Marzo 2013

Fraud management e whistle blowing

Dott. Andrea Bombardieri, Responsabile Controllo Rischi - Asset Management Service S.p.A. (Gruppo Objectway)

La gestione del rischio di frode aziendale, insieme alla lotta al riciclaggio di denaro e al finanziamento del terrorismo, rappresenta uno dei temi caldi del momento.

Diverse sono le definizioni di frode. L'associazione ACFE (Association of Certified Fraud Examiners) la definisce come "l'abuso del proprio ruolo per un arricchimento personale facendo leva sull'utilizzo degli asset e delle risorse aziendali". Gli standard AIIA (Associazione Italiana Internal Auditors) la definiscono – sinteticamente - come "qualsiasi atto illegale caratterizzato da raggiro, occultamento e abuso di fiducia".

Concretamente, l'autore della frode induce in errore la vittima attraverso artifici e raggiri, procurando a sé stesso o ad altri un vantaggio ingiusto unito a un ingiusto danno per la vittima o per altri.

Ma perché si froda? Diversi modelli sono stati sviluppati in proposito: il più famoso di questi è senza dubbio il cosiddetto "triangolo della frode", elaborato nel 1973 dal sociologo americano Cressey. Secondo questo modello tre sono i fattori che possono causare un fenomeno di frode

1. pressione
2. opportunità
3. razionalizzazione.

Una sola di queste variabili non è sufficiente per portare un soggetto a commettere una frode. Laddove invece esista la contemporanea presenza di questi tre fattori, si riscontra che la probabilità di commissione di una frode si alza considerevolmente: è proprio questo l'ambito di ricerca per chi è preposto alla valutazione del rischio di frode (Risk Management), oltre per chi è responsabile della valutazione dell'adeguatezza delle barriere al rischio di frode implementate in azienda (Internal Auditing).

Concentriamo la nostra attenzione sui tre fattori predetti: essi risulteranno determinanti per l'individuazione dei possibili casi di frode in azienda.

Pressione: se eccessiva, può indurre una persona alla commissione di una frode. Deriva da fattori interni o esterni all'organizzazione. Nel caso di fattori interni, un target aziendale ritenuto dalla Direzione come un *must*, potrebbe spingere – per esempio – a una falsificazione delle scritture contabili, a maggior ragione se in azienda sono attivi dei meccanismi di remunerazione correlati alle performance aziendali. Tra i fattori esterni, il bisogno urgente di denaro.

Opportunità: la consapevolezza dell'autore della frode in merito alla presenza di punti deboli del sistema dei controlli interni genera l'opportunità.

Razionalizzazione: avviene quando l'autore della frode riesce a giustificare a sé stesso e, qualora venisse scoperto, anche ai colleghi, la frode realizzata. Psicologicamente ciò accade perché il frodatore non si identifica in un criminale.

Primo passo per la creazione di un efficace programma di gestione del rischio di frode aziendale è l'analisi del cosiddetto "ambiente di controllo", che riflette l'attenzione del Top Management all'importanza della cultura di controllo interno dell'organizzazione. Il *Control Environment* è difatti il primo dei 5 step del COSO Framework (COSO – Committee of Sponsoring Organizations of the Traedway Commissions) ed è scomponibile in 4 elementi di analisi per il rischio frode:

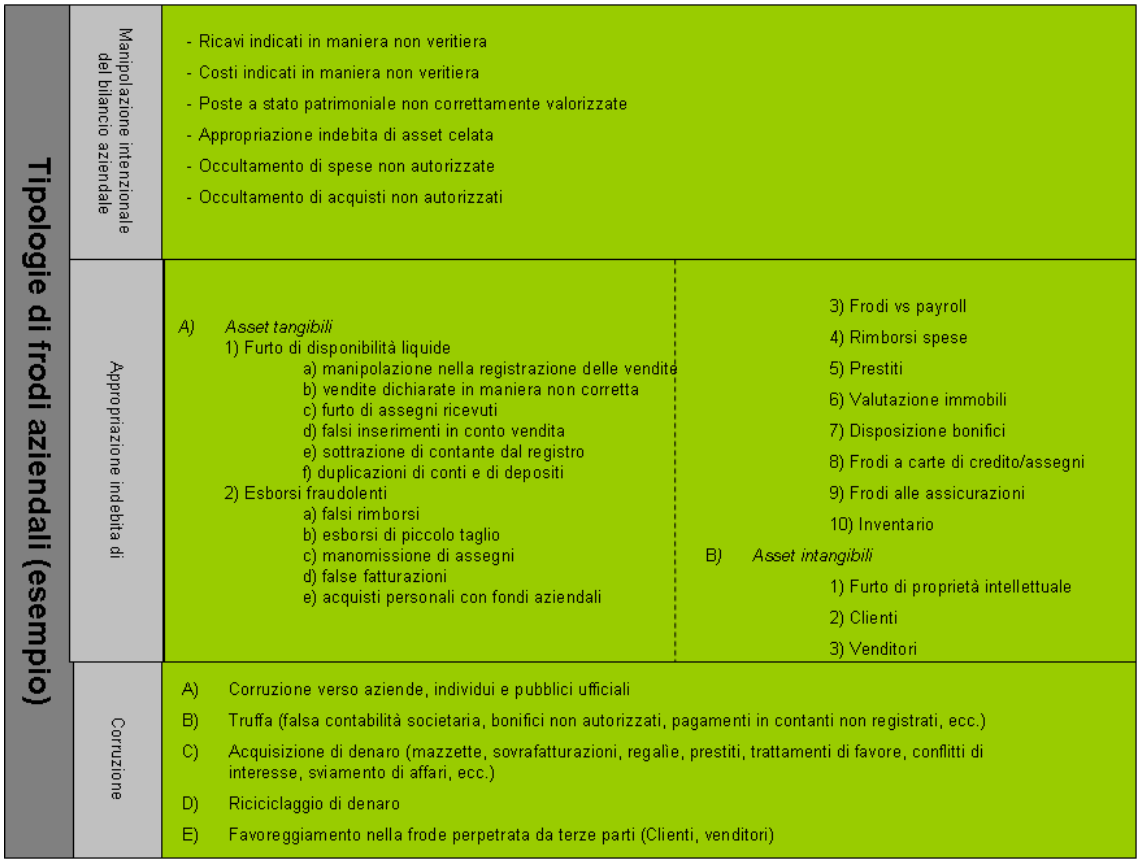
a. filosofia del management e stile di gestione (*Tone at the Top*, adozione Codice Etico, diffusione della cultura etica aziendale attraverso circolari interne, intranet, eventi aziendali, ecc.)

b. struttura organizzativa (p.e. segregazione di responsabilità, flussi informativi, struttura delle deleghe e delle procure interne)

c. politiche di gestione delle risorse umane (procedure di selezione del personale, policy di incentivazione e retribuzione del personale, procedure di valutazione delle performance periodiche)

d. sistemi informativi e flussi di comunicazione (flussi informativi tra Alta Direzione, i soggetti responsabili dei controlli e gli Organi di controllo ma anche processi di *whistle blowing*).

Il secondo step è il *Fraud Risk Assessment*, che conseguirà all'analisi del *Control Environment*, che è invece il processo di identificazione e valutazione dei rischi di frode al fine di identificare i processi sensibili e individuare le azioni di miglioramento da apportare al sistema di controllo interno. Di seguito un esempio di possibili tipologie di frodi aziendali:



Successivamente verranno individuate le attività di controllo della frode (fraud detection e fraud prevention), indi dovrà essere definita una efficace piano di comunicazione aziendale al fine di mantenere alta la consapevolezza del rischio di frode. Da ultimo un costante e efficace monitoraggio del programma di gestione del rischio di frode.

Al fine di avere un efficace gestione del rischio di frode non si può dimenticare che, come dettagliato da uno studio di ACFE, per la metà dei casi le frodi vengono rilevate da comunicazioni o lamentele da parte di dipendenti, indi clienti, fornitori e altre fonti (*whistle blowing*).

È auspicabile quindi che l'azienda si doti di un Whistle Blowing Program (WBP), in prima istanza rivolto ai dipendenti aziendali, che disciplini e implementi idonei canali informativi atti a garantire la ricezione, l'analisi e il trattamento di segnalazioni relative a possibili casi di frode.

Un utile spunto sul tema è fornito dal PAS 1998:2008 "Whistleblowing arrangements – Code of practice", realizzato in Inghilterra da un'autorità indipendente (il Public Concern at Work), in collaborazione con il BSI (British Standards Institution), al fine di dare suggerimenti pratici , anche tenendo conto della normativa cogente (nel regno Unito il PIDA, Public Interest Disclosure Act).

Tra i tanti suggerimenti:

- per le aziende quotate l'Audit Committee deve supervisionare l'operato del WBP
- la responsabilità globale del WBP, a seconda della natura del business e della dimensione dell'azienda di interesse sarà in capo al Consiglio di Amministrazione, l'Amministratore Delegato, la Segreteria di Gruppo, l'Area Legale o quella Finanza
- la responsabilità della gestione del WBP nel *day by day* ricadrà spesso nell'Internal Audit, nella Compliance o nell'Area del Personale
- si deve comunicare efficacemente, attraverso la relativa Policy e le FAQ, la modalità di comunicazione di un possibile caso di frode
- la riservatezza delle informazioni deve essere comunicata e garantita e i dettagli del whistle blower saranno comunicati solo se richiesti dalla Pubblica Autorità (open whistle blowing)
- la Policy non dovrebbe incoraggiare le segnalazioni anonime in quanto renderebbero sicuramente più difficile la conseguente investigazione; di contro, ignorare le eventuali segnalazioni anonime ricevute non è consigliabile
- nel caso in cui la Policy prevede la sottomissione di segnalazioni anonime, devono essere garantite le misure minime di sicurezza prescritte dal Garante della Privacy (data retention, sicurezza delle informazioni, privilegi, accessi)
- è possibile avvalersi di *hotline* dedicate al whistleblowing, fornite quindi da terze parti, che passerebbero poi l'informazione ricevuta al senior – interno all'organizzazione – dedicato al trattamento delle segnalazioni
- l'organizzazione dovrà usare la Policy relativa alla discriminazione, ove ne emergesse a carico del collega segnalante la frode
- gestire una comunicazione regolare ed efficace a tutto il personale in ordine al WBP
- effettuare corsi di formazione al fine di sensibilizzare il personale e rendere proficuo e efficiente il processo di segnalazione
- adottare le misure minime di sicurezza dettate dagli adempimenti del Codice Privacy per l'archiviazione della documentazione inerente alla segnalazione di frode

- in caso di segnalazioni poi rivelatesi di vitale importanza per l'organizzazione, potrebbe essere auspicabile elargire una ricompensa (bonus o altro benefit, di concerto con HR).

Il sopracitato PAS fornisce anche una utile checklist per l'assessment della Policy di whistleblowing in tutte le sue componenti principali, da calare poi nella realtà specifica aziendale; essa è descritta nella tabella che segue:

Checklist per assessment della Policy di whistleblowing	
	La Policy a) offre esempi di tipi di segnalazioni da elevare, così da distinguere il whistleblowing dal reclamo b) dà la possibilità di elevare segnalazioni al di fuori della linea di riporto diretto c) dà la possibilità di accedere in maniera riservata a una linea indipendente per consulenza d) dà la possibilità di elevare segnalazioni garantendone la riservatezza e) indica quali segnalazioni possono essere elevate fuori dall'organizzazione (p.e. un regulator) f) proibisce atti discriminatori contro i whistleblowers in buona fede g) proibisce false accuse dolosamente elevate
	Briefing delle risorse primariamente coinvolte Le risorse coinvolte direttamente nel processo di gestione del whistleblowing sono state opportunamente briefate sul ruolo del management, sul valore della riservatezza e dell'anonimato
	Senso pratico Forme pratiche, gestione dei feedback e cattivi utilizzi del whistleblowing sono presentati al personale
	Comunicazione a) l'organizzazione effettua delle attività di promozione delle disposizioni contenute nella Policy b) la consapevolezza, conoscenza e esperienza della Policy da parte del personale è periodicamente valutata
	Formazione a) Formazione specifica per l'Alta Direzione, il senior management b) Formazione per risorse specificatamene coinvolte nel processo di gestione del whistleblowing
	Record Tutte le segnalazioni inviate secondo le disposizioni della Policy sono registrate e fatte confluire in un database centrale
	Monitoring efficacia delle disposizioni L'efficacia delle disposizioni contenute nella Policy sono periodiocamente sottoposte a valutazione da parte degli Organi coinvolti nella gestione della governance aziendale (p.e. Audit Committee)