

Le frodi aziendali: la prevenzione delle frodi

Parte V

22 Agosto 2019

Angelo Fiori

1. La governance del rischio di frode
2. La valutazione dei rischi di frode
3. La prevenzione del rischio di frode
4. Il controllo e il monitoraggio
5. Le investigazioni
6. Le funzioni aziendali coinvolte

1. La governance del rischio di frode

Il primo aspetto fondamentale è lo sviluppo di un impianto organizzativo atto a gestire il rischio di frode.

Il sistema di gestione può essere sviluppato su una serie di componenti articolate; le componenti del sistema, sono:

- **Impegno del 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. 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 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 i livelli attraverso specifiche e periodiche attività di formazione e *assessment*.
- **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 visione del documento che delinea il codice di comportamento accettandone i contenuti.
- **Conflitto d'interessi**: dovrebbe essere sviluppato un processo aziendale, che faccia emergere e consenta di prevenire e gestire possibili conflitti di interesse di dipendenti, dirigenti e quadri 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) 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.
- **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. La valutazione dei rischi 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* per la valutazione di altre tipologie rischi.

Lo svolgimento di questa attività può essere condotto 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 team dedicato, 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: (a) contabilità e finanza; (b) unità di business; (c) risk management; (d) security; (e) legale; (f) internal audit; (g) information technology; (h) human resources; (i) sales; (l) consulenti e specialisti 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.

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 e di rilevazione degli eventi sospetti o accaduti.

3. La prevenzione del rischio di frode

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.

4. Il controllo e il monitoraggio

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 allerta 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.

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”

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” “il data mining utilizza diverse tecniche al fine di ricercare fra grandi quantità di dati e identificare relazioni e connessioni passate, estrarre regole di decisione o costruire modelli predittivi”.

5. Le investigazioni

La fase di investigazione si esplica nei seguenti stadi:

- **ricezione dell’allerta di frode**, rilevato grazie alle procedure per il controllo delle frodi;
- **valutazione del fatto alla base dell’allerta**: seguendo le procedure stabilite, si dovrebbe valutare l’allerta 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 ingenerale, 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 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.
- **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.

6. Le funzioni aziendali coinvolte

Si sottolinea come la frode rappresenti, in ambito aziendale, 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 (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: (a) internal audit; (b) security; (c) funzione di enterprise risk management; (d) finanza; (e) contabilità; (f) ufficio legale; (g) unità operative e di business; (h) ICT; (i) Human resources.

Un programma di gestione delle frodi si pone quindi in maniera trasversale su tutte le funzioni aziendali.

Tale 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 quindi 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 *commitment* da parte del top management e un adeguato budget economico.

Pertanto, il processo può essere affidato: (a) alla funzione di *security*, (b) all'*internal audit*, (c) alla funzione legale, (d) al *risk management*, 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.

[Parte I](#), [Parte II](#), [Parte III](#), [Parte IV](#) e [Parte VI](#)

Bibliografia

Frodi aziendali – Giuseppe Pogliani, Nicola Pecchiari, Marco Mariani – EGEA 2012.

Global economic crime survey 2016” di Price Waterhouse & Coopers.

Ernst & Young_14th_Global_Fraud_Survey - 2016.

ACFE-(association of certified fraud examiners) 2016 - “Report-to-the-nations 2016”.

Fondazione Luca Pacioli “Oltre il velo societario. L’utilizzo di strutture societarie per finalità illecite. Il rapporto dell’OCSE”.

TAG: frodi aziendali, fraud governance, risk management

Avvertenza

La pubblicazione di contributi, approfondimenti, articoli e in genere di tutte le opere dottrinarie e di commento (ivi comprese le news) presenti su Filodiritto è stata concessa (e richiesta) dai rispettivi autori, titolari di tutti i diritti morali e patrimoniali ai sensi della legge sul diritto d'autore e sui diritti connessi (Legge 633/1941). La riproduzione ed ogni altra forma di diffusione al pubblico delle predette opere (anche in parte), in difetto di autorizzazione dell'autore, è punita a norma degli articoli 171, 171-bis, 171-ter, 174-bis e 174-ter della menzionata Legge 633/1941. È consentito scaricare, prendere visione, estrarre copia o stampare i documenti pubblicati su Filodiritto nella sezione Dottrina per ragioni esclusivamente personali, a scopo informativo-culturale e non commerciale, esclusa ogni modifica o alterazione. Sono parimenti consentite le citazioni a titolo di cronaca, studio, critica o recensione, purché accompagnate dal nome dell'autore dell'articolo e dall'indicazione della fonte, ad esempio: Luca Martini, La discrezionalità del sanitario nella qualificazione di reato perseguibile d'ufficio ai fini dell'obbligo di referto ex. art 365 cod. pen., in "Filodiritto" (<https://www.filodiritto.com>), con relativo collegamento ipertestuale. Se l'autore non è altrimenti indicato i diritti sono di Inforomatica S.r.l. e la riproduzione è vietata senza il consenso esplicito della stessa. È sempre gradita la comunicazione del testo, telematico o cartaceo, ove è avvenuta la citazione.