie Stephenson, Spear Phishing: Who's Getting Caught? Firmex. URL consultato il 27 luglio 2014.
36. What Is 'Whaling'? Is Whaling Like 'Spear Phishing'? About Tech. URL consultato il 28 marzo 2015 (archiviato il 28 marzo 2015).
37. APWG-2020
38. Dunn John E., Ransom Trojans spreading beyond Russian heartland, TechWorld, 9 marzo 2012. URL consultato il 25 maggio 2015 (archiviato dall'url originale il 2 luglio 2014).
39. Adam Young, building a Cryptovirus Using Microsoft's Cryptographic API, in Jianying Zhou e Javier Lopez (a cura di), Information Security: 8th International Conference, ISC 2005, Springer-Verlag, 2005, pp. 389–401.
40. Ransomware: Fake Federal German Police (BKA) notice, SecureList (Kaspersky Lab). URL consultato il 10 marzo 2012 (archiviato dall'url originale il 5 febbraio 2012).
41. Police warn of extortion messages sent in their name, Helsingin Sanomat. URL consultato il 9 marzo 2012 (archiviato dall'url originale il 14 marzo 2012).
42. encyclopedia
43. TransUnion_Formerly iovation
44. Chargebacks911
45. *Treccani*
46. Rischi di riciclaggio nell e gaming Avv. Maurizio Arena, Avv. Marcello Presilla
47. Sisal https://www.sisal.com/iniziative/tutela-consumatore/sicurezza/prevenire-riciclaggio
48. https://www.gdr-online.com/articoli-giochi-online-riciclaggio-di-denaro.asp
49. https://www.gdr-online.com/articoli-giochi-online-riciclaggio-di-denaro.asp
50. *https://fiscomania.com*
51. https://razorpay.com/learn/everything-you-need-to-know-about-tackling-gaming-fraud/
52. Agari; https://docs.apwg.org/reports/apwg_trends_report_q1_2020.pdf
53. https://www.twilio.com/learn/voice-and-video/toll-fraud
54. https://frodi.clusit.it/_files/le_frodi_nella_rete.pdf
55. https://www.ildenaro.it/frodi-assicurative-perche-sono-un-danno-per-tutta-la-collettivita/
56. https://www.laleggepertutti.it/280344_truffa-e-assicurazione-ultime-sentenze
57. https://www.assiteca.it/2020/03/rc-auto-frodi-sinistri/

58. AIIA, Il ruolo dell'internal auditor nella prevenzione ed il controllo delle frodi, Milano AIIA, 2000.
59. AIIA, Position Paper D.Lgs. 231/2001 Responsabilità amministrativa delle società: modelli organizzativi, di prevenzione e controllo, Milano AIIA, 2001.
60. AIIA, Standard per la pratica professionale, Milano AIIA, 2001.
61. An investigation into fraud prevention and detenction of small business in the United States: responsibilities of auditors, managers and business owners"- Accounting Forum Marzo 2001, Vol. 25, Issue I
62. .Auditing e Servizi di Assurance, un approccio integrato. Alvin A. Arens, Randal J Elder, Mark S. Beasley. Casa editrice: Pearson Education Italia s.r.l. Anno: 2006.
63. Behaviour and the concept of Preference (Comportamento e concetto di preferenza). A. Sen. Casa editrice: Il Mulino Bologna. 1986.
64. Corporate Governance e qualità dell'informazione esterna d'impresa. G. Fiore. Giuffrè Editore. Milano. Anno: 2003
65. Frodi in azienda, il ruolo dell'internal auditor, in Amministrazione e finanza, n.13/2000. M. Nobili.
66. • Il sistema di controllo interno. Progetto Corporate Governance per l'Italia. Milano. Il Sole 24 Ore, 2002.
67. La criminalità dei colletti bianchi. Chiara Mirabella.
68. Internal Auditing. Chiave per la corporate governance. Carolyn A. Dittmeier. Casa editrice: Egea S.p.A.. Milano. Gennaio. Anno: 2008.
69. Valori, trasmissione culturale ed imprenditorialità: un'analisi empirica per l'Italia. Working Paper n.11-2009, Paolo Trevisan.
70. "Sistemi di pianificazione e controllo" di Paolo bastia, Il mulino Manuali, 2008
71. "Sistema dei controlli interni: l'organo con funzione di supervisione strategica", dal Sole 24ore di Marcello Priori, Dottore Commercialista, Studio CPAssociati e Studio Legale Guglielmetti, 2013
72. "Indirizzi per l'attuazione della normativa in materia di prevenzione della corruzione e di trasparenza nelle società controllate o partecipate del Ministero dell'Economia e delle Finanze", dal sito del Ministero dell'Economia e delle Finanze, aggiornato al 2015
73. "Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ai sensi del decreto legislativo 8 giugno 2001, n. 231" di Confindustria, marzo 2014
74. G.M. MIRABELLI, Come affrontare la complessità normativa: l'esperienza Edison, in INTERNAL AUDIT -Corporate Governance, Risk Management e Controllo Interno, La Rivista dell'Associazione Italiana Internal Auditors, anno XVIII Pubblicazione quadrimestrale n. 60 Gennaio/Aprile 2008, pp. 8 ss
75. AIIA - Associazione Italiana Internal Auditors, Corporate Governance Paper "Approccio integrato al Sistema di Controllo Interno ai fini di un'efficace ed efficiente governo d'impresa"
76. "Controlli interni. Entro aprile la relazione annuale. Lo stato dell'arte e i problemi aperti" di Ioletta Pannocchia, Direttore PROMO P.A. Fondazione, 2014
77. "L'analisi e la gestione dei rischi aziendali: un'opportunità ad alto valore aggiunto per l'impres" di Paolo Bernardini e Maasimiliano Giacchè, Milano 10 giugno 2010

78. “I sistemi per la gestione del rischio: modelli operativi, ruoli e responsabilità” di Massimo Livatino e Paola Tagliavini, SDA Bocconi, Milano, 2016
79. “Disegno e funzionamento del Sistema integrato di Controllo Interno” della Associazione Italiana Internal Auditors, Milano, 2008
80. Olson D. L., Wu D. D., 2008
81. Report of the National Commission on Fraudulent Financial Information", obtained on March 23, 2011
82. Internal control - Integrated framework ", retrieved on March 23, 2011
83. "The Trouble with COSO", March 15, 2006, accessed March 23, 2011.
84. Bertinetti G., Cavezzali E., Gardenal G., 2013, “The effect of Enterprise Risk Management implementation on the firm value of European companies”.
85. D’Arcy S., Brogan J., 2001, ”Enterprise risk management”, Journal of Risk Management of Korea 12 (1).
86. Liebenberg A., Hoyt R., 2003, “The determinants of Enterprise Risk Management: evidence from the appointment of Chief Risk Officer”, Risk management and Insurance Review 6 (1), 37