Economia Aziendale Online

Business and Management Sciences
International Quarterly Review

Corporate sustainability e prevenzione delle frodi aziendali. Il contributo dei sistemi ERP

Paolo Roffia

Pavia, June 30, 2025
Volume 16 – N. 2/2025

DOI: 10.13132/2038-5498/16.2.471-484

www.ea2000.it
www.economiaaziendale.it

PaviaUniversityPress

Electronic ISSN 2038-5498
Reg. Trib. Pavia n. 685/2007 R.S.P.

Economia Aziendale Online – Business and Management Sciences International Quarterly Review
Vol. 16-2/2025 - DOI: 10.13132/2038-5498/16.2.471-484

Corporate sustainability e prevenzione delle frodi aziendali. Il contributo dei sistemi ERP

Paolo Roffia

Professore Associato in Economia Aziendale. Dipartimento di Management, Università di Verona. Italy.

Corresponding Author:

Paolo Roffia

paolo.roffia@univr.it

Cite as:

Roffia, P. (2025). Corporate sustainability e prevenzione delle frodi aziendali. Il contributo dei sistemi ERP. *Economia Aziendale Online*, *16*(2), 471-484.

Section:

Refereed Paper

Received: April 2025
Published: 30/06/2025

ABSTRACT

I sistemi informativi integrati di tipo Enterprise Resource Planning (ERP) sono stati un driver di valore aziendale, attraverso la gestione integrata delle informazioni ed il miglioramento dell'efficienza e dell'efficacia dei processi. Gli ERP hanno trovato ampia diffusione sia nelle aziende di grandi dimensioni che nelle PMI, divenendo un componente fondamentale del loro sistema di controllo interno (SCI). Tuttavia, data questa loro importanza e centralità, è fondamentale che il loro utilizzo avvenga con il disegno di un sistema di controllo interno adeguato al contesto considerato, pena l'insorgere di gravi vulnerabilità, fra cui quella alle frodi aziendali. Questo articolo analizza l'importanza dei controlli interni inclusi negli ERP a mitigazione del rischio frode, attraverso una review della letteratura e l'analisi di un caso di studio emblematico, riguardante la frode compiuta da Jérôme Kerviel nel 2008 ai danni Société Générale. Con il supporto di altri esempi tratti dal contesto delle PMI e delle organizzazioni non lucrative italiane si intende riflettere sui rischi e gli effetti di un sistema di controllo interno inefficace sul tema della prevenzione delle frodi aziendali, con impatti negativi sulla corporate governance e la gestione sostenibile del business. L'articolo si conclude con alcune raccomandazioni utili al rafforzamento dei controlli interni inclusi nei sistemi ERP.

Integrated Enterprise Resource Planning (ERP) information systems have been a driver of corporate value, through the integrated management of information and the improvement of the efficiency and effectiveness of processes. ERPs have become widely used in both large companies and SMEs, becoming a fundamental component of their internal control system (ICS). However, given their importance and centrality, it is essential that their use takes place with the design of an internal control system appropriate to the context considered, otherwise serious vulnerabilities will arise, including that of corporate fraud. This article analyzes the importance of internal controls included in ERPs to mitigate fraud risk, through a review of the literature and the analysis of an emblematic case study, concerning the fraud committed by Jérôme Kerviel in 2008 against Société Générale. With the support of other examples taken from the context of Italian SMEs and non-profit organizations, we intend to reflect on the risks and effects of an ineffective internal control system on the issue of corporate fraud prevention, with negative impacts on corporate governance and sustainable business management. The article

concludes with some useful recommendations for strengthening the internal controls included in ERP systems.

Keywords: Enterprise Resource Planning (ERP), Sistema di Controllo Interno (SCI), CoSO report, Frodi aziendali, Corporate sustainability, Corporate governance.

1 – Introduzione

Sul finire del secolo scorso nelle società di grandi dimensioni, e successivamente anche in quelle di minore dimensione, sono stati introdotti sistemi informativi integrati di tipo Enterprise Resource Planning (ERP) per integrare, automatizzare ed efficientare processi aziendali divenuti sempre più critici e complessi (Marchi, 2003). Questi sistemi hanno avuto origine negli anni '60 con l'introduzione dei primi *software* per il controllo della produzione (MRP - Material Requirements Planning) (Monk & Wagner, 2009), evolvendosi poi negli anni '90 con l'avvento di piattaforme integrate più sofisticate (Davenport, 1998). Oggigiorno gli ERP più diffusi consentono la piena integrazione dei dati aziendali, conglobando in un unico sistema la gestione dei processi di vendita, acquisto, amministrazione, gestione del magazzino, delle commesse, dei sistemi informativi, del personale anche nel caso di organizzazioni geograficamente distribuite. Ne derivano benefici in termini di velocità di elaborazione, consistenza e non ridondanza dei dati, così come quelli relativi ad una gestione più efficiente delle risorse aziendali oltre che più efficace verso gli obiettivi dell'organizzazione. Tuttavia, la digitalizzazione dei dati e la centralità assunta dagli ERP hanno portato con sé nuovi rischi aziendali, che devono essere opportunamente individuati e gestiti. Fra questi rischi figura quello di frode interna, ossia l'effetto negativo producibile come conseguenza di comportamenti illegali ed opportunistici dei propri collaboratori (Spathis, 2002). In generale, quindi, un sistema ERP oggi pervasivo ed esteso a tutta l'organizzazione può divenire un punto di debolezza se al suo interno non vengono inseriti adeguati presidi di controllo interno. Gli effetti negativi impattano le risorse dell'azienda, la sua reputazione, la *corporate governance* e, in ultima istanza, la sostenibilità del business. La nostra *domanda di ricerca* è quindi incentrata sul contributo che gli ERP possono dare alla *corporate sustainability* esercitando un impatto positivo sul sistema di controllo interno a supporto della prevenzione delle frodi. Esempi di presidi di controllo inclusi negli ERP in grado di rafforzare le componenti del SCI, sono la registrazione senza possibilità di cancellazione di tutte le operazioni aziendali, la previsione di specifici meccanismi autorizzativi per le operazioni più rilevanti, la tracciatura degli accessi, la creazione e diffusione a tutti gli attori delle informazioni utili ai controlli interni. La struttura dell'articolo è come segue: l'analisi della letteratura fornisce una panoramica degli studi sul sistema di controllo interno, sui sistemi informativi di tipo ERP, sulle frodi aziendali e le loro teorie di riferimento. I casi di studio considerati consentono di analizzare le carenze nei controlli interni inclusi nei sistemi ERP. Seguono una discussione critica degli effetti di questi divari e le conclusioni con la proposizione di alcune linee di azione, l'evidenziazione dei limiti della ricerca e dei suoi possibili sviluppi.

2 – Literature review

Per affrontare la *domanda di ricerca* di questo lavoro si è proceduto con l'analisi della letteratura relativamente a quattro *topic* ritenuti rilevanti, ossia: (i) il sistema di controllo interno ed i suoi elementi, (ii) i sistemi ERP, le loro caratteristiche e vulnerabilità, (iii) le frodi aziendali e la loro

prevenzione, (iv) il contrasto delle frodi nel quadro della corporate governance e della sostenibilità.

2.1 – *Il sistema di controllo interno*

Il sistema di controllo interno (SCI), secondo la più autorevole ed accettata definizione contenuta nel CoSO report, è un processo integrato volto a fornire ragionevole certezza del raggiungimento degli obiettivi aziendali relativi all'efficienza ed efficacia delle operazioni e dei processi, all'affidabilità della reportistica economico-finanziaria ed alla conformità alle normative (CoSO, 2013).

Secondo tale documento il SCI è dotato di *cinque* componenti fondamentali, ossia:

1. *L'ambiente di controllo*: Comprende i valori etici, l'impegno della direzione in questo senso e la struttura organizzativa necessaria per promuovere una cultura di integrità e di corretta gestione.

2. *La valutazione dei rischi*: Identifica e valuta i rischi che potrebbero compromettere il raggiungimento degli obiettivi aziendali.

3. *L'attività di controllo*: Comprende le politiche e procedure volte a mitigare i rischi identificati rispetto agli obiettivi dell'organizzazione.

4. *L'informazione e comunicazione*: Garantisce che le informazioni rilevanti siano identificate, raccolte e condivise in modo tempestivo.

5. *Il monitoraggio*: Valuta l'efficacia del sistema di controllo interno nel corso del tempo e promuove le eventuali azioni correttive.

Le cinque componenti di cui sopra richiedono il contributo di tutti i collaboratori dell'organizzazione e non soltanto degli organi di vertice ai quali compete di definire le direttive, mettere a disposizione le risorse necessarie, nonché attuare gli adeguati riscontri affinché il SCI sia progettato ed attuato correttamente (Corbella, 2000).

Sul tema del posizionamento dei controlli all'interno delle organizzazioni, le associazioni professionali europee degli internal auditor (ECIIA) e dei risk manager (FERMA) nel 2008-2010 hanno proposto l'adozione del modello cosiddetto delle "tre linee di difesa", dove il primo livello è costituito dai controlli del management e del superiore gerarchico sulle attività operative, il secondo livello è costituito dal *risk management*, dal controllo di gestione e dalla funzione di compliance nei rispettivi ambiti di attività, ed il terzo livello dall'*internal audit* (sono peraltro da considerare a parte i controlli svolti da altri soggetti esterni come quelli dell'*external auditor* e dell'eventuale soggetto regolatore dell'attività, come potrebbe essere Banca d'Italia per il contesto bancario o IVASS per quello assicurativo). Va segnalato come dal punto di vista della teoria di riferimento, gli studi sul sistema di controllo interno, ad eccezione di alcuni distinguo necessari come nel caso delle aziende familiari, facciano principale riferimento alla teoria dell'Agenzia (Jensen & Meckling, 1976), che individua nell'introduzione dei controlli aziendali un possibile rimedio ai comportamenti opportunistici di manager e collaboratori, stante il conflitto di interesse che è "naturalmente" presente fra tra la proprietà (i soci) e gli agenti (i manager e collaboratori).

Come vedremo più oltre, i controlli interni integrati nei sistemi ERP operano in questa direzione (Nicolaou, 2000).

2.2 – *Gli Enterprise Resource Planning* (ERP)

I sistemi Entreprise Resource Planning (ERP) sono stati introdotti per la prima volta negli anni '60, come strumenti di *Material Requirements Planning* (MRP) (Monk & Wagner, 2009). Questi sistemi erano focalizzati principalmente sulla pianificazione delle necessità di materiali per supportare i processi produttivi. Negli anni '80, i MRP si sono evoluti in Manufacturing Resource Planning (o MRP II), che includevano ulteriori funzionalità per la pianificazione delle risorse produttive. Negli anni '90 con il progresso tecnologico e l'avvento dei moderni ERP, queste piattaforme sono divenute in grado di gestire non solo i processi produttivi, ma anche altre funzioni aziendali con specifici moduli, fra cui si segnalano:

a1. *Modulo Contabilità e Finanza*: Gestisce le transazioni finanziarie, i bilanci, e la reportistica fiscale. Rispetto ai sistemi tradizionali, offre maggiore integrazione tra dati finanziari e operativi, migliorando la trasparenza e il controllo dei costi.

b1. *Modulo Risorse Umane (HR)*: Automatizza la gestione delle buste paga, le valutazioni delle performance e i processi di assunzione. Questo modulo consente un monitoraggio più efficace delle risorse umane rispetto ai sistemi isolati del passato.

c1. *Modulo Gestione della Supply Chain*: Coordina l'approvvigionamento, la produzione e la distribuzione, garantendo una maggiore efficienza operativa. Rispetto ai vecchi sistemi manuali, questo modulo riduce gli sprechi e migliora la pianificazione.

d1. *Modulo Vendite e Marketing*: Aiuta nella gestione degli ordini, delle relazioni con i clienti e delle campagne di marketing. La sua integrazione con altri moduli consente una visione olistica delle operazioni aziendali.

e1. *Modulo Produzione*: Fornisce strumenti per pianificare, monitorare e ottimizzare i processi produttivi. Rispetto ai sistemi MRP iniziali, include funzionalità avanzate per la gestione delle risorse e il controllo qualità.

f1. *Modulo Analisi* e *Business Intelligence (BI)*: Integra dati da diversi moduli per supportare decisioni strategiche basate su informazioni in tempo reale. Esso è oramai disponibile in numerose piattaforme, apportando un miglioramento significativo ai sistemi di reportistica tradizionali.

Questi moduli, integrati fra loro, offrono alcuni importanti vantaggi rispetto ai sistemi del passato: eliminano i silos e divari informativi, migliorano l'efficienza operativa e forniscono una solida base per decisioni aziendali fondate sui dati (Davenport, 1998). Questa evoluzione ha consolidato l'utilizzo degli ERP come strumenti strategici per il miglioramento della competitività aziendale, promuovendone una rapida ascesa (Agliati *et al*., 2001; Caserio, 2019). La diffusione di questi sistemi è stata inizialmente nelle grandi aziende manifatturiere, dove la complessità dei processi richiedeva maggiore integrazione e centralizzazione della gestione, successivamente trasversalmente anche in altri macro-settori, come banche ed assicurazioni o nel contesto delle aziende pubbliche, come quelle sanitarie (Del Bene *et al*. 2012). A partire dagli anni 2000 anche le PMI e le organizzazioni non lucrative hanno iniziato ad implementare sistemi ERP, grazie alla disponibilità di soluzioni economicamente e architetturalmente accessibili oltre che modulari per il loro contesto (Shang & Seddon, 2002).

Oggi, gli ERP sono caratterizzati da un'ampia gamma di funzionalità, che includono l'analisi dei dati, il supporto decisionale in tempo reale e l'integrazione con tecnologie emergenti come

l'intelligenza artificiale e l'Internet of Things (IoT). Queste caratteristiche rendono gli ERP una componente essenziale dell'infrastruttura tecnologica delle aziende più dinamiche e moderne sul tema dell'infrastruttura digitale.

Gli ERP, essendo altamente pervasivi, complessi ed integrati, prestano tuttavia il fianco a diversi tipi di vulnerabilità o rischi, fra cui:

a2. *Carenze nei controlli interni*: Sistemi ERP mal configurati o dotati di controlli interni inadeguati, costituiscono una opportunità per un potenziale frodatore (Nicolaou, 2000).

b2. *Errori umani*: Gli utilizzatori possono commettere errori più o meno involontari, tali da compromettere l'integrità ed attendibilità dei dati del sistema informativo aziendale (Bruni, 1990; Poston & Grabski, 2001).

c2. *Attacchi informatici*: La crescente digitalizzazione e connessione degli ERP alle reti esterne li rende vulnerabili a minacce come *malware*, *ransomware* e accessi non autorizzati (Al-Mashari, 2003).

Va tuttavia rilevato come i rischi connessi all'utilizzo degli ERP di cui sopra possano trovare parziale o totale mitigazione con la previsione di adeguati presidi di controllo, che possono influire sia sulla probabilità di accadimento che sul loro impatto (Monk & Wagner, 2009).

2.3 – *Le frodi aziendali ed i sistemi* ERP

Le frodi aziendali rappresentano una delle conseguenze più significative delle vulnerabilità nei sistemi ERP e dei controlli interni. Secondo Cressey (1953), le frodi aziendali possono essere definite come atti intenzionali volti ad ottenere un vantaggio ingiusto o illegale a scapito di un'organizzazione. La sua teoria denominata "triangolo della frode" identifica tre elementi simultaneamente presenti al verificarsi delle frodi: la pressione, l'opportunità e la razionalizzazione. Più in dettaglio, essi sono definibili come segue:

a1. *Pressione*: Gli individui possono sentirsi spinti a commettere frodi a causa di problemi finanziari personali o pressioni aziendali eccessive (Singleton *et al*., 2006).

b1. *Opportunità*: La presenza di controlli deboli o inesistenti offre ai malintenzionati l'opportunità di perpetrare frodi senza essere scoperti (Wolfe & Hermanson, 2004; Albrecht *et al*., 1984).

c.1 *Razionalizzazione*: Gli autori di frodi giustificano le loro azioni convincendosi che il loro comportamento è accettabile (Kassem & Higson, 2012).

Studi successivi hanno ampliato gli elementi il cui simultaneo concorso favorisce l'insorgere delle frodi aziendali, individuando dapprima un quarto elemento, ossia l'abilità del frodatore (Wolfe, 2004), poi quinto, l'arroganza (Crowe, 2011), ed anche un sesto elemento nella collusione con soggetti interni (Vousinas, 2019) ed anche un settimo elemento, nel piacere e brivido del rischio (Roffia & Poffo, 2025). Questi modelli sono stati definiti in letteratura rispettivamente *fraud diamond, fraud pentagon*, *fraud exagon* and *fraud polynomial*.

La pratica professionale ha censito numerosissimi schemi di frode, che possono essere raggruppati secondo diversi criteri (D'Onza, 2013). Una prima classificazione utile ai nostri scopi è la distinzione fra frodi interne e frodi esterne, a seconda del soggetto che la realizza. Le frodi interne, ossia realizzate da collaboratori in danno dell'organizzazione per cui lavorano, possono essere ulteriormente suddivise secondo lo schema rappresentato nell'albero delle frodi

occupazionali proposto da ACFE e riportato nel *Report to the Nation* (ACFE, 2024). Esso individua tre categorie "radice" di frodi occupazionali, ossia quelle di: corruzione, appropriazione di beni e frodi economico-finanziarie. Ciascuna di esse può essere ulteriormente suddivisa in numerose sottocategorie, a seconda del tipo di corruzione, del bene di cui ci si appropria o della tipologia di frode perpetrata relativamente all'informativa economico-finanziaria. Va segnalato come in taluni casi la frode non sia di un tipo soltanto (interna od esterna), bensì mista, con il concorso di soggetti sia interni che esterni all'organizzazione. Questo può ad esempio accadere nel caso di frodi compiute da fornitori o nel caso di frodi informatiche, allorquando ai soggetti esterni si aggiunge spesso la complicità di collaboratori interni. Circa le frodi esterne, la tipologia che ha conosciuto una forte crescita è quella di tipo informatico, alla luce della digitalizzazione informazioni relative alle operazioni aziendali, le interconnessioni fra la rete interna e quella esterna all'azienda e le difficoltà nel creare protezioni efficaci alle forme di comunicazione e scambio di dati.

Le conseguenze delle già menzionate vulnerabilità insite nell'utilizzo dei sistemi ERP sono spesso significative ed includono le seguenti:

a2. *Perdite economico-finanziarie*: le frodi compiute dai profili medio alti delle organizzazioni sono spesso numericamente inferiori ma hanno conseguenze molto importanti sui bilanci delle società, a differenza di quelle perpetrate dai blue collar che sono più numerose ma dagli effetti più limitati (ACFE, 2024; Wright & Wright, 2002).

b2. *Interruzione operativa*: Problemi conseguenti al rallentamento od al blocco delle operazioni aziendali relativamente ad uno o più processi od attività aziendali.

c2. *Danneggiamento del sistema informativo*: La compromissione dei dati intacca il funzionamento aziendale e richiede tempo per il loro ripristino.

d2. *Perdita della reputazione*: frodi aziendali ripetute possono intaccare la fiducia degli stakeholder e minare la sostenibilità della società.

Per prevenire o limitare gli effetti prodotti dalle frodi aziendali si raccomanda che le aziende impostino una "Fraud Governance", ossia un approccio strutturato per il contrasto delle frodi, con specifiche azioni di prevenzione, rilevamento ed investigazione. Nel dettaglio queste tre azioni sono come segue:

a3. *Prevenzione* (*Prevention*): Si basa su politiche, procedure e una cultura aziendale che promuove l'integrità e minimizza le opportunità di frode. È il pilastro su cui le aziende dovrebbero investire maggiormente per massimizzare il rapporto costo beneficio delle azioni di contrasto alla frode. Include la formazione del personale, la comunicazione delle aspettative etiche e delle azioni di contrasto alla frode messe in campo.

b3. *Rilevamento* (*Detection*): Comprende l'implementazione di sistemi per identificare tempestivamente comportamenti anomali o sospetti a partire da segnali potenziali di frode o red flags.

c3. *Investigazione* (*Investigation*): Sono le procedure adottate per raccogliere informazioni, analizzare e documentare frodi sospette anche con il supporto di consulenti esterni per predisporsi al contrasto anche in sede giudiziale.

Gli ERP forniscono un contributo fondamentale a tutte e tre queste azioni della *fraud governance*. Circa la prevenzione, attraverso un rafforzamento del sistema di controllo interno –

con interventi quali ad esempio la segregazione dei compiti (Li *et al*., 2019), la previsione di autorizzazioni specifiche per determinate operazioni, la protezione delle anagrafiche, i profili utenti con poteri differenziati, la tracciatura e storicizzazione di tutte delle operazioni – si può ottenere un effetto positivo riducendo l'elemento dell'opportunità del "triangolo della frode". In relazione alla seconda azione, il rilevamento della frode, gli ERP consentono un *monitoring* continuo sulle operazioni, rendendo possibile *audit trail* dettagliati (Spathis, 2002) e consentendo l'utilizzo di strumenti di *process mining*, attraverso cui individuare anomalie e *red flags* di frode all'interno del *work flow* dei processi aziendali. Da ultimo, relativamente all'investigazione, gli strumenti ERP consentono l'accesso a dati storici contenenti tutti i dettagli delle operazioni rilevate oltre che dei soggetti che vi hanno preso parte, permettendo la generazione di *report* dettagliati per le indagini.

2.4 – *Il contrasto delle frodi nel contesto di una buona corporate governance e sostenibilità aziendale*

Le recenti azioni dell'Unione Europea con l'adozione della *Corporate Sustainability Reporting Directive* (CSRD) e della *Corporate Sustainability Due Diligence Directive* (CSDD) hanno dato forte impulso in Europa al tema della "sostenibilità" delle aziende, dell'impatto delle loro scelte sul mondo circostante e degli eventuali effetti negativi prodotti sull'ambiente, sulle condizioni di lavoro, sui diritti e libertà degli individui, siano essi frutto di azioni intraprese direttamente che anche indirettamente, attraverso l'operato dei partner e collaboratori.

Parallelamente, anche sul fronte degli investitori e degli operatori nei mercati finanziari nell'ultimo decennio vi sono state forti spinte affinché gli investimenti si canalizzassero verso società con elevato *rating Environment, Social, and Governance* (ESG). L'ultima lettera dell'acronimo ESG, la G, quella forse meno enfatizzata dagli operatori, significa *Governance*, ossia le modalità con cui l'azienda è organizzata a partire dal vertice, nei temini della composizione ed attività dell'organo di governo (tipicamente il consiglio di amministrazione), della sua struttura organizzativa, dei valori etici e di condotta, della politica anti-corruzione, della struttura delle remunerazioni e degli incentivi ai collaboratori, della gestione dei rapporti con i partner e fornitori, dei rapporti con le influenze politiche e le *lobby*, della stessa qualità della *disclosure* sulla tematiche di sostenibilità (Biancone *et al*., 2024). Di questi aspetti, si deve dare conto nella rendicontazione di sostenibilità prodotta secondo lo standard ESRE G1 – *Business conduct* emanato dall'EFRAG, al quale sono tenute a conformarsi le società di grandi e piccola o media dimensione quotate sui mercati regolamentati dell'UE oltre che le società di grandi dimensioni non quotate con un calendario differenziato a seconda del tipo di società a partire dagli esercizi in corso nel 2024.

Sulla base delle precedenti considerazioni, siamo a formulare la seguente ipotesi di ricerca:

Hp1: *Un deficit nei controlli interni attivi nel sistema ERP aziendale costituisce un elemento di opportunità per le frodi aziendali e contribuisce negativamente alla loro prevenzione.*

3 – La Metodologia di ricerca ed i casi di studio

Lo studio adotta un approccio di tipo qualitativo, con l'analisi di un caso di frode relativo alla seconda società bancaria francese, Société Générale e di altri cinque casi di frode aziendale occorsi nel contesto italiano. Il caso di Société Générale è stato selezionato per l'attinenza al tema

della ricerca, la rilevanza della società nel contesto bancario europeo, per il danno economico prodottosi, nonché per la disponibilità di dati pubblici. A supporto dell'analisi e delle considerazioni che verranno fornite nella sezione della discussione sono stati analizzati anche altri cinque casi di studio relativi a PMI italiane od enti non lucrativi selezionati sulla base dello schema di frode attuato (di tipo interno e relativo ai controlli interni agganciati all'utilizzo dei software gestionali ERP) oltre che la disponibilità di informazioni pubbliche. La metodologia seguita ha compreso le fasi della raccolta dei dati tramite informazioni pubbliche presenti in rete internet (documenti ufficiali, report di audit, articoli di giornale e sentenze giudiziarie), la loro analisi tematica (come le carenze nei controlli interni, le vulnerabilità dei sistemi ERP e i comportamenti opportunistici dei collaboratori), la triangolazione delle fonti, che sono state poste a confronto fra loro, nonché l'interpretazione critica, in relazione al contesto considerato, al fine di trarre conclusioni possibilmente rilevanti sia per dottrina che per la pratica manageriale.

Siamo consapevoli della limitazione intrinseca nella metodologia adottata e delle difficoltà di generalizzazione dei risultati; tuttavia, riteniamo di poter accettare questa scelta alla luce del carattere esplorativo della ricerca e della difficoltà di poter impiegare altre metodologie di ricerca, come ad esempio la raccolta diretta di informazioni, per la delicatezza del tema frode oggetto di studio. E' peraltro nei piani di questa ricerca una sua estensione del campione considerato relativamente alla tipologia di frode considerata, al settore di appartenenza delle società, all'orizzonte temporale ed ai Paesi considerati.

3.1 – *Il caso di frode in Société Generale*

La frode perpetrata da Jérôme Kerviel nel 2008 rappresenta uno dei casi più eclatanti di fallimento dei controlli interni che, come è noto, sono radicati nelle grandi organizzazioni anche attraverso procedure e meccanismi operativi inseriti nei sistemi ERP. Société Générale è una società bancaria di grandi dimensioni, oggi la quarta banca operante in Francia, divisa in tre unità di business (Retail banking, Corporate ed investment banking, Global investment management & Services). Al tempo della frode la banca disponeva di oltre 150.000 collaboratori. Di seguito si riporta una cronologia degli sintetica eventi così da fornire una visione di insieme del contesto in cui operà Kerviel:

- 2005: Jérôme Kerviel entra a far parte del team di trading di Societé Générale. Grazie alla sua esperienza precedente in ruoli amministrativi, acquisisce una conoscenza approfondita delle procedure di controllo interno, inclusi i sistemi ERP e i meccanismi di verifica (Lichtblau, 2008).
- 2006-2007: Kerviel inizia a effettuare operazioni non autorizzate, sfruttando la sua conoscenza dei sistemi per mascherare le sue attività. Utilizza tecniche come la creazione di operazioni fittizie e la modifica manuale dei dati nei sistemi ERP per eludere i controlli (Vandewalle, 2009).
- Inizio Gennaio 2008: Le posizioni speculative di Kerviel raggiungono livelli estremamente elevati. Nonostante alcuni segnali d'allarme, come discrepanze nei dati e anomalie nei report, i controlli interni non riescono a individuare tempestivamente la frode (Societé Générale, 2008).

- Gennaio 2008: La frode viene scoperta quando un collega nota incongruenze significative nelle operazioni registrate. Un'indagine interna rivela che Kerviel aveva assunto posizioni non autorizzate per un valore complessivo di oltre 50 miliardi di euro, causando una perdita netta di circa 4,9 miliardi di euro per l'azienda (Le Monde, 2008).
- Ottobre 2010: Condanna in primo grado per tre capi di imputazione di cui Kerviel viene ritenuto colpevole: violazione della fiducia (riposta in lui dalla banca), inserimento fraudolento di dati nel sistema informativo, e falsificazione e uso di documenti falsi. Egli viene ritenuto il solo responsabile del danno di circa di circa 4.9 miliardi di euro subito dalla banca, che pertanto è tenuto a rimborsare, oltre a dover scontare 5 anni di carcere.

Dalla lettura dei fatti si possono cogliere tre elementi che hanno favorito il compimento della frode: le falle nei presidi di controllo del sistema ERP ed in generale nei controlli di primo, secondo e terzo livello, una insufficiente supervisione da parte dei vertici dell'organizzazione, una fiducia eccessiva nella capacità di deterrenza del sistema ERP. La mancanza di segregazione dei compiti, insieme all'assenza di *audit* adeguati e al monitoraggio inefficace, ha permesso a Kerviel di sfruttare vulnerabilità sistemiche per mascherare le sue attività. L'inadeguatezza e le disfunzioni dei controlli interni della banca è stata riconosciuta talmente evidente che la corte di appello di Versailles, nel 2014 ha ritenuto di rivedere la condanna di Kerviel ritenendolo soltanto "parzialmente colpevole" ed emettendo una sentenza di appello di condanna con cui è stata ridotta la sanzione pecuniaria a solo un milione di euro. Il caso Kerviel eclissa quello di Nick Leeson, il "*rogue trader*" che ha fatto perdere 1,5 miliardi di dollari a Barings Bank (UK), causando il fallimento della banca nel 1995, una delle più antiche *merchant bank* britanniche (1762 l'anno di nascita). Anche in quel caso erano stati falsificati i registri delle transazioni nei sistemi informatici.

3.2 – *Alcuni casi di frode aziendale nelle PMI e nelle organizzazioni non lucrative*

Anche nel contesto delle PMI e nelle organizzazioni non profit il supporto alla prevenzione delle frodi aziendali da parte degli ERP è possibile ed auspicabile. Tuttavia, rispetto alle aziende di grandi dimensioni, è la natura stessa di questi soggetti, strutturalmente più deboli sui controlli interni per le più limitate risorse di personale e finanziarie, che ne rende più difficile la realizzazione. Ciò premesso, di seguito si riportano le informazioni, anch'esse di dominio pubblico, relativamente a cinque casi di frode aziendale interna, con valore superiore ai duecentocinquantamila euro, accaduti nelle province di Brescia, di Treviso, Milano e Varese e riportati sulla stampa rispettivamente fra il 2016 ed il 2025.

Il primo caso riguarda una concessionaria per la vendita di autovetture in Valle Camonica (BS) dove un collaboratore amministrativo, godendo della piena fiducia dell'organo dirigente, ha potuto incassare somme di denaro per false operazioni di fornitura per le quali erano anche state create false fatture. La truffa si è perpetrata per oltre un anno ed è stata rilevata incrociando i dati contabili, i giustificativi di spesa, i conti correnti bancari ed i pagamenti effettuati dall'azienda. (Redazione Brescia Today, 2016).

Il secondo caso interessa una azienda produttrice di mangimi per animali sempre in provincia di Brescia, nella quale un collaboratore con funzioni di responsabile amministrativo ha fraudolentemente fatto apparire come pagamenti verso fornitori (fatture passive) operazioni con cui, invece, venivano distratte consistenti somme di denaro a favore di società appositamente costituite con il supporto di complici compiacenti e senza una reale

giustificazione economica (Rodella, 2023). Anche in questo caso la frode si è perpetrata nel tempo, grazie anche al fatto che i beneficiari dei pagamenti avevano nomi simili ai fornitori storici dell'azienda.

Il terzo caso riguarda sempre un caso di frode occupazionale occorsa in provincia di Treviso, questa volta per pagamenti non dovuti ad un collaboratore infedele, che era riuscito ad inserirsi nel pagamento complessivo degli emolumenti dovuti ai dipendenti, creando anche un dipendente "fantasma" il cui stipendio era accreditato sul suo conto. Anche questa frode si è perpetrata nel tempo ed è stata scoperta dall'azienda soltanto a distanza di molti mesi (Lipparini, 2023).

L'ulteriore caso di studio considerato riguarda il Comune di Verolavecchia, provincia di Brescia (Redazione Il Giorno, 2025a). I fatti accaduti sono stati quelli dell'addebito sui conti del Comune di numerosi mandati di pagamento con accredito ai conti personale di un collaboratore, che ha anche potuto incrementare il proprio stipendio, sempre grazie alla possibilità di disporre pagamenti. La frode si è perpetrata per molti anni e anche in questo caso siamo in presenza di una mancata segregazione dei ruoli, che, come si dirà più oltre, avrebbe forse potuto evitare l'accaduto.

L'ultimo caso che qui si riporta è quello di una fondazione teatrale in provincia di Varese, dove per quasi sei anni un impiegato amministrativo è riuscito a "giustificare" con operazioni inesistenti prelevamenti, bonifici ed utilizzi di carte di credito in danno dell'organizzazione (Redazione Il Giorno, 2025b).

Riprendendo il modello del "triangolo della frode", la pressione dichiarata dagli attori della frode è stata l'acquisto di beni di lusso, la passione per il gioco o anche più semplicemente l'accumulo di risorse finanziarie, mentre la razionalizzazione è sostanzialmente legata alla "banalizzazione" o "diffusione" del comportamento. Molto interessante, per il nostro contesto, l'analisi dell'opportunità, che è individuabile nella debolezza del sistema di controllo interno. Più particolarmente, la possibilità di gestire completamente in autonomia il ciclo passivo della ricezione delle fatture da fornitori ed il relativo pagamento del debito senza segregazione dei compiti ed autorizzazione di un superiore gerarchico costituisce una punto di debolezza dei controlli interni. Anche in questi contesti un sistema ERP correttamente configurato con la richiesta di approvazioni dei superiori gerarchici e la gestione delle operazioni con il concorso di più soggetti avrebbe potuto contrastare questa opportunità potenziale. Stesso dicasi nel caso di pagamenti cumulativi, con l'inserimento di un *report* di controllo di quadratura delle operazioni cumulative di pagamento.

I cinque casi di frode interna qui riportati sono soltanto una piccola parte di quelli accaduti nel contesto italiano e riportati sui media, non diversamente da quanto si potrebbe rilevare per il contesto europeo o nel resto del mondo. Per tutti possiamo osservare come i sistemi ERP avrebbero potuto costituire una barriera all'opportunità della frode se il rischio potenziale fosse stato investigato ed i controlli interni adeguatamente implementati. Questa considerazione vale anche nei contesti aziendali più grandi, dove la cultura dei controlli interni dovrebbe essere più sviluppata e la segregazione dei compiti garantita. Possiamo in questo senso riportare il caso di una multinazionale tedesca con sede in provincia di Varese finita alle cronache (Camurani, 2022) per "falsi" pagamenti ai fornitori, ossia disposizioni di pagamento a favore di propri conti correnti avvenuti fra il 2018 e 2019, dopo la sostituzione delle coordinate bancarie presenti nell'anagrafica fornitori. La separazione dei ruoli e la previsione di profili utente differenziati

per tipologia di operazione avrebbe probabilmente impedito questo tipo di operazioni fraudolente.

4 – Discussione

L'analisi condotta attraverso il caso di Société Générale e dei casi di frode interna nelle PMI e nelle organizzazioni non lucrative italiane evidenzia come i sistemi ERP possano giocare un ruolo cruciale nella prevenzione delle frodi aziendali, ma solo se adeguatamente configurati ed inseriti nel disegno di un adeguato sistema di controllo interno.

4.1 – *Il ruolo degli ERP nel controllo interno e nella prevenzione delle frodi*

Come emerso dalla letteratura, i sistemi ERP rappresentano un elemento chiave nel rafforzamento del sistema di controllo interno (Nicolaou, 2000; Li *et al*., 2019). Se ben progettati, essi possono contribuire a mitigare i rischi di frode attraverso la tracciabilità delle operazioni, la segregazione dei compiti e l'automazione di procedure di controllo. Tuttavia, l'efficacia di questi strumenti dipende dalla loro implementazione e dal livello di consapevolezza aziendale rispetto ai rischi associati alle frodi (Spathis, 2002; Li *et al*., 2019).

Nel caso Société Générale, la mancanza di segregazione dei compiti ed il monitoraggio inefficace delle transazioni hanno permesso a Jérôme Kerviel di manipolare i sistemi per un lungo periodo senza essere rilevato (Vandewalle, 2009). Questo evidenzia come un ERP, per quanto sofisticato, non possa essere considerato una soluzione autonoma alla gestione dei rischi aziendali, ma debba essere supportato da un framework di *governance* robusto e da un'adeguata cultura del controllo (COSO, 2013).

Analogamente, nei casi delle PMI e delle organizzazioni non lucrative italiane analizzati, le frodi sono avvenute in presenza di debolezze strutturali nel controllo dei processi contabili ed amministrativi, in particolare dall'assenza di meccanismi di autorizzazione e di controllo di quadratura delle operazioni. Un sistema ERP configurato con la segregazione delle funzioni e *audit trail* efficace avrebbe potuto ridurre significativamente le opportunità di frode, incidendo direttamente sulla componente dell'"opportunità" nel triangolo della frode di Cressey (1953). Ricerche precedenti hanno già evidenziato come l'integrazione di controlli nei sistemi ERP può ridurre il rischio di manipolazioni contabili e migliorare la trasparenza dei processi aziendali (Poston & Grabski, 2001; Wright & Wright, 2002).

Non di meno, l'inclusione di elementi di *detection* delle possibili frodi inseriti come *red flags* nei sistemi ERP può costituire un ulteriore barriera al perpetrarsi delle frodi, se è vero che tutte le frodi qui riportate sono state perpetrate per mesi se non anche anni.

In questo senso possiamo quindi confermare l'ipotesi di ricerca Hp1, ossia che un deficit dei controlli interni inclusi nel sistema ERP aziendale costituisce un elemento di opportunità per le frodi aziendali e contribuisce negativamente alla loro prevenzione (Nicolaou, 2000; Li *et al*., 2019).

4.2 – *Le implicazioni per la corporate governance e la sostenibilità aziendale*

Il collegamento tra frodi aziendali, corporate governance e sostenibilità è sempre più evidente nel contesto normativo attuale. La *Corporate Sustainability Reporting Directive* (CSRD) e la *Corporate Sustainability Due Diligence Directive* (CSDD) richiedono alle imprese europee di monitorare e rendicontare l'impatto delle loro attività, inclusi i rischi legati alla governance e alla gestione dei controlli interni (European Commission, 2022).

Le carenze nei sistemi di controllo, come quelle osservate nei casi analizzati, possono avere ripercussioni significative sulla sostenibilità aziendale, non solo in termini economico-finanziari ma anche in termini di reputazione e fiducia degli *stakeholder*. La mancanza di trasparenza e di meccanismi di *accountability* compromette la percezione dell'affidabilità dell'azienda, influenzando le sue relazioni con investitori, clienti e regolatori (Al-Mashari, 2003; Vousinas, 2019).

D'altra parte, le aziende che investono in sistemi ERP ben strutturati, con adeguate misure di controllo interno, possono beneficiare di un miglioramento complessivo della *governance* e della sostenibilità del *business*. L'integrazione di strumenti di monitoraggio avanzati, come il *process mining* e l'analisi predittiva, può fornire un ulteriore livello di protezione, consentendo un'identificazione tempestiva delle anomalie e una maggiore resilienza contro le frodi (Spathis, 2002; Li *et al*., 2019).

5 – Conclusioni

Questo studio ha analizzato il ruolo dei sistemi ERP nella prevenzione delle frodi aziendali, evidenziando come la loro implementazione possa rappresentare un valido supporto per il sistema di controllo interno, a patto che venga integrata con adeguate misure di controllo interno nelle sue componenti fondamentali.

Attraverso l'analisi dei casi di studio considerati abbiamo riscontrato come l'assenza di controlli interni efficaci all'interno degli ERP abbia facilitato il verificarsi delle frodi. I risultati supportano l'ipotesi di ricerca secondo cui un deficit nei controlli interni presenti negli ERP aumenta le opportunità di frode e contribuisce negativamente alla loro prevenzione. Dal punto di vista pratico, questo studio suggerisce alcune raccomandazioni per rafforzare l'efficacia degli ERP nella gestione del rischio frode. La prima è quella di migliorare la segregazione dei compiti, limitando l'accesso e le autorizzazioni agli utenti sulla base di principi di separazione delle funzioni (Wolfe & Hermanson, 2004). In secondo luogo, occorre tracciare tutte le operazioni aziendali e consentirne *l'audit trail*, così che la loro registrazione sia automatica e immodificabile, per favorire il rilevamento tempestivo di anomalie e risalire facilmente all'autore della transazione (Spathis, 2002). Ulteriormente occorrerebbe promuovere l'utilizzo di strumenti di analisi avanzata con tecnologie come il *process mining* e l'intelligenza artificiale per poter individuare pattern sospetti e segnali di frode (Vousinas, 2019). Inoltre, serve anche promuovere una cultura aziendale orientata alla trasparenza e alla *compliance* attraverso la formazione del personale e una forte etica aziendale (Kassem & Higson, 2012).

Questa ricerca ha adottato un approccio qualitativo basato su analisi di casi, con i limiti tipici di questa metodologia, tra cui la difficoltà di generalizzare i risultati. Futuri studi potrebbero ampliare il campione di casi analizzati o adottare metodologie quantitative per valutare in modo più preciso il rapporto tra implementazione degli ERP e riduzione del rischio frode.

Inoltre, la crescente diffusione di ERP *cloud-based* e l'integrazione con tecnologie emergenti come *blockchain* e *machine learning* potrebbero aprire nuove prospettive di ricerca sull'efficacia dei controlli interni in ambienti digitali più avanzati (Al-Mashari, 2003; Li *et al*., 2019).

6 – Referenze

Agliati, M., Caglio, A., Meloni, G., & Miroglio, F. F. (2001). *L'evoluzione della Funzione Amministrativa. Attività, professionalità e assetti nell'era dell'integrazione informativa*. Milano, Egea.

Albrecht, S., Howe, K. & Romney, M. (1984), *Deterring Fraud: The Internal Auditor's Perspective*, Institute of Internal Auditors Research Foundation, Lake Mary, FL.

Al-Mashari, M. (2003). Enterprise resource planning (ERP) systems: A research agenda. *Industrial Management & Data Systems*, *103*(1), 22-27.

Biancone, P. P., Chmet, F., & Demarchi, L. (2024). Analyzing non-Financial reporting through GRI-ESRS interoperability. *Economia Aziendale Online*, *15*(2), 375-394.

Bruni G., (1990). *Contabilità per l'alta direzione*. Etas Libri, Milano.

Caserio, C. (2019). Integrated information systems and information systems quality: Prospects for analysis and emerging trends. *Economia Aziendale Online*, *10*(2), 293-320.

Corbella, S. (2000). Il Sistema di Controllo Interno: una "rivisitazione" nella prospettiva dell'attività di auditing. *Rivista italiana di ragioneria e di economia aziendale*, *5*(5/6).

Camurani, A. (2022). Gallarate, frode informatica: alla contabile infedele sequestrate barca a vela e moto d'epoca. Corriere della Sera, Edizione Milano, 28 Jannuary 2022. Retrieved from: https://milano.corriere.it/notizie/lombardia/22_gennaio_28/gallarate-frode-informatica-contabile-infedele-sequestrate-barca-vela-moto-d-epoca-3bd3bc50-8011-11ec-9fac-a85f17701932.shtml.

COSO. (2013). *Internal Control - Integrated Framework*. Committee of Sponsoring Organizations of the Treadway Commission.

Cressey, D.R. (1953). *Other Peoples' Money*, Montclair, Glencoe: Free Press.

Crowe, H. (2011). Putting the Freud in Fraud: Why the Fraud Triangle Is No Longer Enough. Retrieved from: https://www.crowe.com/global.

Del Bene, L., Mucelli, A., & Spigarelli, F. (2012). Management control system and ERPs in Italian healthcare organizations. *Economia Aziendale Online*, (2), 1-26.

Davenport, T. H. (1998). Putting the enterprise into the enterprise system. *Harvard Business Review*, 76(4), 121–131.

D'Onza, G. (2013). *La prevenzione delle frodi aziendali: alle radici della responsabilità sociale*. Giuffrè, Milano.

European Commission (2022). Corporate Sustainability Reporting Directive (CSRD), Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2464, Accessed 12/02/2025.

European Commission (2022). Corporate Sustainability Due Diligence Directive (CSDD), Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2464, Accessed 12/02/2025.

IIA. (2013). *The Three Lines of Defense in Effective Risk Management and Control*. The Institute of Internal Auditors.

Redazione Il Giorno (2025a). Dipendente infedele truffa il Comune di Verolavecchia per 350mila euro. *Il Giorno*, Edizione Brescia, 17 Jannuary 2025. Retrieved from: https://www.ilgiorno.it/brescia/cronaca/comune-verolavecchia-truffa-impiegato-infedele-gxm2c4st.

Redazione Il Giorno (2025b). Teatro "Giuditta Pasta", viaggi e shopping con i soldi del teatro: denunciatala contabile della Fondazione. *Il Giorno*, Edizione Varese, 10 February 2025. Retrieved from: https://www.ilgiorno.it/varese/cronaca/fondazione-teatro-contabile-b07akh4o.

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs, and ownership structure. *Journal of Financial Economics*, *3*(4), 305–360.

Kassem, R., & Higson, A. (2012). "The New Fraud Triangle Model." Journal of Emerging Trends in Economics and Management Sciences, *3*(3), 191–195.

Le Monde. (2008). *Kerviel: Chronologie d'une affaire*. Retrieved from: https://www.lemonde.fr

Li, Y., Dai, J., & Vasarhelyi, M. A. (2019). *Audit Analytics and Continuous Monitoring in ERP Systems*. *Journal of Information Systems*, *33*(3), 109–128.

Lichtblau, E. (2008). Trader exploits flaws in oversight at French bank. *The New York Times*. Retrieved from: https://www.nytimes.com

Lipparini, V. (2023). Impiegata fa sparire 278mila euro dalle casse della sua azienda: "Sono malata di gioco" *Il Gazzettino*. Edizione del 18/01/2023. Retrieved from: https://www.ilgazzettino.it/nordest/treviso/serigrafia_diemme_impiegata_infedele_gioco_d_azzardo_san_vendemiano-7174032.html#:~:text=di%20Valeria%20Lipparini,corrente%20dell'azienda%20al%20proprio.

Marchi, L. (2003). *I sistemi informativi aziendali*. A. Giuffrè Editore.

Monk, E., & Wagner, B. (2009). *Concepts in Enterprise Resource Planning*. Cengage Learning.

Nicolaou, A. I. (2000). A contingency model of perceived effectiveness in accounting information systems: Organizational coordination and control effects. *International Journal of Accounting Information Systems*, *1*(2), 91–105.

Poston, R., & Grabski, S. (2001). Financial impacts of enterprise resource planning implementations. *International Journal of Accounting Information Systems*, *2*(4), 271-294.

Rashid, M. A., Hossain, L., & Patrick, J. D. (2002). The evolution of ERP systems: A historical perspective. *Information Systems Development*, 105-124.

Redazione Brescia Today (2016). Truffa il datore di lavoro per lo shopping: segretaria patteggia pena di due anni. *Brescia Today*, 06 March 2016.
Retrieved from: https://www.bresciatoday.it/cronaca/segretaria-truffa-furto-valle-camonica.html.

Rodella M., Contabile infedele ruba 790 mila euro dalle casse aziendali, no a patteggiamento. *Corriere della Sera* (2023), Edizione Brescia, 04 October 2023. Retrieved from www.corriere.it. Accessed: 14/02/2025.

Shang, S., & Seddon, P. B. (2002). Assessing and managing the benefits of enterprise systems: The business manager's perspective. *Information Systems Journal*, *12*(4), 271–299.

Sihombing, T., & Panggulu, G. E. (2022). Fraud Hexagon Theory And Fraudulent Financial Statement In IT Industry In Asean. Jurnal Reviu Akuntansi dan Keuangan, *12*(3), 524-544.

Singleton, T. W., Singleton, A. J., Bologna, G. J., & Lindquist, R. J. (2006). *Fraud auditing and forensic accounting*. John Wiley & Sons.

Societé Générale. (2008). *Kerviel case: Internal investigation report*. Retrieved from: https://www.socgen.com

Spathis, C. (2002). Enterprise systems implementation and accounting benefits. *Journal of Enterprise Information Management*, *15*(4), 103–120.

Vandewalle, N. (2009). Understanding the Kerviel affair: Failures in control and governance. *European Financial Review*, *23*(1), 45–54.

Vousinas, G. L. (2019). Advancing Theory of Fraud: The S.C.C.O.R.E. Model. *Journal of Financial Crime*, *26*(1), 372-382.

Wolfe, D. T., Hermanson, D., R. (2004). The Fraud Diamond: Considering the Four Elements of Fraud. *The CPA Journal*, *74*(12), 38-42.

Wright, S., & Wright, A. (2002). Information system assurance for enterprise resource planning systems: Unique risk considerations. *Journal of Information Systems*, *16(s-1)*, 99-113.