S.O.X

Nel 2002, il Congresso ha approvato il Sarbanes-Oxley Act (SOX) in risposta alle ricadute e all'incertezza a seguito di eventi di frode e scandali finanziari in diverse società, tra cui WorldCom ed Enron. Il SOX Act ha introdotto diverse importanti riforme alla regolamentazione dell'informativa finanziaria e della corporate governance con l'obiettivo di ripristinare la fiducia del pubblico nella revisione contabile e nell'informativa finanziaria. Il SOX Act, noto anche come "Public Company Accounting Reform and Investor Protection Act" o "Corporate and Auditing Accountability and Responsibility Act", prende il nome dai suoi principali architetti, il senatore Paul Sarbanes e il rappresentante Michael Oxley.

I requisiti di conformità nuovi o ampliati si applicano a tutti i consigli di amministrazione, alle società di gestione e alle società contabili statunitensi per le società pubbliche. Anche le aziende private che contemplano un'IPO o si preparano a una fusione o acquisizione possono trovare prudente rivedere i loro controlli interni SOX. Tra le altre disposizioni, le SOX impongono:

Tutti i rapporti finanziari delle società includono un rapporto sui controlli interni.

Dati finanziari accurati e controlli in atto per salvaguardare i dati finanziari.

L'emissione di relazioni finanziarie di fine anno.

Divulgazione di frodi aziendali tutelando i dipendenti whistleblower.

Kim Pham offre una panoramica della conformità SOX, dell'impatto, delle sfide e delle preoccupazioni e dell'utilizzo delle soluzioni tecnologiche per la conformità SOX.

Sarbanes-Oxley ha aggiunto requisiti di responsabilità per i leader e il management, rendendoli responsabili dell'accuratezza dei rendiconti finanziari della loro organizzazione. La cattiva condotta dei dirigenti ha svolto un ruolo importante negli scandali Enron, WorldCom e Tyco, tra gli altri, e continua a influenzare l'atteggiamento delle organizzazioni nei confronti delle divulgazioni finanziarie e delle pratiche contabili. Pertanto, SOX ha aperto la porta a ritenere i dirigenti responsabili di frodi nella rendicontazione finanziaria. TL; La conformità DR SOX garantisce che le aziende aderiscano a rigorosi standard di rendicontazione finanziaria e controlli interni, migliorando la trasparenza e la fiducia degli investitori. Questo articolo illustra gli elementi essenziali della conformità SOX, la sua implementazione e i vantaggi che offre oltre la semplice conformità alle normative.

Questo articolo analizzerà i diversi requisiti di conformità SOX, le sfide SOX, i vantaggi di essere conformi a SOX e cosa aspettarsi durante il processo di audit SOX.

La conformità con SOX è applicata dalla Securities and Exchange Commission (SEC) In qualità di principale agenzia federale responsabile della protezione degli investitori e del mantenimento di mercati equi ed efficienti, la SEC garantisce che le aziende aderiscano ai severi requisiti stabiliti dal Sarbanes-Oxley Act. La supervisione della SEC contribuisce a migliorare la trasparenza, la responsabilità e l'integrità della rendicontazione finanziaria, promuovendo così la fiducia degli investitori e la

stabilità del mercato. Il Public Company Accounting Oversight Board (PCAOB) è una nuova agenzia istituita da SOX ed è responsabile della supervisione della società di contabilità pubblica e della qualità degli audit delle società pubbliche. Il Sarbanes-Oxley Act del 2002 è composto da 11 titoli, ma ci sono due disposizioni chiave riguardanti i requisiti di conformità: le sezioni 302 e 404.

Art. 302: Responsabilità delle imprese per le relazioni finanziarie

La sezione 302 del SOX stabilisce che gli amministratori delegati (CEO) e i direttori finanziari (CFO) sono direttamente responsabili dell'accuratezza dei rapporti finanziari. I funzionari firmatari devono rivedere e certificare l'accuratezza dei rendiconti finanziari, stabilire e mantenere i controlli interni e divulgare tutte le carenze significative, le frodi e i cambiamenti significativi nei controlli interni.

Questo mandato consente ai CEO e ai CFO di essere ritenuti responsabili per le inesattezze nei bilanci della loro organizzazione, fino a includere sanzioni penali. Il mancato rispetto della Sezione 302 del SOX può comportare sanzioni civili e penali significative, tra cui multe fino a 5 milioni di dollari e reclusione fino a 20 anni per i dirigenti che certificano consapevolmente falsi rapporti finanziari.

Art. 404: Valutazione gestionale dei controlli interni

La sezione 404 stabilisce che tutte le relazioni annuali devono includere una relazione sul controllo interno che delinei esplicitamente la responsabilità della direzione di mantenere un'adeguata struttura di controllo interno, una valutazione della sua efficacia e eventuali carenze in tali controlli. I revisori esterni

indipendenti devono inoltre attestare l'accuratezza della dichiarazione dell'azienda secondo cui i controlli interni sono in atto ed efficaci. La sezione 404 include requisiti aggiuntivi come la revisione dei controlli interni di una società da parte di revisori esterni e prevede esenzioni per alcune società. L'esame del SOX 404 da parte dell'Audit Board offre informazioni più dettagliate su questa sezione SOX.

Per limitare i conflitti di interesse, l'audit esterno 404 deve essere eseguito da revisori indipendenti che esercitano scetticismo e giudizio professionale per esaminare lo stato dei controlli interni presso le società quotate in borsa.

I vantaggi della conformità SOX 404

Uno dei risultati critici della sentenza Sarbanes Oxley è stata la fine dell'autoregolamentazione e l'istituzione di una supervisione indipendente del processo di revisione contabile attraverso il Public Company Accounting Oversight Board (PCAOB). Il PCAOB può stabilire standard di settore, indagare su accuse di frode e regolamentare le società di revisione. Infatti, il PCAOB esegue audit regolari degli auditor per garantire che la qualità rimanga elevata e che vengano seguite le migliori pratiche del settore.

Per quanto le aziende abbiano inizialmente lottato con i costi e l'onere delle risorse della conformità, nel tempo stanno vedendo che l'investimento nella conformità SOX sta dando i suoi frutti in diversi modi significativi.

1. Miglioramento della governance aziendale: la conformità SOX ha migliorato la governance aziendale attraverso una maggiore regolamentazione dei comitati di revisione. Prima del SOX, il 51% delle società pubbliche aveva comitati di revisione

completamente indipendenti dal management. SOX ha imposto che tutte le società quotate abbiano un comitato di revisione i cui membri siano indipendenti dal management e comprendano almeno un esperto finanziario. Di conseguenza, i comitati di revisione contabile oggi sono meglio attrezzati per fornire report finanziari accurati e veritieri. I comitati di revisione indipendenti hanno un mandato diverso rispetto agli altri, aggiungendo un ulteriore livello di governance al processo di informativa finanziaria.

2. Maggiore responsabilità: la conformità SOX rende i dirigenti più responsabili e protegge gli investitori. I dirigenti sono tenuti a certificare personalmente i rapporti finanziari, con sanzioni significative in caso di attività fraudolente. Anche i revisori dei conti hanno una maggiore responsabilità nel mantenere l'integrità e l'indipendenza, poiché gli scandali di frode che hanno alimentato la Sarbanes-Oxley hanno anche portato alla caduta della Arthur Andersen, una delle più grandi società di contabilità dell'epoca.

3. Miglioramento dell'indipendenza e della qualità del revisore: la conformità SOX migliora l'indipendenza del revisore vietando alle società di revisione di fornire funzioni contabili, attuariali o gestionali alle società che controllano. I revisori esterni devono mantenere l'indipendenza nell'aspetto e nei fatti. Ciò migliora la qualità dell'audit e il rigore dell'audit.

4. Meno riformulazioni finanziarie: dopo il SOX, il numero di ridichiarazioni dei record finanziari continua a diminuire anno su anno, passando da 1.784 nel 2006 a 738 nel 2012.

5. Miglioramento della gestione del rischio e della sicurezza informatica: molte delle best practice implementate dalle organizzazioni odierne nell'ambito della conformità SOX, in particolare i controlli generali IT, si sovrappongono alle linee guida dei framework di sicurezza informatica come il NIST CSF. Un esempio di questa sovrapposizione è la richiesta di un controllo e di una gestione degli accessi forti e limitati per proteggere i sistemi e le informazioni sensibili da accessi non autorizzati: la maggior parte degli audit SOX 404 lo richiede per i sistemi informativi finanziariamente rilevanti e il NIST CSF lo raccomanda vivamente come parte del loro pilastro "Protect".

Per riassumere, alcuni dei principali vantaggi del mantenimento e dell'iterazione della conformità SOX all'interno dell'organizzazione, oltre al semplice mantenimento della conformità, sono: 1) miglioramento della governance aziendale, 2) maggiore responsabilità, 3) maggiore indipendenza e qualità del revisore, 4) meno rivalutazioni finanziarie e 5) migliore gestione del rischio e della sicurezza informatica.

L'evoluzione delle SOX: adozione della tecnologia e attenzione ai costi tra cambiamenti aziendali, cyber e mandati ESG

Il processo di audit SOX

Gli audit SOX possono essere suddivisi in un numero qualsiasi di fasi, dall'esecuzione delle valutazioni dei rischi a ciò che includere in un rapporto del comitato di revisione. Abbiamo ristretto il nostro schema del processo di audit SOX ai seguenti otto passaggi:

Definizione dell'ambito dell'audit utilizzando un approccio di valutazione dei rischi

Determinazione della rilevanza e dei rischi – Conti, estratti conto, sedi, processi, sistemi e transazioni principali

Identificazione dei controlli SOX - Controlli generali IT (ITGC), controlli applicativi, controlli a livello di entità (ELC), ecc.

Esecuzione di una valutazione del rischio di frode

Gestione della documentazione di processo e controllo

Test dei controlli chiave

Valutazione delle carenze

Consegna della relazione della direzione sui controlli

1) Definizione dell'ambito dell'audit SOX utilizzando un approccio di valutazione del rischio

Per l'esecuzione di una valutazione del rischio, il PCAOB Accounting Standard n. 5 afferma: "Un approccio top-down inizia a livello di bilancio e con la comprensione da parte del revisore dei rischi complessivi per i controlli interni sull'informativa finanziaria. Il revisore si concentra quindi sui controlli a livello di entità e lavora fino ai conti significativi, alle informazioni e alle relative affermazioni". In sintesi, il PCAOB raccomanda che l'audit inizi al livello più alto, diventando più granulare. L'ambito dell'audit dovrebbe concentrarsi su quelle risorse, persone, sistemi e processi che influenzano il processo di divulgazione finanziaria, il che significa che non tutto nell'organizzazione sarà nell'ambito. L'ambito di un audit SOX dovrebbe includere e considerare tutti i rischi per i controlli interni di un'organizzazione

sulla rendicontazione finanziaria in un approccio incentrato sul rischio per la conformità SOX.

Questo passaggio di un audit di conformità SOX non deve comportare un elenco di procedure di conformità. Tuttavia, dovrebbe aiutare il revisore a identificare i potenziali rischi e le fonti, il modo in cui potrebbero influire sull'azienda e se i controlli interni forniranno una ragionevole garanzia che un errore materiale sarà evitato, prevenuto o rilevato.

2) Determinazione della materialità nel SOX – Conti, estratti conto, ubicazioni, processi e transazioni principali

Passaggio 1 – Determinare ciò che è considerato rilevante per il conto economico e lo stato patrimoniale. Come: Le voci di bilancio sono considerate "rilevanti" se possono influenzare le decisioni economiche degli utenti. I revisori possono in genere determinare ciò che è rilevante calcolando una certa percentuale dei principali conti di bilancio. Ad esempio, il 5% delle attività totali, il 3-5% del reddito operativo o un'analisi di più conti economici e di bilancio chiave.

Passaggio 2 - Determinare tutte le ubicazioni con i saldi dei conti materiali. Come: analizza i dati finanziari di tutte le sedi in cui fai affari. Se uno qualsiasi dei saldi dei conti di bilancio in queste sedi supera ciò che è stato determinato come materiale (nella fase 1), è probabile che sarà considerato materiale e nell'ambito di SOX nel prossimo anno. Passaggio 3 – Identificare le transazioni che popolano i saldi dei conti materiali Come: Incontrare il controller e i proprietari del processo specifici per determinare le transazioni (ad es. debiti e crediti) che causano l'aumento o la diminuzione del conto del bilancio. Il modo in cui queste transazioni avvengono e il modo in cui vengono registrate devono

essere documentati in una narrazione, in un diagramma di flusso o in entrambi.

Passaggio 4 – Identificare i rischi di rendicontazione finanziaria per i conti rilevanti. Come: Cerca di capire cosa potrebbe impedire la corretta registrazione della transazione o l'evento di rischio. Quindi, documenta l'effetto che l'evento di rischio potrebbe avere sul modo in cui il saldo del conto potrebbe essere registrato in modo errato o la rottura dell'affermazione di bilancio.

3) Identificazione dei controlli SOX – Controlli chiave e non chiave, ITGC e altri controlli a livello di entità (ELC)

Durante l'analisi di materialità, i revisori identificheranno e documenteranno i controlli SOX che potrebbero impedire o rilevare la registrazione errata delle transazioni. Cercheranno di identificare i controlli e gli equilibri nel processo di rendicontazione finanziaria che garantiscono che le transazioni siano registrate correttamente e che i saldi dei conti siano calcolati in modo accurato. Alcuni esempi di controlli SOX preventivi o investigativi includono:

Separazione dei doveri contrastanti e incompatibili (ad esempio, la capacità di registrare e approvare le fatture),

Revisione di una o più operazioni registrate nel periodo, e

Riconciliazioni dei conti.

Inoltre, i conti materiali necessitano spesso di più controlli per evitare che si verifichi un errore rilevante. Dovrai analizzare tutti i controlli per determinare quali forniscono la migliore garanzia, tenendo presente le persone, i processi e la tecnologia in atto.

I team di audit sono avvertiti di non applicare un approccio di forza bruta e di creare un nuovo controllo SOX ogni volta che viene identificato un nuovo rischio. Inavvertitamente, ogni nuovo controllo viene spesso classificato come "chiave" senza eseguire una vera valutazione del rischio, contribuendo al numero di controlli in continuo aumento. Comprendendo le differenze tra controlli chiave e non chiave, i team di audit interno possono combattere efficacemente l'aumento del numero di controlli e lo "scope creep".

Per semplificare le cose, il metodo più rapido per differenziare un controllo vs. key non chiave è fare riferimento al livello di rischio da affrontare. Il controllo mitiga un rischio basso o alto? Comprendendo i rischi che influiscono sul processo di conformità SOX, i team di audit possono stabilire meglio le priorità e concentrare i propri sforzi sui controlli chiave.

Infine, per finalizzare e pianificare un sistema efficace di controlli interni, il team di audit deve identificare i controlli manuali e automatizzati. Per i controlli automatizzati identificati, è necessario valutare se il sistema sottostante rientra nell'ambito dei test ITGC (IT General Controls), il che influirà sulla strategia di test complessiva del controllo. Se si dispone di ITGC comfort rispetto al sistema sottostante, è possibile ridurre sostanzialmente la quantità di test di controllo da eseguire. L'utilizzo di ITGC solidi e controlli relativi alla sicurezza informatica sono un altro vantaggio della conformità SOX.

4) Esecuzione di una valutazione del rischio di frode

Un sistema efficace di controlli interni comprende una valutazione delle possibili attività fraudolente. La prevenzione e il rilevamento precoce sono fondamentali per ridurre i casi di

frode in un'organizzazione. I controlli interni svolgono un ruolo chiave nel ridurre le opportunità disponibili di commettere frodi e l'impatto sostanziale che avrebbe se si verificasse una frode, compreso l'annullamento manuale dei controlli interni.

Di seguito sono riportati esempi di controlli interni antifrode e pratiche che le organizzazioni possono implementare per ridurre notevolmente le perdite dovute alle frodi.

Segregazione dei compiti: l'Institute of Internal Auditors (IIA) descrive l'idea di base alla base della segregazione dei doveri come "nessun dipendente o gruppo di dipendenti dovrebbe essere in grado sia di perpetrare che di nascondere errori o frodi nel normale svolgimento delle proprie funzioni". Cioè, il lavoro di un individuo dovrebbe essere indipendente o servire a controllare il lavoro di un altro. Esempi:

Custodia dei Beni

Autorizzazione/approvazione delle relative operazioni che interessano tali attività

Registrazione e segnalazione delle relative operazioni

Rimborsi spese: secondo il rapporto ACFE del 2014, una parte significativa degli schemi di appropriazione indebita di beni coinvolge situazioni in cui un dipendente presenta una richiesta di rimborso di spese aziendali fittizie o gonfiate. Per prevenire tali schemi, la direzione dovrebbe garantire che le politiche e le procedure pertinenti relative ai rimborsi dei dipendenti siano comunicate ai dipendenti e aggiornate ogni volta che è necessario. Inoltre, il flusso di approvazione di tali rimborsi dovrebbe includere, insieme al supervisore diretto, altre parti

interessate chiave, come i membri del team aziendale interessati, le buste paga o l'audit interno.

Hotline per gli informatori: nonostante le normative federali, la responsabilità ultima dell'implementazione di un forte programma per gli informatori spetta alla direzione. Storicamente, le soffiate interne ai dipendenti hanno fornito il miglior mezzo per rilevare le frodi. Pertanto, la direzione non può permettersi di trascurare un meccanismo di whistleblowing interno all'organizzazione.

Riconciliazione periodica dei conti bancari: le riconciliazioni bancarie evidenziano le differenze tra la cassa per bilancio e l'estratto conto bancario, confermando anche l'accuratezza dei dati registrati nel libro mastro dell'organizzazione. Il compito principale di eseguire una riconciliazione bancaria non è solo quello di identificare differenze impreviste, ma comporta anche la prevenzione di eventi futuri, come ritardi contabili, limitazione degli addebiti automatici ai fornitori, ecc. A seconda delle dimensioni dell'organizzazione, le riconciliazioni bancarie devono essere eseguite giornalmente, settimanalmente o mensilmente per monitorare e rilevare attività fraudolente.

È l'approccio proattivo del management verso il rilevamento e la prevenzione delle frodi, insieme a solidi controlli interni, che alla fine ridurrà le opportunità di commettere frodi e instillerà una cultura etica all'interno di un'organizzazione.

5) Gestione della documentazione dei controlli di processo e SOX

La narrazione e la documentazione del controllo stabiliscono i dettagli del funzionamento dei controlli chiave, come le

descrizioni dei controlli, la frequenza, le procedure di test, il rischio associato, la popolazione e le prove. La mappatura dei rischi e dei controlli ha spesso una relazione molti-a-molti, rendendo difficile la documentazione manuale. Alcuni esempi includono i rischi che si manifestano in più processi o business unit, problemi di audit che influiscono su più controlli o processi e principi COSO che si associano a molti controlli. Come può attestare un responsabile dell'audit, se un membro del team non riesce a effettuare una modifica tempestiva o dimentica di apportare aggiornamenti a tutti i fogli di test, l'effetto a catena a valle può costare ai manager ore e ore di pulizia. La soluzione consiste nell'sfruttare un database relazionale sottostante che funga da repository centrale e da base del programma di audit. Il software SOX costruito su strutture di database appositamente costruite può consentire ai revisori di estrarre o inviare rapidamente informazioni da e verso un database e di far sì che tali risultati si diffondano istantaneamente in tutto il programma SOX. La documentazione di Controls è semplice e non richiede modifiche in diversi file di fogli di calcolo autonomi. Inoltre, per i risultati degli audit annuali da utilizzare anno dopo anno, un foglio di calcolo non è in grado di gestire grandi volumi di dati. La velocità, l'accuratezza e la scalabilità di una soluzione di database supereranno i vantaggi della "familiarità con i fogli di calcolo".

6) Test dei controlli chiave

L'obiettivo generale dei test di controllo SOX è triplice: 1) garantire che il processo o le procedure di test come delineato siano un metodo efficace per testare il controllo, 2) il controllo venga eseguito durante l'intero periodo e dal proprietario del processo assegnato e 3) il controllo sia riuscito a prevenire o rilevare

eventuali errori materiali. In breve, i test di controllo convalidano la progettazione e l'efficacia operativa dei controlli.

L'effettivo processo di test dei controlli SOX può includere una varietà o una combinazione di procedure di test, tra cui la valutazione continua, l'osservazione, le indagini con i proprietari del processo, la procedura dettagliata, l'ispezione della documentazione e/o una nuova esecuzione del processo.

7) Valutazione delle carenze di SOX

L'investimento continuo in un programma SOX si tradurrà naturalmente in un miglioramento delle azioni, delle politiche e delle procedure. Con il miglioramento dell'ambiente di controllo, è probabile che le aziende vedano anche un chiaro aumento del livello di automazione e una corrispondente diminuzione della quantità di test manuali richiesti dagli auditor. In definitiva, questo porterà il tuo team a dedicare meno tempo alla gestione di un minor numero di problemi complessivi. Le carenze dovrebbero essere ridotte a un livello accettabile e prevedibile e ci dovrebbero essere poche o nessuna sorpresa.

Durante il processo di test e analisi del controllo SOX, l'auditor può identificare un'esenzione, una carenza o una lacuna nel campione testato. Se ciò accade, viene creato un "problema". Oltre a rimediare e correggere il problema, il team di audit valuta quindi se si è trattato di un errore di progettazione nel controllo o di un errore operativo in cui è necessario adeguare la formazione, le responsabilità o il processo. Infine, il management e il team di audit valutano se si tratta o meno di una debolezza materiale (come descritto sopra è tipicamente una percentuale di varianza e con un livello di rischio elevato) e saranno riportati nei dati

finanziari di fine anno o se si è trattato solo di una debolezza significativa.

8) Consegna della Relazione della Direzione sui Controlli

Il prodotto finale dei test di controllo SOX è la relazione della direzione sui controlli sulla rendicontazione finanziaria che viene consegnata al comitato di revisione. Sebbene durante il processo venga raccolta una notevole quantità di documentazione e dati, il rapporto dovrebbe includere:

Sintesi del parere della direzione e sostegno a tali conclusioni.

Revisione del framework utilizzato, delle prove raccolte e del riepilogo dei risultati.

Risultati di ciascuno dei test: a livello di entità, IT, controlli chiave.

Identificazione dei guasti di controllo, delle lacune e delle cause principali corrispondenti.

Valutazione effettuata da un revisore esterno indipendente della società.

ITGC SOX e controlli di sicurezza

Con il panorama tecnologico in rapida evoluzione, la dipendenza delle aziende dalla tecnologia dell'informazione e dai sistemi per la gestione delle informazioni finanziarie influisce in modo significativo sul modo in cui un'azienda compila e fornisce i propri rapporti della Securities and Exchange Commission (SEC). Poiché la maggior parte delle aziende ha trasferito funzioni e operazioni finanziariamente significative ai sistemi informativi, comprese le funzioni contabili, le funzioni finanziarie e persino le funzioni di vendita al dettaglio/e-commerce, l'impatto di attacchi informatici riusciti su un'organizzazione può essere grave. Anche

senza influire sulle attività di conformità SOX di un'azienda, gli incidenti di sicurezza possono portare a violazioni e perdite di dati, creando un'altra serie di sfide per un'azienda.

Alcuni degli ITGC fondamentali che vengono testati nell'ambito di SOX possono aiutare a evitare violazioni della sicurezza e manomissioni di informazioni finanziariamente rilevanti. Stabilendo controlli di sicurezza efficaci sulla protezione dei dati, sulla gestione delle modifiche e sui dati sensibili, i reparti IT possono rilevare, prevenire ed eseguire meglio la correzione di eventuali incidenti di sicurezza. Anche le aziende che sfruttano pesantemente i servizi cloud e non dispongono di data center propri dovrebbero rivedere regolarmente i report di conformità dei loro fornitori di terze parti per verificare che gli standard dei fornitori per la sicurezza dei dati siano conformi alle tue organizzazioni. La non conformità da parte di un fornitore può comunque comportare un rischio considerevole per i clienti di tale fornitore.

Sfide comuni per la conformità alle SOX

Fogli di calcolo e problemi con l'utente finale

L'umile foglio di calcolo si è evoluto per essere più di un semplice strumento di contabilità. Nel corso del tempo, il semplice foglio di calcolo si è trasformato in un punto fermo del flusso di lavoro SOX, in parte grazie alla sua capacità di collegare i dati tra diversi documenti e automatizzare le attività di base. Allo stesso tempo, i moderni progetti di audit richiedono ora più attributi e dettagli sul controllo. Che si tratti di documentare la completezza e l'accuratezza delle prove o di convalidare l'integrità di un rapporto chiave, le procedure di test si sono evolute oltre la semplice spunta e legatura degli attributi. Il moderno foglio di

calcolo è in grado di gestire questo robusto processo di test, ma manca di velocità, efficienza e coerenza.

Oltre a quanto menzionato sopra, ci sono alcuni rischi legati all'utilizzo di fogli di calcolo per il tuo programma SOX, tra cui, ma non solo:

Digitazione errata da parte di un utente o dati cancellati

Analisi di un set di dati incoerente, ovvero la popolazione non è corretta

Proprietari dei processi lasciati all'oscuro

I proprietari dei processi che gestiscono le attività di controllo quotidiane sono spesso lasciati all'oscuro quando si tratta dei propri controlli. I team di internal audit si affidano a fogli di calcolo e cartelle condivise per gestire i controlli, quindi la documentazione rimane spesso sul desktop dei team di internal audit, lontano dai proprietari dei processi.

Quando la documentazione dei controlli è compatibile con l'Internal Audit, i responsabili dei processi ottengono visibilità sui loro controlli solo una volta al trimestre e quindi creano le proprie attività quotidiane guidate dalla propria versione delle attività e non necessariamente nel contesto dei propri controlli.

Aumento dei costi e delle risorse

Sebbene il SOX abbia avuto un impatto positivo sulla rendicontazione finanziaria, permangono preoccupazioni per l'aumento del costo della conformità SOX e per i pesanti oneri delle risorse. I costi SOX continuano ad aumentare anno dopo anno per molte aziende, secondo l'indagine annuale Sarbanes

Oxley di Protiviti. I motivi includono l'introduzione di nuovi quadri come il COSO e l'evoluzione dei requisiti dei revisori esterni per la conformità alla Sezione 404. Le aziende oggi spendono in media da un milione a due milioni di dollari e fino a 10.000 ore all'anno in programmi SOX.

Semplifica la conformità SOX con una tecnologia appositamente progettata

Una chiave per ridurre la natura costosa e dispendiosa in termini di tempo della conformità SOX e massimizzare le risorse SOX risiede nell'utilizzo di una tecnologia appositamente progettata per automatizzare i processi. I team SOX lungimiranti stanno sfruttando gli strumenti di automazione SOX per ridurre le ore amministrative e gli sforzi spesi per SOX. Il software di conformità SOX consente ai team di liberare tempo per eseguire più audit a valore aggiunto, aumentare la qualità dei controlli interni, migliorare la visibilità in tempo reale negli ambienti SOX, aumentare la collaborazione con i revisori esterni e, in ultima analisi, evitare rivalutazioni finanziarie.

Domande frequenti sulla conformità SOX

Che cos'è il Sarbanes-Oxley Act (SOX) e perché è stato emanato?

Il Sarbanes-Oxley Act, comunemente noto come SOX, è una legge federale degli Stati Uniti emanata nel 2002 per proteggere gli investitori migliorando l'accuratezza e l'affidabilità delle informative aziendali. È stato approvato in risposta a importanti scandali societari e contabili, compresi quelli che hanno coinvolto Enron e WorldCom, per ripristinare la fiducia del pubblico nei mercati finanziari.

Quali sono i requisiti chiave della conformità SOX?

La conformità SOX richiede alle aziende di implementare e mantenere solidi controlli interni sulla rendicontazione finanziaria. I requisiti chiave includono la certificazione dei bilanci da parte di CEO e CFO (Sezione 302), l'istituzione di un quadro di controllo interno (Sezione 404) e l'indipendenza dei revisori esterni (Sezione 301). Le aziende devono inoltre condurre regolari audit SOX per garantire la conformità a questi standard.

In che modo un'azienda può garantire la conformità SOX di successo?

Per garantire il successo della conformità SOX, le aziende dovrebbero istituire un team dedicato alla conformità SOX, implementare controlli interni completi e condurre una formazione regolare per i dipendenti. L'utilizzo di software di gestione degli audit come Audit Board può semplificare i processi di conformità automatizzando i flussi di lavoro, fornendo analisi dei dati in tempo reale e generando report di conformità dettagliati. Anche gli audit regolari e il monitoraggio continuo sono essenziali per mantenere la conformità e affrontare tempestivamente eventuali problemi.

Vizio

Vice Vicente ha iniziato la sua carriera in EY e ha trascorso gli ultimi 10 anni nel settore della conformità IT, della gestione del rischio e della sicurezza informatica. Vice ha prestato servizio, audit o consulenza per oltre 120 clienti, implementando programmi e tecnologie di sicurezza e conformità, svolgendo incarichi relativi a SOX 404, SOC 1, SOC 2, PCI DSS e HIPAA e guidando le aziende attraverso la preparazione alla sicurezza e alla conformità. Connettiti con Vice su LinkedIn.