10 passi essenziali per ottimizzare la gestione del rischio di terzi (TPRM)

APRILE 2020

White Paper/Guida

OneTrust Vendorpedia™
THIRD-PARTY RISK SOFTWARE

10

Passi essenziali per ottimizzare la gestione del rischio di terzi (TPRM)

La gestione del rischio di terzi (TRRM, Third-Party Risk Management) non è un concetto nuovo, tuttavia, gli eventi recenti hanno portato la disciplina in primo piano come mai prima d'ora. Le organizzazioni di tutti i settori si affidano a terzi, che si tratti di provider di servizi cloud, fornitori o collaboratori subordinati.

Fondamentalmente, quando la catena di fornitura viene interrotta, o le terze parti non sono in grado di fornire, possono verificarsi impatti devastanti e di lunga durata. In questo breve whitepaper, descriveremo i 10 passi essenziali che le organizzazioni possono intraprendere per costruire un programma TPRM efficiente.

FASE UNO: STABILIRE LE BASI DEL PROGRAMMA

1. Delimitare la propensione al rischio

L'Institute of Risk Management descrive la propensione al rischio come "la quantità e il tipo di rischio che un'organizzazione è disposta ad assumersi per raggiungere i propri obiettivi strategici".

La propensione al rischio varia da azienda a azienda e il modo migliore per descrivere la propria è sviluppare una dichiarazione sulla propensione al rischio. Il Peter Firstbrook di Gartner offre i seguenti consigli: "Per evitare di focalizzarsi esclusivamente sulle questioni relative alle decisioni in ambito IT, creare dichiarazioni di propensione al rischio semplici, pratiche e pragmatiche, che siano collegate agli obiettivi aziendali e rilevanti per le decisioni a livello di consiglio di amministrazione". Firstbrook collega le dichiarazioni di propensione al rischio direttamente ai risultati aziendali.

Quindi, per capire quale rischio si è disposti ad accettare, è necessario sviluppare prima di tutto una dichiarazione di propensione al rischio.

2. Riflettere sui rischi

Esistono due termini comuni legati al rischio, spesso associati alla TPRM.

RISCHIO INERENTE:	Il rischio potenziale o il rischio non trattato senza alcun controllo in atto
RISCHIO RESIDUO:	Il rischio rimanente dopo l'attuazione dei controlli di sicurezza

Il rischio inerente è spesso utilizzato per classificare i fornitori in base alla criticità, di cui parleremo nella terza fase di questo whitepaper. Il rischio residuo è, in ultima analisi, una delle metriche più importanti per qualsiasi programma di TPRM. Tuttavia, il tracciamento dei rischi residui può essere complesso e dovrebbe essere pensato a strati, includendo:

Il fornitore	Asset, app, prodotti o servizi forniti dal fornitore
L'impegno individuale relativo alle modalità di utilizzo di asset, app, prodotti o servizi	I singoli processi aziendali coinvolti

Solo attraverso un'analisi a livello di processo aziendale è possibile comprendere veramente i rischi associati ai propri fornitori. Senza dimenticare che non è necessariamente il fornitore a presentare il rischio, ma piuttosto *come il fornitore viene utilizzato e quali dati sono coinvolti.*

FASE DUE: CREARE UNA SOLIDA BASE

3. Scelta degli standard e framework

Lo standard adeguato per un' organizzazione dipende principalmente dal suo programma di rischio interno, oltre che dall'industria, dalla regione e da altri fattori correlati. Molte organizzazioni selezionano uno standard e lo personalizzano per soddisfare le loro esigenze. Alcuni degli standard e dei framework più comuni utilizzati per valutare le terze parti sono:

SFG SHARED ASSESSMENTS The Trusted Source in Third Party Risk Management

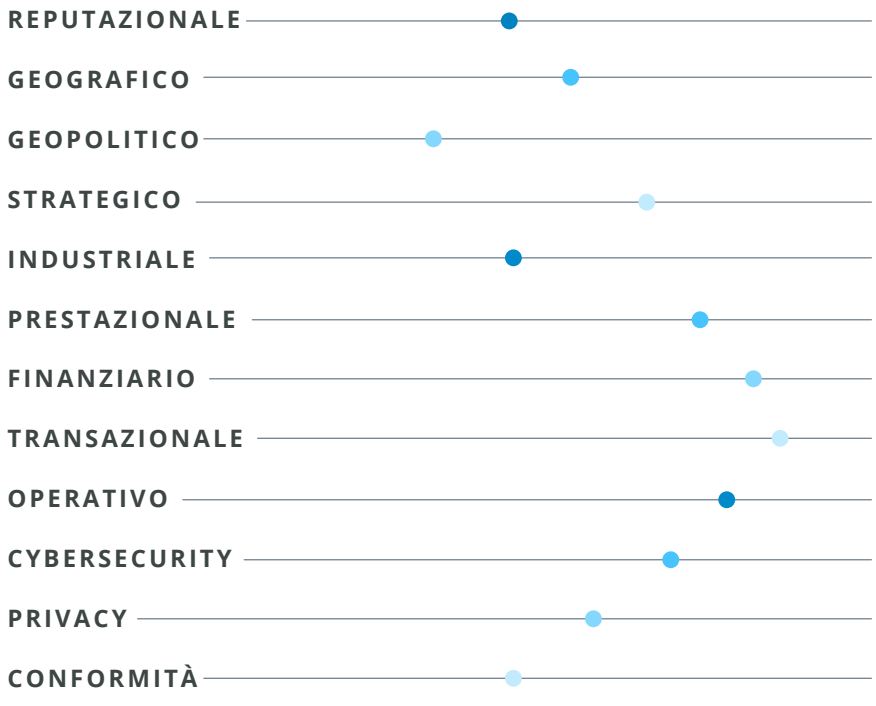
ISO

NIST

CSA cloud security alliance®

4. Definire i rischi che più interessano

Esistono molti tipi diversi di rischi da considerare quando si sviluppa il programma TPRM. Le aziende spesso classificano i rischi per meglio segnalare le potenziali minacce poste da un fornitore. Le classificazioni dei rischi più comuni includono:



FASE TRE: CREARE IL PROPRIO INVENTARIO

5. Conoscere le terze parti

Esistono diversi modi per scoprire con quali terze parti l'organizzazione lavora. Questo processo può richiedere tempo, tuttavia è possibile compiere delle azioni per semplificarlo.

Utilizzare le informazioni esistenti
Molte organizzazioni mantengono record dei loro provider di servizi in un foglio excel o in un database ma spesso questi elenchi sono disorganizzati, obsoleti e incompleti. È Il modo migliore dunque per utilizzare questi dati e' di importarli in maniera massiva in un inventario centrale ed utilizzarli come punto di partenza.

Sfruttare il DataDiscovery per identificare le tecnologie delle terze parti
Identificare i provider di servizi esistenti in uso guardando alle tecnologie esistenti, come i CMDB, i provider di SSO, i contratti, gli approvvigionamenti e altri strumenti per raccogliere e centralizzare tutte le informazioni relative ai provider di servizi.

Condurre assessment o interviste
Condurre assessment interni e interviste per identificare le terze parti in uso. Molte organizzazioni invieranno un breve assessment ai responsabili dei vari settori aziendali, come il marketing, le risorse umane, la finanza, le vendite, la ricerca, e sviluppo e altri dipartimenti. Questi leader aziendali sono in grado di fornire preziosi dettagli sugli strumenti in uso in tutta l'organizzazione.

Utilizzare i portali self-service
Con un portale self-service, è possibile permettere all'azienda di contribuire alla creazione dell'inventario. Per accedere facilmente, collegarsi al portale all'interno della rete intranet o SharePoint, e utilizzare un breve assessment preliminare per identificare i fornitori e raccogliere informazioni preliminari delle terze parti, come ad esempio:

- Nome fornitore
- Prevista data di acquisizione
- Scopo commerciale
- Contatto principale del fornitore (e-mail, numero di telefono, indirizzo postale)
- Tipo di dati coinvolti
- Revisioni o certificazioni di sicurezza precedenti, se applicabile
- Informazioni personali coinvolte
- Informazioni dell'hosting
- Scudo della Privacy e altre certificazioni
- Contesto aziendale
- Ambito di coinvolgimento

6. Classificare le terze parti

Per classificare i terzi, le aziende spesso determinano il rischio connesso ai loro fornitori. Per determinare i rischi connessi, le organizzazioni inviano un rapido questionario per comprendere i dettagli, come ad esempio

- Servizio fornito
- Accesso ai dati
- Sensibilità/tipo di dati
- Aspettative in relazione a sicurezza e privacy
- Posizione finanziaria del fornitore
- Valore del contratto
- Precedente relazione con il fornitore
- Trasferimenti di dati
- Sede operativa e luogo di conservazione dei dati
- Valore strategico dell'azienda
- Durata della relazione

Utilizzando il rischio connesso, i team di TPRM possono suddividere i fornitori in livelli, con i fornitori di primo livello solitamente designati come i più critici.

FASE QUATTRO: SEMPLIFICARE GLI ASSESSMENT E LA DUE DILIGENCE

7. Eseguire assessment e mitigare i rischi

Gli assessment richiedono tempo e richiedono molte risorse. Invece di inviare un assessment dettagliato tramite un foglio di calcolo, molti programmi TPRM sfruttano le nuove tendenze del mercato, come ad esempio:

- Valutazioni precompilate rese disponibili attraverso un Cyber Risk Exchange
- Servizi di ricerca del fornitore per richiedere gli assessment come servizio
- Tecnologia di automazione degli assessment per semplificare la compilazione dei questionari

Se si sceglie di effettuare l'assessment da soli, uno degli obiettivi principali è quello di capire quali controlli ha in atto un fornitore. Dopo aver identificato i controlli critici (o la loro mancanza), è possibile calcolare i rischi e iniziare la mitigazione. I flussi di lavoro comuni per la mitigazione dei rischi includono:

IDENTIFICAZIONE → VALUTAZIONE → TRATTAMENTO → MONITORAGGIO

IDENTIFICAZIONE
In questa fase, i rischi vengono segnalati e viene assegnato un livello di rischio o un punteggio.

VALUTAZIONE
Durante la fase di valutazione, le organizzazioni determineranno la propensione al rischio.

TRATTAMENTO
Quando si verifica il trattamento, un proprietario del rischio deve convalidare che siano in atto i controlli necessari per ridurre il rischio al livello di rischio residuo desiderato.

MONITORAGGIO
In questa fase, le organizzazioni monitorano i rischi per qualsiasi evento che possa aumentare il livello di rischio, come ad esempio una violazione dei dati.

8. Gestire i termini chiave del contratto

I contratti sono spesso lunghi ed estremamente dettagliati, con alcuni aspetti che non rientrano nel campo di applicazione della TPRM. Tuttavia, sono presenti disposizioni, clausole e termini chiave a cui i team di TPRM dovrebbero prestare attenzione quando esaminano i contratti dei fornitori. Alcuni di questi includono:

- Ambito definito dei servizi o dei prodotti
- Prezzo e condizioni di pagamento
- Clausole di recesso e di risoluzione
- Clausola di proprietà intellettuale
- Clausola sui prodotti o servizi
- Rappresentanza e garanzie
- Clausola di riservatezza
- Esclusione di responsabilità o indennizzo
- Limitazione di responsabilità
- Assicurazione
- Clausola di relazione
- Accordo sul trattamento dei dati
- Clausole di modifica della 4a parte o del collaboratore subordinato
- Clausola di conformità
- Accordo sulla protezione dei dati
- Contratti sul SLA, prestazioni del prodotto, tempi di risposta

Molti esperti di TPRM estraggono i termini chiave in un formato strutturato per determinare se le clausole contrattuali chiave sono adeguate, inadeguate o mancanti. Questo metodo di tracciamento "strutturato" e semplificato rende possibile un reporting a livello esecutivo e offre chiarezza quando si tratta di contratti.

FASE CINQUE: MANTENERE E MONITORARE

9. Generare rapporti e mantenere i record per la conformità

Per costruire un programma TPRM giustificabile e pronto per gli audit, le organizzazioni devono mantenere i record per dimostrare la conformità. Questo passo è spesso trascurato - fino a quando non si verificano degli audit - ed è uno degli aspetti più significativi di un programma TPRM adeguatamente collaudato. Mantenere questi record in fogli excel è quasi impossibile su larga scala. Il software TPRM progettato su misura può automatizzare la conservazione dei record e lasciare tracce dettagliate delle attività per semplificare gli audit.

Grazie alla conservazione di record dettagliati, diventa molto più facile segnalare le cose che contano di più per l'organizzazione. In pratica, vediamo le organizzazioni creare dashboard che mostrano:

- Conteggio totale dei fornitori
- Fornitori ordinati per livello di rischio
- Status di tutti gli assessment dei rischi dei fornitori
- Numero di fornitori con contratti in scadenza o scaduti
- Rischi raggruppati per livello (alto, medio, basso)
- Rischi per fasi del flusso di lavoro di mitigazione del rischio
- Rischi per la vostra organizzazione madre e rischi per le vostre filiali
- Cronologia del rischio nel tempo

10. Monitorare i cambiamenti dei fornitori, del mercato e della normativa nel corso del tempo

La TPRM è ben lontana da una disciplina statica. Con le nuove normative, le minacce emergenti, le violazioni dei dati di alto profilo e l'evoluzione degli standard, le organizzazioni hanno il loro lavoro da svolgere - e questo è il motivo per cui il settore sta spingendo per un continuo monitoraggio del rischio da parte di terzi. Gli assessment offrono una visione istantanea della posizione attuale del rischio di un fornitore, tuttavia questi possono cambiare drasticamente in qualsiasi momento. Oltre alla sicurezza informatica, sono da monitorare anche eventi significativi che cambiano il rischio:

- Fusioni, acquisizioni o cessioni
- Modifiche interne al processo
- Notizie negative o comportamenti non etici
- Disastri naturali e altri eventi che danneggiano la continuità operativa
- Versioni del prodotto
- Modifiche al contratto
- Sviluppi industriali o normativi
- Redditività finanziaria o liquidità
- Riduzione del personale
- E molto di più...

Se non si dispone di uno strumento per monitorare costantemente i fornitori, è opportuno considerare la possibilità di rivalutare i propri fornitori a cadenza regolare. Questo programma può essere determinato sulla base del rischio inerente o residuo delle terze parti, su un programma a tempo, o quando i contratti sono in scadenza per il rinnovo.

Se si desidera vedere in dettaglio come **OneTrust Vendorpedia** può aiutare a maturare e a gestire il programma del rischio di terzi, ***è possibile richiedere una demo oggi stesso.***

OneTrust Vendorpedia™

THIRD-PARTY RISK SOFTWARE

Informazioni su Vendorpedia

OneTrust Vendorpedia™ è la piattaforma tecnologica più grande e più utilizzata per rendere operativa la gestione del rischio, della sicurezza e della privacy di terzi. Più di 5.000 clienti di tutte le dimensioni utilizzano OneTrust, che si avvale di 75 brevetti rilasciati per offrire la soluzione per la privacy, sicurezza e rischio di terzi più approfondita e ampia sul mercato. OneTrust Vendorpedia è un software appositamente progettato per aiutare le organizzazioni a gestire con fiducia le relazioni con i fornitori e si integra perfettamente con l'intera piattaforma OneTrust, compresi OneTrust Privacy, OneTrust GRC, OneTrust DataGuidance™, e OneTrust PreferenceChoice™.

Sostenuta e co-diretta dai fondatori di Manhattan Associates (NASDAQ: MANH) e AirWatch (acquisita da VMware per $1,54Mld), e supportata da un finanziamento di 200 milioni di dollari di capitale investito da Insight Partners, il team della leadership di OneTrust ha una significativa esperienza nella creazione di piattaforme software aziendali scalabili. OneTrust è guidato da un comitato consultivo esterno di rinomati esperti di privacy e un team globale interno di ricerca legale e sulla privacy. OneTrust ha sede ad Atlanta e Londra con ulteriori uffici a Bangalore, San Francisco, Melbourne, New York, San Paolo, Monaco e Hong Kong, Bangkok.

Per qualsiasi domanda scrivi a Ludovica Colombo - responsabile del mercato italiano - a **lcolombo@onetrust.com**

Per saperne di più visita **Vendorpedia.com** o seguici sulla pagina **LinkedIn** OneTrust Italia.