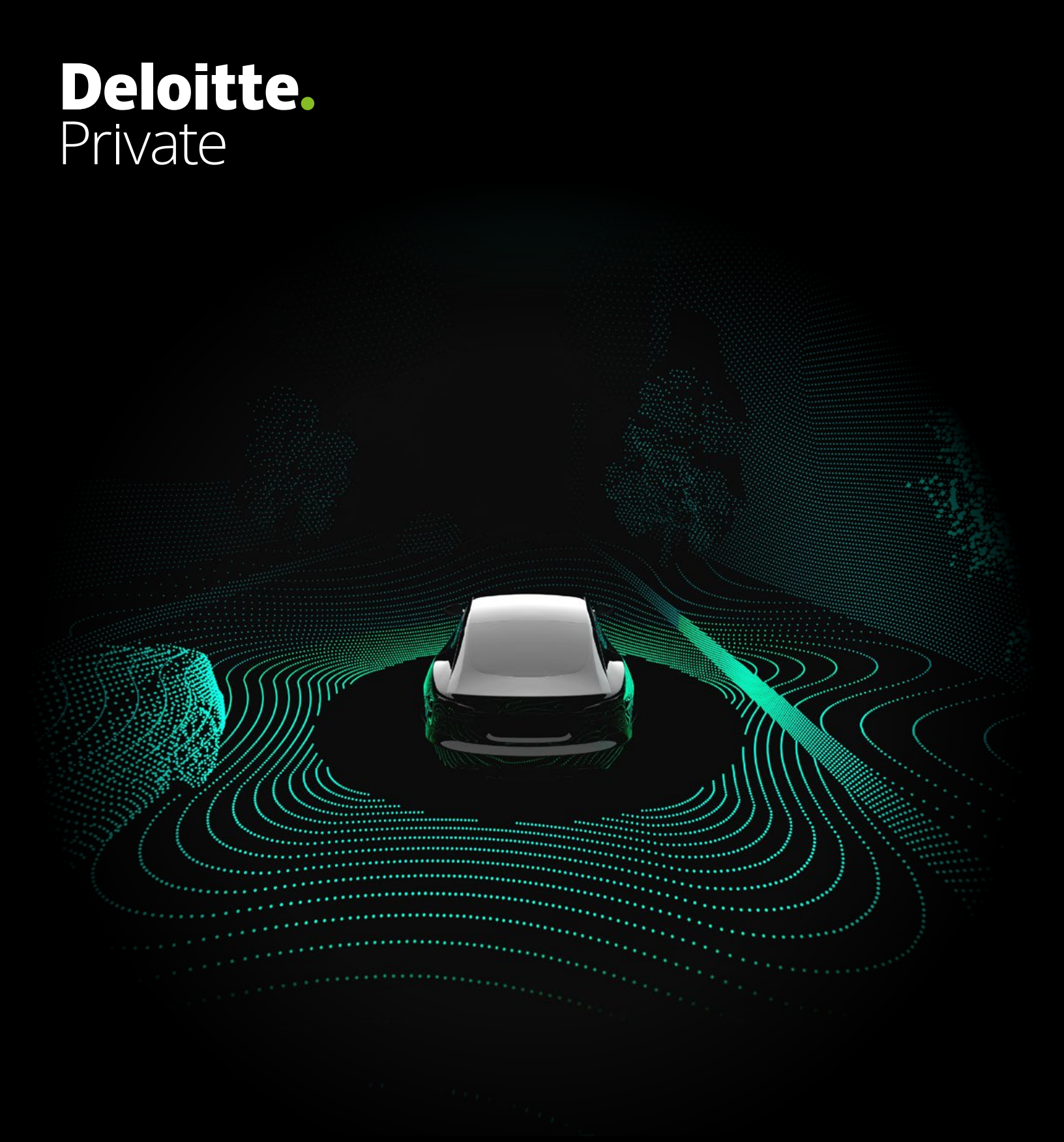
Deloitte.
Private



Monitoraggio intelligente dei rischi operativi

Introduzione

Le aziende possono affrontare i rischi operativi in ogni momento. Indipendentemente dal fatto che siano immediatamente evidenti o meno, questi pericoli possono provenire dall'interno come, ad esempio, quelli derivanti dalla cattiva condotta dei dipendenti, dalla gestione impropria dei dati, o dalla inadeguatezza del sistema di controllo interno. Inoltre, possono anche provenire dall'esterno, come dalle azioni di terze parti e da dubbi culturali ed etici derivanti dall'operatività in un contesto globale. Oltre a questi rischi, si aggiunge la prospettiva di reagire troppo lentamente a evoluzioni della tecnologia "disruptive". Da qualsiasi direzione provengano, molti di questi rischi possono iniziare con la forma di piccoli fallimenti incrementali che diventano poi fallimento di sistema aziendale.

L'elenco delle specifiche vulnerabilità è lungo e può riguardare ogni parte di un'organizzazione. Un'ampia gamma di settori si trova ad affrontare una carenza di forza lavoro e una strategia di gestione del rischio aziendale adatta in passato potrebbe non esserlo a causa delle sfide tecnologiche e digitali di oggi (Figura 1). Queste e altre questioni diventano cruciali per molte realtà e i leader aziendali cercano di adattarsi al contesto di incertezza geopolitica ed economica in atto ed alle evoluzioni di contesto digitale.

Per affrontare queste minacce in evoluzione, le aziende possono fare affidamento su un monitoraggio "sempre attivo", simile alle auto autonome che offrono questo tipo di protezione. Si tratta di prodotti con uno o più sensori radar utili a rilevare rischi come veicoli e oggetti nelle vicinanze, rimanere nella propria corsia oppure eseguire arresti di emergenza. L'idea alla base è che i singoli componenti di un sistema necessitano di un monitoraggio continuo per evitare conseguenze negative.

Figura 1: Tematiche più rilevanti in ambito di tecnologia e rischio digitale nel 2024, secondo il Deloitte Center for Board Effectiveness

Classifica	In tutti i settori	Servizi finanziari	Servizi non finanziari
1	Sicurezza informatica	Sicurezza informatica	Sicurezza informatica
2	Trasformazione digitale e cambiamento IT	Ambienti cloud	Gestione e qualità dei dati
3	Gestione e qualità dei dati	Trasformazione digitale e cambiamento IT	Intelligenza artificiale
4	Intelligenza artificiale	Resilienza tecnologica	Trasformazione digitale e cambiamento IT
5	Ambienti cloud	Outsourcing e terze parti critiche	IT preesistente e semplificazione
6	Resilienza tecnologica	Gestione e qualità dei dati	Ambienti cloud
7	Outsourcing e terze parti critiche	Intelligenza artificiale	Resilienza tecnologica
8	IT preesistente e semplificazione	Identità e gestione degli accessi	Outsourcing e terze parti critiche
9	Identità e gestione degli accessi	IT preesistente e semplificazione	Identità e gestione degli accessi
10	Trend tecnologici emergenti: Risorse digitali e blockchain, regime di controllo del Regno Unito, marketing responsabile e canali digitali	Trend tecnologici emergenti: Risorse digitali e blockchain, marketing responsabile e canali digitali	Trend tecnologici emergenti: regime di controllo del Regno Unito, marketing responsabile e canali digitali

Tenere il passo e mantenere il controllo sulla proprietà intellettuale (IP)

Un modo in cui i rischi aziendali si sono evoluti negli ultimi mesi è legato alla crescente adozione di tecnologie emergenti come l'intelligenza artificiale generativa (Gen AI). Ma c'è un altro lato rispetto alle principali sfaccettature della tecnologia, come il codice generato dall'Intelligenza Artificiale e i modelli basati sul linguaggio naturale. Una recente survey rivela che il 56% dei responsabili IT e Information Security intervistati sta esplorando attivamente soluzioni per rafforzare la posizione di sicurezza delle proprie organizzazioni per affrontare i rischi associati all'Intelligenza Artificiale. Nel sondaggio, il 34% delle organizzazioni dichiara di utilizzare già o di implementare strumenti di sicurezza per evitare questi rischi emergenti derivanti dall'Intelligenza Artificiale.

Mentre le aziende delineano i piani per monitorare i rischi legati all'Intelligenza Artificiale, una delle principali preoccupazioni è quella di mantenere la loro proprietà intellettuale sicura. Alcune aziende che utilizzano l'Intelligenza Artificiale generativa hanno dovuto affrontare critiche per aver utilizzato materiale protetto da copyright senza avere il permesso di "addestrare" le richieste dell'Intelligenza Artificiale con materiale protetto. Inoltre, alcune aziende hanno proibito l'uso dell'Intelligenza Artificiale generativa perché i dipendenti hanno utilizzato dati proprietari tramite il ricorso all'Intelligenza Artificiale di tipo generativo che alla fine sono trapelati al di fuori dell'organizzazione.

Le incertezze possono accumularsi nel tempo, causando potenzialmente problematiche più ampie. Se una società non è in grado di gestire e proteggere efficacemente la proprietà intellettuale, può rischiare di perdere il controllo dei propri beni proprietari e di conseguenza affrontare conseguenze di tipo legale, finanziario e competitivo.

Alcune domande che tali realtà potrebbero porsi sono:

- Il patrimonio informativo aziendale è veramente protetto?
- Il patrimonio informativo aziendale è considerato proprietà intellettuale?
- Qual è la azione di rimedio in caso di perdita di controllo degli asset proprietari?

Coinvolgere leader e partner

Sebbene le capacità di monitoraggio dei rischi si evolvano, queste non dovrebbero essere sempre lasciate lavorare in background, anche nel caso di supporto tramite sistemi di controllo interni, trattati in articoli precedenti. I leader aziendali dovrebbero contribuire a mantenere le loro organizzazioni sulle buone prassi, facendo evolvere le capacità di monitoraggio dei rischi attingendo a nuovi livelli di competenza per affrontare le sfide operative.

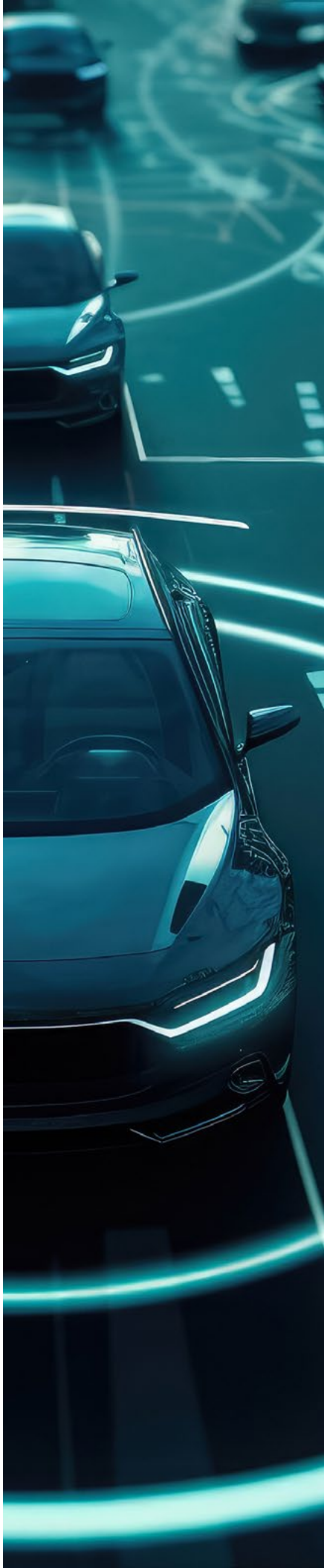
Nello sviluppo della gestione dei rischi operativi emergono posizioni come quella del Chief Trust Officer, il cui ruolo sta assumendo importanza in quanto figura responsabile del monitoraggio delle esigenze dei clienti, della spinta verso decisioni affidabili e della promozione di iniziative che rinforzano la responsabilità e fiducia aziendale. Secondo un'indagine Deloitte, il 62% delle persone che riferisce di avere un'elevata fiducia in un marchio acquista quasi esclusivamente da quel marchio rispetto ai concorrenti della stessa categoria.

Consapevolezza e intelligenza legate al tema del rischio sono fattori chiave per garantire il successo dei Consigli di Amministrazione e del management nel governo dell'organizzazione. Ad esempio, i Consiglieri possono fornire un differente livello di percezione del rischio con nuovi punti di vista e di attenzione. Alcuni Consigli di Amministrazione designano comitati con responsabilità di supervisione dei rischi, come ad esempio un "comitato compliance" o un "comitato risk management" che sono incaricati di interrogare il management rispetto alla posizione di rischio dell'organizzazione.

Inoltre, alcune realtà possono decidere di interagire con stakeholder esterni, come organizzazioni commerciali o non - profit specializzate in supporto al miglioramento delle attività aziendali. Questi input possono essere utili per migliorare e influenzare le pratiche di gestione del rischio e creare una cultura del rischio "intelligente".

A seconda della cultura di rischio, del "risk appetite" o della "attitudine al rischio" dell'azienda, in genere esiste un Membro del Consiglio di Amministrazione responsabile di monitorare le decisioni prese del management che possono influenzare il profilo di rischio dell'azienda. Questa figura verifica che le decisioni prese dal management siano in linea con la strategia generale di rischio dell'azienda e pone domande pertinenti per contribuire a mantenere una posizione di rischio equilibrata e adeguata.

Naturalmente, ogni azienda ha la sua tolleranza al rischio. Alcune realtà adottano un approccio al rischio più aggressivo, che potrebbe essere allineato agli obiettivi di crescita; altre, invece, hanno una posizione più cauta. Qualunque sia la posizione di rischio assunta dall'azienda, è importante capire quando le decisioni di gestione espongono l'organizzazione a rischi aggiuntivi. Tale responsabilità spesso spetta al Consiglio di Amministrazione, che esamina le decisioni e garantisce che siano in linea con i valori, gli obiettivi e i livelli di rischio accettabili da parte dell'azienda.



Creare una cultura di capacità reattiva

Possedere una cultura che tenga conto dei rischi aziendali sottostanti è un punto di partenza importante, ma avere misure di protezione e sapere come attivarle tempestivamente, reagendo ai rischi che si palesano, è il passo successivo che conferisce un maggiore senso di sicurezza. I leader dovrebbero essere vigili e coerenti nella comunicazione delle buone pratiche relative ai processi come quelle di condivisione di dati e di accesso ai sistemi. Per le aziende manufatturiere, è necessario che vi sia una valutazione continua sulle modalità che garantiscono la corretta produzione dei prodotti. I leader dovrebbero impostare il "tone at the top" per implementare i comportamenti più appropriati all'interno della loro azienda a qualsiasi livello di operatività. Gli audit possono individuare discrepanze e generare segnali d'allarme; tuttavia, le aziende possono aver bisogno di processi operativi e controlli solidi e continui per proteggersi.

Ecco alcuni modi per iniziare a garantire che i rischi operativi non escano dal radar:

Definire l'attitudine al rischio. Iniziare con una valutazione dei rischi, includendo struttura operativa, ambiente normativo ed esposizione alle minacce, al fine di proteggere ambienti complessi, prepararsi a potenziali incidenti e ridurre al minimo i tempi di inattività derivanti da scenari di interruzione delle attività. Per quanto riguarda il rischio informatico, ad esempio, un Consiglio di Amministrazione potrebbe voler sapere se c'è un'enfasi sui rischi di sicurezza al di fuori dell'IT.

Prestare attenzione all'esperienza dell'utente. Invece di ricorrere a manuali di grandi dimensioni e ingombranti su processi e procedure, è cruciale pensare a come utilizzare l'esperienza dell'utente a vantaggio di tutti. Fornire le policy in un formato facile da comprendere e incoraggiare la comunicazione costante e il rafforzamento della circolazione delle informazioni sul come gestire al meglio ed in sicurezza i processi. Anche per i dettagli più critici, ciò che è fondamentale è ottenere il *buy-in*, quindi pensare a modi per garantire che le persone possano conservare le informazioni e avere un incentivo a implementare le prassi considerate migliori per evitare che quei rischi si concretizzino. Ciò può essere particolarmente utile nelle organizzazioni con un *turnover* elevato e un limitato periodo di *on-boarding* dei nuovi assunti.

Non dimenticare i dettagli. Anche se molte aziende private possono essere grandi e complesse come le maggiori aziende pubbliche, spesso hanno un livello di controllo inferiore. Ed invece, anche nelle aziende private è importante disporre di controlli operativi rigorosi. Dopotutto, una mancanza di disciplina operativa in aree come esigenze di capitale, tecnologia o transizioni di leadership potrebbe spingere compromettere l'ascesa dell'azienda più innovativa e all'avanguardia.

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, Deloitte Transactions and Business Analytics LLP

keflanigan@deloitte.com

James Cascone
Partner and Sustainability, Climate & Equity (SC&E) Leader Deloitte & Touche LLP

cjcascone@deloitte.com

Deloitte.

Deloitte Creative Team - Italia | SG.008.24