Deloitte.
Private

Rafforzare i controlli interni per migliorare il *risk management*

Introduzione

Le aziende private e le imprese familiari spesso si compiacciono del loro status di operatori sottoposti a regolamentazioni meno stringenti rispetto alle aziende quotate o di pubblico interesse. In particolare, i requisiti di segnalazione meno esigenti e la meno invasiva presenza di controllo esterno, fanno sì che molti operatori privati assumano di poter essere più agili e liberi di concentrarsi sulle loro priorità aziendali più strategiche.

Ma questa libertà relativa può implicare che le aziende che hanno meno presidi attivi per gestire il rischio incorrano in incidenti che ne minano l'affidabilità ed il valore oltre che la reputazione sul mercato. La mancanza di controlli interni efficaci può causare la perdita di risorse a causa di inefficienze non rilevate, o di furti, mentre soluzioni inappropriate di reazione e di non prevenzione del rischio, possono danneggiare la reputazione e la credibilità della gestione presso stakeholder e investitori.
Gran parte dell'attenzione rivolta ai programmi di gestione del rischio aziendale (ERM) da parte di aziende private, anche familiari, è determinata da battute d'arresto avvenute che avrebbero potuto essere evitate del tutto se il sistema di controllo interno fosse stato efficace.

Aspetto su cui, a volte, non ci si focalizza nella discussione sui controlli interni è il come potenziare il processo decisionale, in quanto l'organizzazione conduce i suoi leader a fare affidamento su informazioni inesatte o incomplete in merito all'importanza del controllo interno. I leader delle aziende private e delle imprese familiari, in casi non sporadici, assumono che i controlli interni compromettano l'agilità aziendale, quando invece, in molti casi, è vero l'esatto contrario. Quasi tutte le decisioni importanti che i leader intraprendono si basano sulla qualità delle informazioni a loro disposizione. I controlli interni offrono loro un comfort maggiore, poiché le informazioni che hanno a disposizione sono attendibili, consentendogli di agire con velocità e sicurezza.

Per molti versi, i controlli interni efficaci sono come un sistema di controllo del traffico aereo, il cui obiettivo non è rallentare il traffico o impedire agli aerei di volare, quanto piuttosto di permettergli il movimento senza soluzione di continuità e in modo sicuro.

Le imprese private e le imprese familiari dovrebbero considerare nello stesso modo il sistema di controllo interno. Le minacce di contesto si palesano improvvisamente, con impatti immediati, creando la necessità, per i responsabili aziendali, di raccogliere informazioni accurate rapidamente e agire con decisione. Questa capacità di azione, resa possibile da buoni controlli interni, può fare la differenza tra il decollare e il rimanere a terra. Inoltre, le aziende private, con la flessibilità tipica della ridotta regolamentazione, hanno l'opportunità di ispirarsi alle *best practice* di disegno e implementazione dei controlli interni adottate dalle aziende maggiormente regolamentate, accogliendo ciò che funziona meglio e si attaglia alla loro organizzazione e cultura aziendale.

La domanda da porsi allora è *Da dove iniziare?*

Iniziare con il *risk assessment*

Nel primo articolo di questa serie è stato approfondito il rischio che, nella fase di *risk assessment*, non vengano correttamente indentificati i processi critici di un'organizzazione, creando rischi non necessari per l'azienda. Una valutazione dei rischi relativa ai controlli interni ben eseguita inizia con la comprensione di ciò che è rilevante per l'azienda e di quali sono i processi più importanti.

Da lì, si tratta di documentare i processi e i controlli correnti e identificare le inefficienze nel processo, nonché le potenziali lacune nei controlli. Una volta individuate tali lacune, i responsabili del rischio possono stimare il tempo e gli sforzi necessari per affrontarle e definire un piano di risoluzione passo dopo passo.

La maggior parte delle aziende private ha una serie di policy e procedure di elaborazione delle transazioni. Una assunzione non corretta, fatta da molte aziende, è che una policy o una procedura ben disegnata funga anche da controllo stesso. Procedure e i controlli **non** sono la stessa cosa.

La distinzione tra procedura e controlli è fondamentale perché hanno due scopi molto diversi. Una *procedura* disciplina il modo in cui viene elaborata una transazione o il modo in cui un utente esegue una determinata attività; un *controllo* è un meccanismo che viene messo in atto per garantire che la procedura venga eseguita nel modo in cui è stata disegnata.

Si consideri un semplice esempio di effettuazione di pagamento ai fornitori. Molte aziende hanno una policy che stabilisce che prima che un fornitore possa essere pagato, ci deve essere un triplice controllo tra le quantità e i prezzi tramite: (1) l'ordine di acquisto approvato, (2) la prova che le merci sono state consegnate e (3) la fattura ricevuta dal fornitore.

In questo esempio, ci sono diverse procedure per garantire che ci sia l'effettuazione della triplice verifica: è presente una procedura di approvazione dell'ordine di acquisto, una relativa alla ricezione delle merci in magazzino ed una in cui qualcuno immette la fattura nel sistema; inoltre, c'è una procedura per abbinare i tre elementi insieme e inviare il pagamento.

Ma quale controllo è in atto per garantire che questi processi vengano eseguiti come previsto? Come si fa a sapere che i fornitori non vengano pagati prima che si verifichino questi passaggi? Come fa l'azienda a sapere che i prezzi e le quantità tra l'ordine di acquisto, la ricezione delle merci e la fattura corrispondano? Come fa l'azienda a sapere che l'importo pagato al fornitore è giusto?

In questo esempio, si potrebbe disegnare un controllo in base al quale una persona, indipendente dal processo di verifica, esegua una analisi della documentazione prima dell'esborso per garantire che tale verifica sia avvenuta e che tutto sia coerente. Un'altra opzione di controllo potrebbe essere che un'azienda configuri il proprio sistema ERP in modo da impedire il pagamento a un fornitore senza che prima siano soddisfatti tutti i campi richiesti nel sistema per certificare l'avvenuta effettuazione dei controlli, ad evidenza dell'avvenuta effettuazione delle procedure sopra richiamate.

Distinzione tra controlli preventivi e di monitoraggio

Dopo la fase di *risk assesment*, l'attività si sposta sul disegno e l'implementazione dei controlli. È importante trovare un equilibrio tra controlli preventivi e controlli di monitoraggio.

Nella nostra esperienza, molte aziende private, in particolare quelle meno strutturate, tendono a fare più affidamento sui controlli di monitoraggio. Come suggerisce il nome stesso, tali controlli di monitoraggio sono pensati per rilevare un errore o un problema dopo che si è verificato, ma prima che una *deficiency* di poca rilevanza si trasformi in qualcosa di maggiore dimensione. I controlli di monitoraggio non aiutano a evitare che il problema si verifichi (come se i sistemi di controllo del traffico aereo emettessero un allarme solo dopo che si è verificato un incidente), ma a ridurne l'impatto ad esito di accertamento dell'accaduto.

I controlli preventivi, al contrario, contribuiscono in primo luogo ad evitare che si realizzino situazioni di *deficiency*. Tornando all'esempio sul pagamento ai fornitori, la maggior parte delle aziende vorrebbe evitare che pagamenti non approvati, inaccurati o fraudolenti vengano mai eseguiti. Ma questo spesso non accade in aziende che non hanno investito in controlli interni e che invece si aspettano di identificare tali questioni analizzando eventuali variazioni in estratti conto bancari o bilanci mensili. È vero che questi controlli potrebbero identificare pagamenti non autorizzati, imprecisi o fraudolenti, ma dopo che sono avvenuti; perché non considerare di poterli evitare fin dall'inizio?

Questa tipologia di controllo preventivo può essere ottenuta anche senza ricorrere a una notevole quantità di richieste di documentazione da parte del responsabile del controllo. Le aziende private e familiari sono riluttanti a intraprendere iniziative di ERM, perché sono preoccupate di rallentare la gestione aziendale. In un webinar Deloitte Private è emerso che quattro executive di aziende private su dieci hanno affermato che la loro impresa ha disegnato controlli interni non chiaramente documentati o non ne ha disegnati affatto. Ed invece, per un efficace *risk management*, risulta necessaria una certa formalizzazione per far sì che tutti si orientino nella stessa direzione, e questo significa avere controlli espliciti e ben documentati che aiutino le persone a tutti i livelli a prendere decisioni migliori.

La perfezione non è l'unico criterio

Si dice spesso che la gestione dei rischi si basi su tre fattori fondamentali: persone, processi e tecnologia. Tuttavia, il modo in cui ogni organizzazione combina questi fattori per ottenere il massimo effetto varia ampiamente e i vincoli di risorse spesso evidenziano che la combinazione ottimale è inarrivabile. Quando manca la competenza, ad esempio, l'aggiunta di personale potrebbe non essere una soluzione praticabile per migliorare un ambiente di controllo. Risorse limitate, sia di competenza che finanziarie, rappresentano una sfida comune per le aziende private e familiari. Nello stesso webinar Deloitte Private precedentemente richiamato, quasi la metà dei dirigenti aziendali ha dichiarato che il tempo e le risorse limitate sono le barriere più significative per eseguire una valutazione appropriata dei rischi o implementare controlli interni. Molti semplicemente non hanno abbastanza personale nel back-office con le competenze richieste per sviluppare e mantenere un sistema formale di controllo interno.

Questo può portare a una sorta di circolo vizioso: le aziende con back office poco numerosi, che non dispongono delle risorse necessarie per mettere a punto un adeguato sistema di controllo, sono anche comunemente quelle più a rischio di creazione, segnalazione e utilizzo di informazioni finanziarie e operative inadeguate. Situazione che i controlli adeguatamente disegnati dovrebbero invece evitare. Per queste aziende, è importante capire che la ricerca della perfezione potrebbe ostacolare l'introduzione di controlli solidi ed efficaci. Quando un'organizzazione può implementare (o introdurre) controlli automatizzati anziché manuali, o preventivi invece che di monitoraggio, l'efficacia del controllo può aumentare. Tuttavia, effettuare un controllo di monitoraggio e manuale risulta più efficace di non aver controlli.

Riprendendo ancora una volta l'esempio del pagamento, in un mondo ideale con risorse illimitate sarebbe ottimale implementare controlli automatizzati all'interno di un sistema ERP per eseguire automaticamente, in modo preventivo, la verifica di triplice corrispondenza e autorizzare il pagamento, o rifiutarlo in caso di discrepanze. Se le persone, i processi o la tecnologia non sono disponibili per far sì che ciò accada, va considerata la possibilità di mettere in atto controlli di monitoraggio come punto di partenza. Va inoltre tenuto conto che molti degli strumenti di automazione del flusso di lavoro disponibili sul mercato sono relativamente economici, in quanto i provider li includono come soluzione standard del loro pacchetto, e stanno aiutando molte aziende private a fare di più in ambito di controllo predittivo.

In breve: non focalizzarsi nella ricerca della perfezione perché ciò raramente è compatibile con il concetto di sistema di controllo che, per definizione, implica flussi e processi soggetti ad imperfezione. Il punto importante è iniziare questo processo, identificando le aree più a rischio per poi concentrarsi sul miglioramento continuo. E tale meccanismo può avviarsi, iniziando a rispondere ad alcune domande sullo stato attuale dei controlli interni della propria azienda:

- Quali rischi, se verificatisi, potrebbero avere il maggiore impatto sull'azienda?
- Dove sono i rischi che potrebbero compromettere la contabilità o la capacità di acquisire, aggregare e riportare i dati?
- In che modo il management sa quali rischi impattano l'operatività?
- Quali sono i criteri per analizzare eventuali evoluzioni del grado di rischio?
- Chi valuta e approva le transazioni o scritture contabili?
- In quali casi ci si affida ancora a processi manuali che sono soggetti a giudizi ed errori?

Nel prossimo articolo della serie verranno esaminate le implicazioni dell'ERM nella gestione della crescente minaccia del rischio informatico.

In virtù dell'esperienza maturata nei contesti più diversi, **Deloitte Private** sviluppa progetti di collaborazione che si fondano sulle reali esigenze espresse dai clienti, creando per loro soluzioni su misura in base alle loro dimensioni e alla loro storia. Partendo dall'ascolto dei bisogni, Deloitte Private affianca l'imprenditore posizionandosi come *Trusted Business Advisor* di soluzioni multidisciplinari destinate a:

- Le imprese familiari e i loro imprenditori e famiglie
- I *Family Office* e gli investitori privati con i loro consulenti (*private banker* e *wealth manager*)
- Le Piccole e Medie Imprese quotate e non quotate
- I *Private Equity*, con portafoglio dedicato alle Piccole e Medie Imprese
- Le micro-imprese, anche in forma di start-up

CONTATTI ITALIA

Ernesto Lanzillo
Deloitte Private Leader Deloitte Central Mediterranean (Italia, Grecia e Malta)

elanzillo@deloitte.it

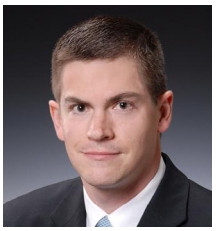
Ezio Pagliano
Partner Deloitte Risk Advisory, Enterprise Risk Management Expert

epagliano@deloitte.com

AUTORI

Kevan Flanigan
US Deloitte Private Leader, Risk & Financial Advisory US Deloitte Private Leader, Private Equity

keflanigan@deloitte.com



Aaron Zboril
Audit & Assurance Managing Director

azboril@deloitte.com

Deloitte.

Deloitte Creative Team - Italia | SG.008.24