Lo sviluppo di un sistema antifrode: considerazioni programmatiche e ruolo della Security

di Umberto Saccone

Abstract

La frode rappresenta una grave minaccia per le aziende. Diversi indicatori registrano come i danni, economici ma anche reputazionali e gestionali, provenienti da questo rischio possano compromettere l'efficenza e l'efficacia di un'organizzazione nel perseguimento dei propri obiettivi di business.

La frode è un rischio. In quanto tale necessita di un dedicato sistema capace di identificare, analizzare, valutare, prevenire e in ultima istanza gestire tale fattualità. Il sistema antifrode implementato in un'azienda dovrà necessariamente includere nel proprio perimetro di azione tutte le funzioni aziendali che, in relazione alle proprie attività, abbiano necessità di rafforzare i sistemi di controllo e di monitoraggio dei rischi di business per contenere le minacce in una visione olistica. La funzione aziendale deputata al Security Risk Management può, in questo campo, essere un elemento strategico che, grazie alle sue expertise e capabilities nel campo delle indagini e delle investigazioni, è in grado di implementare corretti sistemi di fraud detection e fraud prevention.

In sintesi lo sviluppo di un sistema antifrode il più "comprehensive" possibile, e quindi capace di inglobare sinergicamente tutte le rilevanti funzioni aziendali, è ormai la chiave per contrastare fenomeni emergenti che possono arrecare ingenti danni all'azienda se non considerati unitariamente in un contesto di Enterpise Risk Management.

Profilo dell'autore

Senior Vice President Security di Eni, è laureato in Scienze Politiche, ha frequentato master sulla tutela dei dati personali, sul rapporto privacy-security, sulle infrastrutture critiche e altri relativi alla sicurezza nazionale presso il Defense Intelligence College in Washington D.C.

Già professore a contratto presso la cattedra di Criminologia e membro del comitato scientifico dell'Università Cattolica di Milano. È inoltre membro del Consiglio Scientifico del Master in Homeland Security presso l'Università Campus Biomedico di Roma, della Technical Advisory Board OSDIFE Osservatorio sulla Sicurezza e Difesa CBRNe, del Comitato Scientifico del corso di formazione per "Professionista della Security Aziendale" dell'Università Vita-Salute San Raffaele, del Comitato Scientifico della rivista *Antifurto & Security*, nonché di numerosi "fora" tra le principali Oil Company tra cui il G7 e l'OCSC. È relatore sui temi di security presso Istituzioni pubbliche e private e presso Istituti di formazione. Autore di numerosi articoli e autore del libro *La security aziendale nell'ordinamento italiano* nonché coautore del libro *Uno sguardo sul mondo 2.0*.

Ha iniziato la propria carriera nel 1974 nell'Arma dei Carabinieri. A partire dal 1981, ha ricoperto numerosi incarichi in Italia e all'estero presso gli Organismi per l'informazione e la sicurezza. Nel 2006, congedatosi dall'Amministrazione militare ha assunto l'incarico di Direttore della Security di Eni. È Commendatore Ordine al Merito della Repubblica Italiana.

La descrizione delle fenomenologie fraudolente, nonché delle modalità e dei contesti in cui le stesse si manifestano, richiede un approccio multidisciplinare come in pochi altri campi di osservazione. Come dicono gli americani, nel *fraud management* non esiste un unico *body of knowledge*, ma un approccio organico che comprende aspetti umani, organizzativi, normativi, nonché una conoscenza delle tecnologie e delle fenomenologie sociali e culturali.

La frode, nelle sue diverse forme, si manifesta in ogni contesto e situazione ove c'è qualcuno che possiede un valore e qualcun altro che ne vuole ottenere il possesso senza pagare alcun "prezzo", utilizzando tecniche volte a eludere ostacoli che si frappongono tra lui e il bene senza l'impiego di mezzi "violenti" e magari facendo ricadere su altri (inclusa la vittima) la responsabilità delle proprie azioni.

La frode è un reato di opportunità, nel senso che si manifesta laddove le "barriere" non esistano o non siano sufficientemente efficaci.

La frode è caratterizzata da una forte componente umana e colpisce indifferentemente persone giuridiche e fisiche a prescindere dalla loro localizzazione, natura e status economico e sociale.

Nelle aziende la frode è finalizzata alla sottrazione di tutto ciò che possa avere un valore commerciale ed economico e può essere perpetrata da soggetti interni ed esterni all'azienda attraverso differenti tecniche.

Per tal motivo, è necessario che all'interno delle organizzazioni aziendali sia data una corretta collocazione delle responsabilità del *fraud management* come componente del sistema di protezione degli asset aziendali.

Nelle moderne organizzazioni, questo ruolo trova una sua naturale collocazione nell'area della Security, che per cultura, approccio e competenza può garantire una efficace attività di *fraud management* e prevenzione, o del *risk management*.

Le frodi a danno delle aziende

La frode risulta particolarmente pericolosa per le realtà aziendali, principalmente per le conseguenze economiche che ne derivano (sebbene non debbano essere sottovalutati anche i danni reputazionali e di immagine).

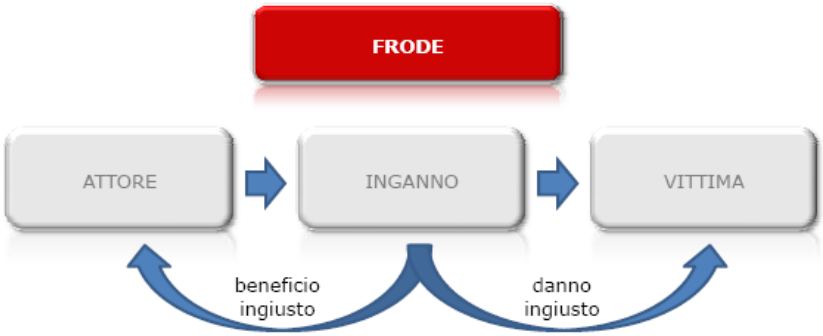
Per frode aziendale s'intende "qualsiasi atto illegale, commesso da persone interne o esterne all'azienda, caratterizzato da condotte quali il raggiro, l'artificio, l'occultamento, l'abuso di fiducia. Le finalità sono di ottenere illecitamente denaro, beni o servizi, di evitare un pagamento o la perdita di servizi, oppure procurarsi ingiusti vantaggi personali o aziendali"[1].

"Gli elementi costitutivi della frode sono:

[1] Catalano, Silvia. *Lezioni antifrode per l'Internal Audit*. Rivista Internal Audit, Gennaio/Aprile 2010. p. 4.

- l'attore: il soggetto attivo che compie l'atto fraudolento;
- la vittima: il soggetto passivo che subisce la frode;
- l'inganno: il comportamento, azione o atto teso a raggirare la vittima della frode;
- l'ingiusto guadagno per l'attore e il danno patrimoniale per gli stakeholder.[2]"

La frode si sviluppa quindi sulla base dell'interazione tra attore e vittima, caratterizzata dall'inganno da parte dell'attore nei confronti della vittima. Lo schema dell'attività fraudolenta può essere efficacemente ripreso dal grafico sviluppato sulla base di quello presentato nel volume *Le frodi aziendali*.[3]



La frode. Aspetti normativi e concettuali di rilevanza per le imprese

Nella lingua italiana, il dizionario fornisce la seguente definizione di frode: "Atto o comportamento diretto a ledere con l'inganno un diritto altrui; in diritto penale, il termine *frode* indica una serie di condotte caratterizzate da modalità elusive previste come reato dal codice o dalle leggi speciali (frode in commercio, frode fiscale, frode alla legge, frode pia, frode processuale). Più in generale, si può definire frode qualsiasi inganno, artificio o astuzia malvagia con cui si sorprende l'altrui buona fede"[4].

La frode consta di due elementi distintivi: l'intento di conseguire un risultato che altrimenti non si sarebbe realizzato (almeno non in quella misura) e la concretizzazione dell'intento attraverso inganni, astuzie o raggiri. Gli articoli rilevanti del codice penale da prendere in considerazione sono sostanzialmente inerenti al reato di truffa e ad alcune fattispecie specifiche come la frode informatica, la frode assicurativa, l'insolvenza fraudolenta.

La truffa è un reato previsto dall'art. 640 del codice penale, ai sensi del quale chiunque, con artifizi o raggiri, inducendo taluno in errore, procuri a sé o ad altri un ingiusto profitto con altrui danno, viene punito secondo quanto previsto dall'articolo. È un reato a dolo generico e di evento, cioè si consuma nel momento della verifica dell'evento dannoso per la vittima e

[2] *Ibidem.*
[3] Allegri, Marco et al. *Le frodi aziendali. Frodi amministrative, alterazioni di bilancio e computer crime*. p. 14.
[4] *Vocabolario Treccani*.

proficuo per il reo. È perseguibile a querela di parte a meno che non si verifichi una delle circostanze aggravanti previste dall'art. 61 codice penale, nel qual caso è perseguibile d'ufficio.

Vi sono due particolari circostanze aggravanti del reato di truffa, al verificarsi delle quali il reato è parimenti perseguibile d'ufficio:

- se la truffa è a danno dello Stato o di altro ente pubblico;
- se è commessa facendo nascere nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dover eseguire un ordine dell'autorità.

Inoltre, sono presenti alcune fattispecie particolari, alcune delle quali denominate frode. In particolare:

- Art. 640-bis: truffa aggravata per il conseguimento di erogazioni pubbliche. La pena è la reclusione da uno a sei anni e si procede d'ufficio se il fatto di cui all'articolo 640 riguarda contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o della Comunità Europea.
- Art. 640-ter: frode informatica. Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o a esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito ai sensi dell'articolo.
- Art. 641: insolvenza fraudolenta. Chiunque, dissimulando il proprio stato d'insolvenza, contrae un'obbligazione col proposito di non adempierla è punito, a querela della persona offesa, qualora l'obbligazione non sia adempiuta, ai sensi dell'articolo.
- Art. 642: frode assicurativa. Fraudolenta distruzione della cosa propria e mutilazione fraudolenta della propria persona. Chiunque, al fine di conseguire per sé o per altri il prezzo di un'assicurazione contro infortuni, distrugge, disperde, deteriora od occulta cose di sua proprietà è punito … Alla stessa pena soggiace chi, al fine predetto, cagiona a sé stesso una lesione personale, o aggrava le conseguenze della lesione personale prodotta dall'infortunio.

Appaiono rilevanti anche alcuni articoli del codice civile che disciplinano la materia. Di seguito si espongono gli articoli di particolare interesse per declinare il concetto di frode e comprenderne pienamente le caratteristiche:

- Art. 2041. Azione generale di arricchimento. Chi, senza giusta causa, si è arricchito ai danni di un'altra persona è tenuto, nei limiti dell'arricchimento, a indennizzare quest'ultima della corrispettiva diminuzione patrimoniale. Qualora l'arricchimento

abbia per oggetto una cosa determinata, colui che l'ha ricevuta è tenuto a restituirla in natura, se sussiste ancora al tempo della domanda.

- Art. 2043. Risarcimento per fatto illecito. Qualunque fatto doloso o colposo, che cagiona un danno ingiusto, obbliga colui che ha commesso il fatto a risarcire il danno.

Si vede quindi come il legislatore abbia inquadrato la frode in fattispecie di reato specifiche, attribuendo, tuttavia, a queste norme un'efficacia ridotta laddove la vittima, che non sia ente pubblico o non ricada nei casi denunciati d'ufficio, non proceda con regolare querela verso il frodatore.

Al di fuori degli enunciati articoli, in Italia, come del resto in Europa, non è a oggi attivo uno specifico impianto normativo a eccezione della fattispecie dei reati informatici (Convenzione di Budapest) e nelle esperienze anglosassoni con riferimento al *Fraud Act* emanato nel Regno Unito nel 2006.

La convenzione di Budapest [5]

La Convenzione di Budapest è il primo trattato internazionale sulle infrazioni penali commesse via internet e su altre reti informatiche, e tratta in particolare le violazioni dei diritti d'autore, la frode informatica, la pornografia infantile e le violazioni della sicurezza della rete. Contiene inoltre una serie di misure e procedure appropriate, quali la perquisizione dei sistemi di reti informatiche e l'intercettazione dei dati.

Il suo obiettivo principale, enunciato nel preambolo, è perseguire una politica penale comune per la protezione della società contro la cibercriminalità, in special modo adottando legislazioni appropriate e promuovendo la cooperazione internazionale.

Il *Fraud Act*

Nel 2006 la Gran Bretagna ha varato una speciale normativa, il *Fraud Act*[6], volto alla definizione e punizione di questa tipologia di attività nelle sue varie forme e applicazioni.

Tra le previsioni della norma, è interessante notare come siano state individuate principalmente tre tipologie di frode:

[5] Convenzione sulla criminalità informatica: <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ITA&NT=185> (ultima consultazione 2014-02-21).

[6] UK Fraud Act 2006. <http://www.legislation.gov.uk/ukpga/2006/35/contents> (ultima consultazione 2014-02-21).

- Frode per falsa rappresentazione: nei casi in cui una persona effettua una rappresentazione di un fatto o una legge, in maniera implicita o esplicita, che sa essere falsa o fuorviante.

- Frode per non rivelazione di informazioni: nel caso in cui una persona non riveli delle informazioni in violazione di un obbligo di legge.

- Frode per abuso di posizione: nei casi in cui un soggetto che riveste un ruolo professionale che comporti un dovere di tutela degli interessi finanziari di un altro soggetto abusi della propria posizione, inclusi i casi di omissione.

In tutti e tre i casi vi deve essere una condotta disonesta posta in essere da un soggetto nei confronti di una parte offesa, perpetrata con l'intento di trarre per sé o altri un ingiusto guadagno, così facendo cagionando una perdita alla parte offesa.

Le esperienze oltre oceano

Altri ordinamenti, a esempio quello statunitense, prevedono una definizione della frode maggiormente flessibile e omnicomprensiva. Nel predetto ordinamento, infatti, il crimine di *fraud* è costituito, così come stabilito dalla Corte Suprema della Carolina del Sud nel 2009[7], da nove elementi:

1. la rappresentazione di un fatto esistente;
2. la sua falsità;
3. la sua materialità;
4. la conoscenza, da parte dell'attore, della falsità del fatto;
5. l'intento dell'attore di incidere sulla vittima;
6. l'ignoranza da parte della vittima della falsità del fatto;
7. la convinzione della vittima della buona fede e della veridicità del fatto portato dall'attore;
8. il diritto della vittima di basarsi sul fatto riportato dal soggetto;
9. il danno che la vittima ha in conseguenza della frode.

[7] South Carolina Judicial Department. Supreme Court of South Carolina. Casi Morlan vs Kelly (2009) e Schnellmann vs Roettger (2006). "…(*stating a cause of action for fraud requires the following elements: (1) a representation; (2) its falsity; (3) its materiality; (4) knowledge of its falsity or a reckless disregard for its truth or falsity; (5) intent that the representation be acted upon; (6) the hearer's ignorance of its falsity; (7) the hearer's reliance on its truth; (8) the hearer's right to rely thereon; and (9) the hearer's consequent and proximate injury*).

Corporate fraud e *white-collar crime*

Parlare di frodi in azienda obbliga a operare alcune classificazioni tra le quali, la principale, è quella tra le tipologie fraudolente ove l'azienda è "vittima" di frode e ove invece l'azienda stessa è utilizzata come strumento o mezzo per perpetrare il delitto.

Nella prima fattispecie ricadono tutte le forme dei *white-collar crimes*, dove ad agire contro l'azienda sono organizzazioni o singoli in varie forme e con diverse tecniche. Nella seconda categoria siamo di fronte alle tipologie dei *corporate crimes*.

Tipici *white-collar crimes* sono le bustarelle e la corruzione tra manager e staff, insider trading, crimini informatici, violazione di copyright e segreti industriali, riciclaggio, furto di dati e informazioni personali, falsificazione, *Ponzi scheme*.

I *corporate crimes*, che partono a volte da interventi della struttura aziendale (in termini di attribuzioni di responsabilità e/o abusi di potere e dei meccanismi di governo e di controllo) al fine di assecondare l'intento fraudolento, sono spesso organizzati e perpetrati da figure apicali dell'azienda, e da membri del consiglio di amministrazione.

Come *corporate crimes* possono essere classificati false comunicazioni sociali, pratiche commerciali fraudolente, scalate "ostili", liquidazione fraudolenta di attività, falsi in bilancio.

Frodi interne e frodi esterne

Un'altra classificazione va fatta in termini di frode esterna e interna a seconda che il soggetto che agisce contro l'azienda stia operando all'esterno o all'interno dell'organizzazione (non necessariamente dello spazio fisico).[8]

Nella maggior parte dei casi, le frodi vedono una "combinazione tra attacchi esterni portati con la complicità di insider."

Il triangolo della frode

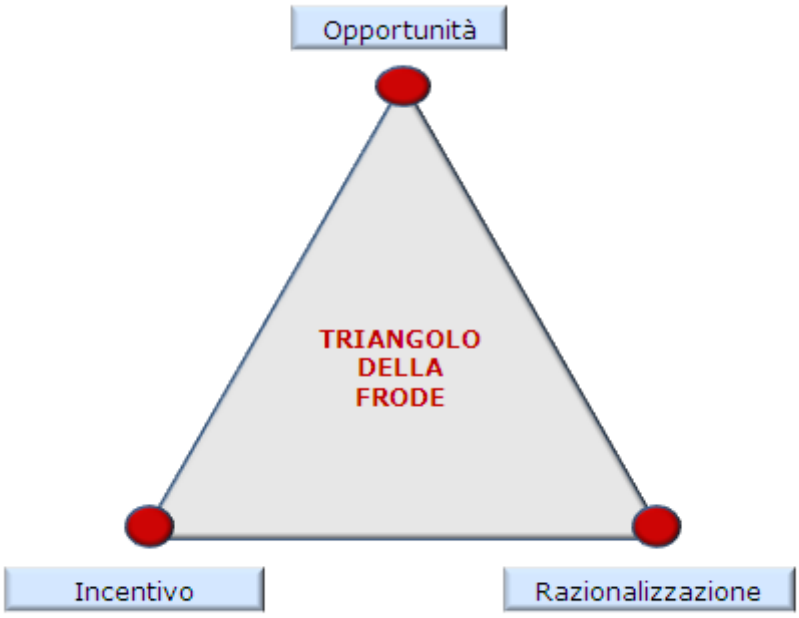
Donal R. Cressey ha pubblicato, nel 1973, quella che oggi è la teoria di riferimento per spiegare i presupposi al verificarsi della frode in azienda: il *Fraud Triangle o triangolo di Cressey*.

Nel triangolo della frode[9], gli apici rappresentano i presupposti al verificarsi della frode:

- l'incentivo (pressione) alla commissione della frode (pressioni finanziarie, professionali, ecc.);

[8] Si pensi al caso di un consulente o personale esterno che abbia accesso ai locali aziendali.
[9] Donald R. Cressey, 1973.
Magri, Michele. *Presentazione Fraud Examination nel settore Finance*. ACFE Italy Chapter, 18 febbraio 2010.
Catalano, Silvia. *Lezioni antifrode per l'Internal Audit*. Rivista Internal Audit, Gennaio/Aprile 2010. p. 5

- l'opportunità di commettere la frode (mancanza o fallacità dei sistemi di controllo, meccanismi aziendali che permettono la commissione della frode);
- la razionalizzazione della frode, in altri termini la giustificazione che l'attore si dà per la commissione dell'evento fraudolento ("in fondo non danneggio nessuno", "l'azienda se lo merita", ecc.).



La teoria è stata sviluppata con un ardito ma efficace riferimento al triangolo del fuoco, che rappresenta, invece, i presupposti allo scoppio di un incendio e l'utilizzo di questo schema per identificare la tecnica più efficace per il suo spegnimento.

Nella teoria del triangolo del fuoco si fa riferimento ai tre elementi principali, ossia l'ossigeno, l'elemento combustibile e la fonte di calore: per spegnere un incendio è sufficiente agire su uno solo di questi tre elementi.

Analogamente per agire efficacemente in chiave di prevenzione delle frodi, sarebbe sufficiente intervenire su almeno uno dei tre elementi tra motivazione, opportunità e incentivo.

Un fenomeno complesso da misurare

A eccezione delle frodi informatiche, in Europa non ci sono statistiche attendibili circa la natura e le dimensioni del fenomeno e dei suoi impatti sulle aziende.

A livello internazionale ci sono invece diversi studi[10] da cui trarre interessanti informazioni sulle diverse tipologie di frode e sulle dimensioni del fenomeno su scala globale.

Particolarmente interessante è il rapporto *Global Fraud Report*, elaborato da Kroll Advisory Solutions, con il supporto dell'Economist Intelligence Unit, inerente all'impatto delle attività di frode sulle aziende. Lo stesso, condotto su 839 imprese di diverse regioni mondiali[11], ha rilevato come il 61% di queste abbia registrato eventi di frode, di cui i 2/3 (67%) consistenti in frodi interne. Inoltre, il rapporto ha evidenziato come, in media, il costo degli eventi di frode sia pari a 0,9% dei ricavi delle imprese.

I principali eventi fraudolenti registrati dalle imprese intervistate sono il furto di asset fisici e di informazioni, il conflitto di interessi del management, le frodi provenienti da venditori, fornitori o dal procurement, le frodi finanziarie interne, la corruzione. Forte elemento di preoccupazione risultano le frodi informatiche, anche nella forma di cyber attacchi.

Un'azienda, quindi, non può fare a meno di implementare un programma antifrode, nella forma di policy e procedure. Gli elementi fondamentali da implementare in azienda, secondo uno studio di Silvia Catalano di Banca Generali[12], sono:

- assessment dei fattori che determinano la frode (analisi e valutazione dei rischi di frode per l'azienda);
- definizione di un sistema di controllo interno (audit, organismo di vigilanza, ecc.);
- creazione di un ambiente di controllo e commitment da parte del top management;
- adozione di un codice etico per favorire l'instaurarsi di una cultura aziendale contro i comportamenti fraudolenti;
- adozione di hotline e sistemi di *whistleblowing* che permettono di denunciare in modo anonimo i fenomeni di frode;
- gestione delle assunzioni e incentivazione del personale. Tale processo deve prevedere la verifica del *background* di un candidato in fase di assunzione e l'adozione di una politica di premi e promozioni per il personale più fedele;
- promozione di processi per l'investigazione delle frodi;
- proceduralizzazione delle attività investigative;
- certezza della sanzione;
- miglioramento continuo;
- monitoraggio continuo dei rischi di frode.

[10] Vedi ACFE (*Report to the Nation*), Deloitte, Protivity, KPMG, Ernst Young, Symantec.
[11] Europa 28%, America del Nord 26%, Asia-Pacifico 24%, America Latina 13%, Medio Oriente 10%.
[12] Catalano, Silvia. *Lezioni Antifrode per l'Internal Audit*. Rivista Internal Audit, Gennaio/Aprile 2010. p. 6-7.

Nel prosieguo si andrà ad analizzare l'articolazione di un sistema di gestione del rischio di frode, sulla base delle *best practices* a livello internazionale. Si vedrà come tutti questi elementi indicati da Catalano vengono inclusi nelle varie parti fondanti un programma di *fraud governance* a livello aziendale.

In conclusione, quindi, la frode rappresenta una fonte di rischio molto rilevante per le aziende. Si tratta, infatti, di un rischio operativo che investe molteplici aspetti della realtà aziendale. È stato ampiamente dimostrato[13] che le aziende che intraprendono percorsi proattivi nell'implementazione di meccanismi volti a prevenire il verificarsi di comportamenti fraudolenti, ne registrano un minor numero di casi e, ricevendo minori danni, conseguentemente risultano maggiormente tutelate.

In questo senso, bisogna sempre ricordare che la frode rappresenta un rischio: in quanto tale, deve essere gestito attraverso opportuni sistemi di *risk management*. La sola adozione di un modello di gestione, però, non è sufficiente. La definizione e introduzione di un programma di *fraud governance* permette di mitigare il livello di rischio, grazie all'effetto di deterrenza, ma non assicura di per sé una soluzione del problema.

Un serio e organico programma di contrasto ai fenomeni illeciti, per essere davvero efficace, deve essere adottato in modo esteso dalla struttura organizzativa e deve essere costantemente aggiornato per riflettere le continue evoluzioni degli scenari esterni e interni all'impresa. In questo senso, riprendendo il Modello 231, si può affermare che il sistema deve essere adottato ed efficacemente implementato.

Si ricordi, inoltre, che la frode rappresenta, oltre che un rischio per l'azienda, anche un reato ai sensi della legislazione italiana. In questo senso, un programma di *fraud governance* aziendale, non solo rappresenterebbe uno strumento per la protezione dei beni, materiali e immateriali, dell'impresa, ma altresì un meccanismo esimente della responsabilità dell'azienda nel caso in cui risorse interne (in posizione apicale o subordinata) effettuino un reato di frode a vantaggio della stessa (art. 640 c.p. truffa, art. 640-bis truffa aggravata per erogazioni pubbliche, art. 640-ter frode informatica, art. 642 frode assicurativa). Svilupperemo qui le considerazioni fondamentali per l'implementazione di un progetto di realizzazione di un programma di *fraud governance* efficace all'interno dell'azienda, secondo alcuni principi contenuti in documenti e linee guida internazionali.

La realizzazione di un programma di *fraud governance* aziendale

A seguito degli enormi scandali accaduti a grandi aziende americane (si pensi ai casi Worldcom e Enron) negli USA è stata pubblicata la *Sarbanes-Oxley Act* del 2002[14], che, oltre a rappresentare il punto di riferimento per l'introduzione, a livello internazionale, di regolamentazioni sulla governance aziendale, (il SOX delinea alcuni fondamentali principi di

[13] Si vedano i report di UK Financial Services Authority e National Fraud Authority.
[14] <http://www.soxlaw.com> (ultima consultazione 2014-02-21).

gestione, di accounting e di corporate governance), è il punto di partenza su cui sviluppare programmi di *fraud governance* aziendale.

Lo standard di riferimento a livello internazionale per l'implementazione di un sistema di gestione del rischio di frode aziendale è la guida *Managing the Business Risk of Fraud: A Practical Guide*[15], sviluppata da un gruppo di lavoro internazionale e sponsorizzata dall'*Institute of Internal Auditors*, dal *The American Institute of Certified Public Accountants* (AICPA) e dall'*Association of Certified Fraud Examiners* (ACFE).

Questa Guida inoltre è sostenuta da diverse organizzazioni, tra le quali:

- l'*Institute of Management Accountant;*
- *l'Association of Chartered Certified Accountants;*
- *la Society of Corporate Compliance and Ethics;*
- *la Chartered Accountants of Canada.*

Il documento, quindi, risulta particolarmente utile per accompagnare le aziende nel delineare gli elementi principali costitutivi di un efficace sistema di gestione del rischio di frode, in quanto sviluppata sulle *best practices* organizzative e gestionali, sul framework CoSO, e su varie normative (perlopiù statunitensi). La Guida descrive un modello di gestione basato sui seguenti cinque principi:

1. Un programma di *fraud risk governance* deve essere attivo come parte di una struttura di governance di una organizzazione. Il programma deve prevedere più policy per garantire il coinvolgimento del top e del senior management.

2. L'esposizione dell'organizzazione al rischio di frode dovrebbe essere periodicamente valutato al fine di identificare gli schemi e gli eventi che necessitano di essere mitigati.

3. Dovrebbero essere sviluppate e implementate tecniche di prevenzione di potenziali eventi di frode, per mitigare i possibili impatti sull'organizzazione (*fraud prevention*).

4. Dovrebbero essere sviluppate e implementate tecniche di rilevazione al fine di scoprire gli eventi di frode (*fraud detection*), quando le misure di prevenzione o di mitigazione del rischio falliscono.

5. Ogni organizzazione deve implementare un sistema di reporting e di flussi comunicativi che fungano da input alle attività di investigazione e che aiutino ad attivare azioni correttive.

[15]<http://www.acfe.com/products.aspx?id=4294971162> (ultima consultazione 2014-02-21).

La governance del rischio di frode

Il primo aspetto fondamentale è lo sviluppo di un impianto organizzativo atto a gestire, in maniera diretta, il rischio di frode. Il sistema di gestione può essere sviluppato su una serie di componenti alquanto articolate, comuni in generale ai sistemi di gestione improntati alla qualità.

Le componenti fondamentali del sistema, sono:

- Impegno del CdA e del top management: all'interno del CdA 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. 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. Il CdA deve assumersi la responsabilità del monitoraggio della efficacia dei processi antifrode e garantire adeguate risorse a quest'area.

- Concretezza: il programma di *fraud governance* deve prevedere un insieme di documenti scritti, dove obiettivi, attribuzioni di responsabilità, piano di comunicazione, incentivazione, azioni disciplinari e legali, sono definiti in modo chiaro e portati a conoscenza del personale a tutti livelli attraverso specifiche e periodiche attività di formazione e assessment.

- Consapevolezza: coerentemente con la definizione degli obiettivi aziendali in termini di politica di gestione dei rischi, il programma deve prevedere un'attività costante di monitoraggio delle tipologie di rischio, probabilità e rilevanza, efficacia delle misure adottate per la loro prevenzione e mitigazione dei livelli di rischio.

- Informazione/accettazione comportamento antifrode: va definito un piano di formazione e informazione attraverso il quale il management, i dipendenti, e in genere tutte le risorse coinvolte nell'organizzazione aziendale prendono ufficialmente visione del documento che delinea il codice di comportamento accettandone i contenuti.

- Conflitto d'interessi: dovrebbe essere sviluppato un processo che faccia emergere e consenta di prevenire e gestire possibili conflitti di interesse di dipendenti, dirigenti e agenti dell'organizzazione.

- Valutazione del rischio di frode: dovrebbe essere sviluppato un processo continuo di analisi e valutazione del rischio di frode 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 *in primis*) sull'azienda.

- Procedure di reporting e *whistleblowing*: si dovrebbero definire piani di comunicazione e procedure che permettano di riportare alle funzioni competenti eventi fraudolenti e comportamenti sospetti.

- Processo di investigazione: le organizzazioni dovrebbero sviluppare processi investigativi opportunamente proceduralizzati, che riescano a intervenire a seguito del sospetto e della segnalazione di un fatto considerato fraudolento.

- Azioni correttive: dovrebbero essere sviluppate, anche in funzione di deterrenza, delle procedure di azione correttiva che sanzionino e prevedano conseguenze per l'attore che effettua una frode (sanzioni amministrative, risoluzione di contratto, denuncia, ecc.).

- 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.

- Valutazione e miglioramenti del processo antifrode: ispirandosi agli standard di qualità, il processo complessivo di *fraud management* dovrebbe essere valutato in termini di efficienza ed eventualmente migliorato nel suo complesso.

- Analisi del contesto normativo: tutte le attività ricomprese in un programma di *fraud governance* 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.

Valutazione del rischio di frode

Un processo chiave di un efficace programma di *fraud governance* aziendale è il processo di valutazione del rischio di frode che può essere assimilato ai principi generali del risk management (*fraud risk assessment*) per la valutazione di altre tipologie rischi. Lo svolgimento di questa attività può essere condotta da diverse funzioni aziendali, o essere parte di un più ampio processo di *enterprise risk management*, se presente nell'organizzazione.

Questo processo diventa più efficace quanto più ampio è il coinvolgimento delle diverse funzioni aziendali in un *fraud risk assessment team* che sviluppa il processo di valutazione del rischio di frode. In relazione alla natura della frode, il *team* sarà quindi composto da diverse funzioni aziendali, coinvolte nel processo di risk management, al fine di disporre di persone con le necessarie abilità, competenze e conoscenze.

Si potrà quindi avere un gruppo di lavoro (anche virtuale) con figure professionali di:

- contabilità e finanza;
- unità di business;
- risk management;
- security;

- legale;
- internal audit;
- IT;
- HR;
- *sales*;
- consulenti e *fraud specialist* interni e esterni.

Il processo si articola nelle fasi di identificazione dei rischi, valutazione e predisposizione delle azioni correttive.

- Identificazione dei rischi di frode: si identificano le fattispecie di frode rilevanti che possono interessare l'organizzazione, identificando, al contempo, gli schemi fraudolenti e i possibili scenari, gli incentivi, le motivazioni e le opportunità di commettere una frode nell'organizzazione.

- Valutazione del rischio di frode: si valutano i rischi di frode identificati, in particolare con riguardo alla probabilità di accadimento e ai possibili impatti, valutandone, quindi, la rilevanza per l'organizzazione.

- Predisposizione delle azioni di risposta ai rischi di frode considerati rilevanti e probabili: si identificano e pianificano le possibili azioni di risposta, in chiave costi-benefici, da intraprendere per mitigare il rischio di frode.

Fraud prevention e *fraud detection*

Al fine di minimizzare la possibilità di accadimento di eventi fraudolenti si dovrebbero sviluppare e implementare dei processi e delle procedure di prevenzione delle frodi (*fraud prevention*) e di rilevazione degli eventi sospetti o accaduti (*fraud detection*). La *fraud prevention* riguarda le procedure, le *policies*, 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 a livello internazionale 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, *exit interviews* dei dipendenti e dirigenti che lasciano l'organizzazione per valutare la loro opinione/conoscenza di fatti o comportamenti fraudolenti di colleghi o 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.

Fraud Detection

Un ulteriore sistema da implementare riguarda la *fraud detection*. Si tratta di tecniche e metodologie che permettono di rilevare la commissione di attività fraudolente, valutando, al contempo, la efficacia delle misure di mitigazione previste.

Controllo e monitoraggio

Nell'istituzione di un programma di *fraud governance* aziendale, fondamentali risultano le attività volte al controllo e al monitoraggio costante nonché alla definizione di un piano di comunicazione e reporting aziendale.

Accanto alle metodologie classiche di *fraud auditing*, consistenti principalmente in verifiche su base campionaria o basate su rilevazione di alert da sistemi di ethic-line e processi di *whistleblowing*, oggi si possono utilizzare nuove tecniche e strumenti basati su modelli logico/matematici in grado di elaborare e analizzare enormi quantità di dati: attraverso specifici algoritmi, questi sistemi sono in grado di elaborare schemi di segnalazione e prevenzione di possibili attività fraudolente. Questi strumenti sono indispensabili in aziende moderne, grazie alla possibilità che offrono di integrare e analizzare i dati dei differenti sistemi informativi e gestionali aziendali.

In sintesi, quindi, tecnologie avanzate permettono di sviluppare sistemi antifrode di *fraud prevention* e *fraud detection*. Per essere efficaci, queste indagini devono essere supportate da modelli di *data mining,* ovvero da "modelli di estrazione dati idonei ad aggregare, collegare o associare informazioni provenienti da sistemi informativi diversi ed eterogenei"[16].

Il *data mining* viene definito come "il processo che utilizza intelligenze statistiche, matematiche, artificiali e tecniche di *machine learning* al fine di estrarre e identificare informazioni utili e conseguentemente ottenere conoscenza da un grande database"[17]. Un'altra definizione afferma che "il *data mining* utilizza diverse tecniche al fine di ricercare

[16] Bedarida, Maurizio. *Utilizzo delle tecnologie avanzate di fraud prevention e di fraud detection*. Diritto 24, <http://fiere24.ilsole24ore.com/law24/avvocatoAffari/professioneLegale/2011/11/utilizzo-delle-tecnologie-avanzate-di-fraud-prevention-e-di-fraud-detection.html> (ultima consultazione 2014-02-21).
[17] Frawley, W.J. et al. *Knowledge discovery in databases: An overview*. AI Magazines 13, 1992. pp. 57-60.

fra grandi quantità di dati e identificare relazioni e connessioni passate, estrarre regole di decisione o costruire modelli predittivi"[18] .

Come affermato da Maurizio Bedarida[19], al fine di sviluppare un sistema di *data mining*, è necessario sviluppare specifiche capacità, e, in particolare, implementare delle metodologie che garantiscono di:

- assicurare la qualità del dato in origine;
- assicurare la normalizzazione delle informazioni;
- definire le correlazioni e il modello logico/matematico più efficiente per estrarre informazioni in grado di individuare, con il minor numero di errori (falsi positivi e negativi) il fenomeno fraudolento da prevenire e/o rilevare;
- definire i criteri di controllo sull'efficacia del modello applicato;
- assicurare la qualità del dato inteso come unificazione della semantica delle varie tipologie di dati da sottoporre al processo di *data mining*. Il dato deve rispecchiare la qualità sintattica e deve essere affidabile.

Bedarida rileva come il secondo aspetto necessario alla definizione del modello di *data mining* sia la normalizzazione del dato. Questa operazione è volta a uniformare la semantica e la sintassi delle diverse informazioni al fine di poter farle elaborare e riconoscere dall'applicativo di *data mining*.

Le metodologie menzionate dall'autore per le attività di *fraud prevention* e di *fraud detection* sono:

- i *link* o *pattern analysis*: si tratta di ricerca di associazioni e interconnessioni tra gruppi di eventi e/o di persone;
- i *geometric clustering*: sotto-insieme del precedente modello, in cui i raggruppamenti sono funzioni di distanze geometriche; sia le *link pattern analysis* che i *geometric clustering* sono spesso denominati social network *analysis*, in quanto permettono di identificare le interconnessioni tra diversi avvenimenti-fattori e ricostruirne il nesso causa-effetto;
- *machine learning*: modelli auto-apprendenti che modificano i propri parametri in funzione delle variazioni nel tempo dei dati esaminati, vengono generalmente utilizzati per analizzare database con grandi quantità di dati e rinvenire le reciproche relazioni fra essi. Gli strumenti di *machine learning* sono estremamente utili per la

[18] Gray, G. e Debreceny, R. *The Application of Data Mining to Fraud Detection in Financial Statement Audits*. 3 dicembre 2006, p. 4.
[19] Bedarida, Maurizio. *Utilizzo delle tecnologie avanzate di fraud prevention e di fraud detection*. Diritto 24, http://www.diritto24.ilsole24ore.com/avvocatoAffari/professioneLegale/2011/11/utilizzo-delle-tecnologie-avanzate-di-fraud-prevention-e-di-fraud-detection.html> (ultima consultazione 2014-02-21).

predisposizione di modelli di prevenzione essendo in grado di correlare centinaia di migliaia di eventi, definendone le dinamiche e potendone quindi prevedere gli accadimenti;

- *neural networks*: sistemi particolari di auto-apprendimento derivati dalla teoria delle reti neuronali. Sono gli strumenti più avanzati, che simulano il processo neuronale di apprendimento e memorizzazione dell'essere umano. Anche gli strumenti sviluppati sulle reti neuronali sono estremamente efficaci per lo sviluppo di sistemi che riescano a "prevedere" la commissione di attività fraudolente.[20]

Sharma e Panigrahi[21] sviluppano una trattazione che prevede sei tipologie di classi di applicazione di *data mining*:

- *classification*: prevede la costruzione e l'utilizzo di un modello al fine di poter categorizzare i dati e, attraverso ciò, prevedere la categoria di appartenenza di dati sconosciuti. Per fare ciò si identificano e stabiliscono delle relazioni e schemi comuni ai dati classificando in relazione a essi le informazioni e i dati a disposizione in classi o concetti;

- c*lustering*: utilizzato per effettuare una partizione di oggetti in gruppi concettuali inediti (i cluster), per caratteristiche gli oggetti all'interno dei cluster sono molto simili, ma fra un cluster e un altro vi è grande differenza. L'analisi *cluster* scompone i dati in gruppi dissimilari al fine di far sì che i dati in un gruppo siano il più simili possibile e che i dati contenuti fra i gruppi siano il più differenti possibile.

- *prediction*: stima valori futuri su base numerica e ordinale sulla base dello schema di un set di dati;

- *outlier detection*: misura la "distanza" tra i dati al fine di individuare quei dati che sono molto differenti dai set predeterminati. Quei dati che hanno caratteristiche diverse dai set predeterminati vengono denominati *outlier*;

- *regression*: è un metodo statistico che rivela le relazioni tra una o più variabili indipendenti e una variabile dipendente. Spesso questa tecnica viene utilizzata nelle ricerche di evidenza empirica come *benchmark*;

- *visualization*: metodologia che converte le complicate caratteristiche e schemi di dati in presentazioni grafiche facilmente comprensibili.

Sulla base di queste sei tipologie, gli autori menzionano otto tecniche di *data mining* specificamente destinabili all'applicazione in funzione antifrode[22]:

[20] Ibidem. Si rimanda all'articolo di Bedarida per una trattazione puntuale delle metodologie.
[21] Sharma, A. e Panigrahi, P.K. *A Review of Financial Accounting Fraud Detection based on Data Mining Techniques*. International Journal of Computer Applications. Volume 39, n. 01, Febbraio 2012. Pag. 38.

- *Regression model;*
- *Neural networks;*
- *Bayesian Belief Network;*
- *Decision Trees;*
- *Naive Bayes;*
- *Nearest Neighbour Method;*
- *Fuzzy logic and Genetic Algorithm;*
- *Expert Systems*.

Le investigazioni

Una volta identificati, attraverso le varie tecniche sopra illustrate, i possibili eventi/comportamenti sospetti o di natura fraudolenta, al processo di segnalazione dovrebbe seguire il processo di investigazione, al fine di chiarire la reale minaccia/consistenza dell'attività sospetta. Per questo motivo l'organizzazione dovrebbe prevedere un sistema di investigazioni improntato ai migliori standard e opportunamente proceduralizzato.

La fase di investigazione, quindi, si esplica nei seguenti stadi:

- ricezione dell'alert di frode (rilevato grazie alla *fraud detection*);

- valutazione del fatto alla base dell'alert: seguendo le procedure stabilite, si dovrebbe valutare l'alert ricevuto, valutando la tipologia ed entità dell'evento/comportamento segnalato, la/le persone coinvolte, le eventuali conseguenze per l'organizzazione, decidendo come proseguire la fase di indagine;

- valutazione dei costi in relazione all'evento fraudolento e al contesto legale, normativo, etico;

- analisi delle possibili responsabilità aziendali e delle possibili conseguenze economiche, reputazionali e legali a carico dell'azienda;

- conduzione delle investigazioni: è la parte maggiormente specialistica e sensibile, pertanto è opportuno che venga espletata da personale specialista, in conformità alla legislazione in vigore (codice privacy, statuto dei lavoratori, codice penale, ecc.) e con criteri ispirati alle investigazioni criminali. La fase di investigazione comprende la conduzione di interviste (ipotetico attore, persone coinvolte, figure neutrali, ecc.), la raccolta di documenti utili, come a esempio documenti interni (file personali, registro telefonate, registrazioni video-sorveglianza, ecc.) e documenti esterni (registri pubblici, rapporti detective privati), e l'analisi degli elementi raccolti;

- reporting dei risultati: il team di investigazione effettua il reporting alle parti interessate, come a esempio direttori di unità di business, CdA, senior management in

[22] Per una trattazione puntuale delle varie tecniche, e delle ricerche in tema di *data mining*, si consiglia di visionare l'articolo di Sharma e Panigrahi.

generale, in base alla tipologia di frode investigata e alle previsioni organizzative e legali;

- azioni correttive: sulla base dei riscontri dell'investigazione, le figure e le funzioni aziendali competenti sviluppano le azioni di risposta al fatto fraudolento, che possono comportare, a titolo meramente esemplificativo, l'adozione di provvedimenti di natura civile (sospensione o risoluzione di contratto), la denuncia per le fattispecie a rilevanza penale, sanzioni amministrative e disciplinari.

È importante notare come vi siano alcuni fattori estremamente rilevanti per l'esecuzione delle investigazioni che risaltano, per questa fase del processo di gestione del rischio di frode, il ruolo della funzione di security aziendale:

- fattore tempo: le investigazioni potrebbero dover essere svolte entro tempi stabiliti dalla normativa di riferimento, o dover essere svolte in tempistiche brevi al fine di minimizzare i danni per l'organizzazione;

- notificazione/rapporti con le Forze di Polizia: se la fattispecie di frode sotto investigazione ha rilevanza penale, o comunque giuridica, vi sarà il coinvolgimento e l'interfaccia con le Forze di Polizia. Inoltre, ai fini dell'attività investigativa, vi può essere la necessità che il team di investigazioni intrattenga rapporti con esponenti delle Forze di Polizia;

- confidenzialità: capacità di mantenere confidenziale il fatto alla base dell'investigazione, l'investigazione stessa e il reporting finale, includendo nel processo solo quelle figure/funzioni che necessitano di essere coinvolte/informate;

- aspetti legali: la attivazione della procedura di investigazione implica aspetti legali rilevanti;

- compliance: le investigazioni, come già indicato, devono essere svolte in conformità alla normativa vigente;

- sicurezza delle prove e degli elementi rilevanti: questi dovrebbero essere protetti e salvaguardati al fine di evitare manomissioni e/o distruzioni;

- obiettività: l'investigazione va svolta con obiettività;

- obiettivi: alcune tematiche o avvenimenti hanno una influenza sul focus, sul raggio e sulla tempistica dell'investigazione.

Le funzioni aziendali coinvolte nel sistema antifrode

In conclusione, si sottolinea come la frode rappresenti un rischio trasversale e profondamente eterogeneo. Può essere compiuto internamente o esternamente all'azienda, e quindi

comportare, a esempio, la fuga di notizie commerciali sensibili, infedeltà aziendale attraverso l'accaparramento di risorse economiche dell'azienda, e così via. Ancora, la frode può coinvolgere risorse, comportando perdite, economiche e finanziarie, o, come osservato negli ultimi anni, essere perpetrata attraverso frodi informatiche, che puntano alla distruzione/sottrazione di dati aziendali (in questo aspetto rientra il tema della protezione dei dati sensibili e personali, ex codice della privacy).

In quanto tale, il rischio di frode coinvolge molteplici funzioni aziendali, che hanno un impatto e/o effetti su di esso, tra le quali:

- internal audit;
- security;
- enterprise risk management;
- finance;
- contabilità;
- legale;
- unità operative e di business;
- ICT;
- HR.

Un programma di *fraud governance* si pone quindi in maniera trasversale su tutte le funzioni aziendali. La sua implementazione non richiede uno stravolgimento delle policy aziendali o una riscrittura in toto delle *job description* delle diverse funzioni. Un programma deve prevedere un adeguamento del modello organizzativo aziendale esistente, ampliandone i contenuti, senza creare sovrapposizioni di competenza o fenomeni di ridondanza in termini di policy e codici aziendali. È piuttosto necessario prevedere un coordinamento organizzativo che sappia relazionarsi funzionalmente (e non necessariamente gerarchicamente) con tutte le funzioni aziendali garantendo il funzionamento di uno specifico piano di comunicazione (comprensivo della condivisione di obiettivi e informazioni), di controllo e monitoraggio continuo.

Questa risorsa (o funzione organizzativa) deve avere un'elevata sensibilità verso le esigenze di protezione degli asset aziendali e profonde competenze ed esperienze nella gestione dei rischi. Inoltre al responsabile di un programma di *fraud governance* deve essere garantito il pieno committment da parte del top management e un adeguato budget economico.

Pertanto, il processo può essere affidato alla security, all'internal audit, alla funzione legale, al risk management, e così via, oppure ancora essere suddiviso in aree di responsabilità fra di esse. La necessità che si pone è, inoltre, di sviluppare un sistema di gestione antifrode che riesca a essere omogeneo e sinergico, facendo cooperare tutte le funzioni aziendali coinvolte attraverso una chiara suddivisione delle aree di responsabilità.

Il ruolo della security aziendale

Come si è visto nello sviluppo del sistema di gestione, la funzione di security aziendale è coinvolta in maniera diretta nelle attività sviluppate all'interno di un programma di *fraud governance*. Diversi sotto-processi, infatti, afferiscono in maniera specifica alla funzione security.

La necessità di includere la funzione security nella *fraud governance* aziendale è stata rilevata in diversi report internazionali. In particolare, il rapporto del 2006 della *Financial Services Authority* della Gran Bretagna ha evidenziato come, specialmente per gli aspetti relativi alla identificazione delle fattispecie rilevanti e la gestione delle investigazioni, l'assegnazione di ruoli e responsabilità alla security fosse un fattore estremamente rilevante per l'efficacia del processo.

In definitiva, così come rilevato a livello internazionale, possiamo affermare che la security aziendale, anche per la sempre crescente professionalizzazione della funzione, che sta portando a ricomprendere sotto la sua sfera attività che si allontanano dal tradizionale campo della "sicurezza fisica" (come il *crisis management* o la *business continuity*), all'interno del sistema di gestione antifrode potrebbe:

- contribuire a identificare le fattispecie di attività di frode rilevanti per l'organizzazione, contribuendo a sviluppare gli indicatori di rischio di frode su cui basare l'attività di *fraud prevention e fraud detection;*
- eventualmente contribuire allo sviluppo e gestione degli applicativi informatici di *fraud prevention;*
- gestire e condurre le investigazioni, in raccordo e collaborazione con le altre funzioni aziendali: la funzione security, per competenze e forma mentis, è la funzione aziendale idonea a condurre e gestire le investigazioni all'interno dell'azienda, in ottemperanza alle normative vigenti;
- garantire confidenzialità nella gestione di sospetti casi di frode;
- offrire supporto alla funzione legale nella gestione di eventuali contenziosi provocati da casi di frode in danno all'azienda;
- gestire i rapporti con le Forze di Polizia e di Pubblica Sicurezza.

Un modello che preveda questo tipo di coinvolgimento della security sarebbe, senza dubbio, efficace, e permetterebbe di utilizzare know how ed expertise specifico con il fine ultimo di tutelare l'azienda da potenziali attività fraudolente, siano esse interne o esterne.