S.O.X

Im Jahr 2002 verabschiedete der Kongress den Sarbanes-Oxley Act (SOX) als Reaktion auf die Folgen und Unsicherheiten nach Betrugsfällen und Finanzskandalen bei mehreren Unternehmen, darunter WorldCom und Enron. Mit dem SOX Act wurden mehrere wichtige Reformen der Regulierung von Finanzangaben und der Unternehmensführung eingeführt, mit dem Ziel, das Vertrauen der Öffentlichkeit in die Wirtschaftsprüfung und Finanzberichterstattung wiederherzustellen. Der SOX Act, auch bekannt als "Public Company Accounting Reform and Investor Protection Act" oder "Corporate and Auditing Accountability and Responsibility Act", wurde nach seinen Hauptarchitekten, Senator Paul Sarbanes und dem Abgeordneten Michael Oxley, benannt.

Die neuen oder erweiterten Compliance-Anforderungen gelten für alle Vorstände, Management- und Wirtschaftsprüfungsgesellschaften von US-Aktiengesellschaften. Private Unternehmen, die einen Börsengang in Betracht ziehen oder sich auf eine Fusion oder Übernahme vorbereiten, könnten eine Überprüfung ihrer internen SOX-Kontrollen ebenfalls für klug halten. SOX schreibt unter anderem Folgendes vor:

Die Finanzberichte aller Unternehmen enthalten einen Bericht über die internen Kontrollen.

Genaue Finanzdaten und Kontrollen zum Schutz von Finanzdaten.

Die Veröffentlichung von Finanzberichten zum Jahresende.

Offenlegung von Unternehmensbetrug durch Schutz von Whistleblower-Mitarbeitern.

Kim Pham gibt einen Überblick über die SOX-Compliance, die Auswirkungen, Herausforderungen und Bedenken sowie die Nutzung von Technologielösungen für die SOX-Compliance.

Sarbanes-Oxley fügte Rechenschaftspflichten für Führungskräfte und Management hinzu und machte sie für die Richtigkeit der Finanzberichte ihres Unternehmens haftbar. Das Fehlverhalten der Führungskräfte spielte unter anderem bei den Skandalen um Enron, WorldCom und Tyco eine wichtige Rolle und beeinflusst weiterhin die Einstellung der Unternehmen zu Finanzoffenlegungen und Rechnungslegungspraktiken. Damit öffnete SOX die Tür, um Führungskräfte für Betrug in der Finanzberichterstattung verantwortlich zu machen. TL; Die DR SOX-Compliance stellt sicher, dass Unternehmen strenge Standards für die Finanzberichterstattung und interne Kontrollen einhalten, was die Transparenz und das Vertrauen der Anleger erhöht. In diesem Artikel werden die Grundlagen der SOX-Compliance, ihre Implementierung und die Vorteile behandelt, die sie über die bloße Einhaltung gesetzlicher Vorschriften hinaus bietet.

In diesem Artikel werden die verschiedenen SOX-Complianceanforderungen, die SOX-Herausforderungen, die Vorteile der SOX-Konformität und die während des SOX-Auditprozesses zu erwartenden Punkte aufgeschlüsselt.

Die Einhaltung von SOX wird von der Securities and Exchange Commission (SEC) durchgesetzt. Als wichtigste Bundesbehörde, die für den Schutz von Anlegern und die Aufrechterhaltung fairer und effizienter Märkte verantwortlich ist, stellt die SEC sicher,

dass Unternehmen die strengen Anforderungen des Sarbanes-Oxley Act einhalten. Die Aufsicht der SEC trägt dazu bei, die Transparenz, Rechenschaftspflicht und Integrität der Finanzberichterstattung zu verbessern und so das Vertrauen der Anleger und die Marktstabilität zu stärken. Das Public Company Accounting Oversight Board (PCAOB) war eine neue Behörde, die von SOX gegründet wurde und für die Überwachung der Wirtschaftsprüfungsgesellschaft und die Qualität ihrer Prüfungen von börsennotierten Unternehmen verantwortlich ist. Der Sarbanes-Oxley Act von 2002 besteht aus 11 Titeln, aber es gibt zwei wichtige Bestimmungen in Bezug auf die Compliance-Anforderungen: die Abschnitte 302 und 404.

§ 302 Corporate Responsibility für Finanzberichte

SOX Section 302 besagt, dass Chief Executive Officers (CEOs) und Chief Financial Officers (CFOs) direkt für die Richtigkeit von Finanzberichten verantwortlich sind. Die unterzeichnenden Beamten müssen die Richtigkeit der Jahresabschlüsse überprüfen und bescheinigen, interne Kontrollen einrichten und aufrechterhalten sowie alle wesentlichen Mängel, Betrug und wesentlichen Änderungen der internen Kontrollen offenlegen.

Dieses Mandat ermöglicht es CEOs und CFOs, für Ungenauigkeiten in den Finanzberichten ihres Unternehmens zur Rechenschaft gezogen zu werden, bis hin zu strafrechtlichen Sanktionen. Die Nichteinhaltung von SOX Section 302 kann zu erheblichen zivil- und strafrechtlichen Sanktionen führen, einschließlich Geldstrafen von bis zu 5 Millionen US-Dollar und Gefängnisstrafen von bis zu 20 Jahren für Führungskräfte, die wissentlich falsche Finanzberichte zertifizieren.

§ 404 Beurteilung der internen Kontrollen durch das Management

Abschnitt 404 besagt, dass alle Geschäftsberichte einen internen Kontrollbericht enthalten müssen, in dem die Verantwortung des Managements für die Aufrechterhaltung einer angemessenen internen Kontrollstruktur, eine Bewertung ihrer Wirksamkeit und etwaige Mängel bei diesen Kontrollen ausdrücklich dargelegt werden. Unabhängige externe Prüfer müssen auch die Richtigkeit der Aussage des Unternehmens bestätigen, dass interne Kontrollen vorhanden und wirksam sind. Section 404 enthält zusätzliche Anforderungen, wie z. B. eine Überprüfung der internen Kontrollen eines Unternehmens durch externe Wirtschaftsprüfer, und sieht Ausnahmen für bestimmte Unternehmen vor. Die Überprüfung von SOX 404 durch das Audit Board bietet detailliertere Informationen zu diesem SOX-Abschnitt.

Um Interessenkonflikte zu begrenzen, muss die externe 404-Prüfung von unabhängigen Wirtschaftsprüfern durchgeführt werden, die den Stand der internen Kontrollen bei börsennotierten Unternehmen mit professioneller Skepsis und Urteilsvermögen untersuchen.

Die Vorteile der SOX 404-Konformität

Eines der entscheidenden Ergebnisse von Sarbanes Oxley war das Ende der Selbstregulierung und die Einrichtung einer unabhängigen Aufsicht über den Prüfungsprozess durch das Public Company Accounting Oversight Board (PCAOB). Die PCAOB kann Branchenstandards festlegen, Betrugsvorwürfe untersuchen und Prüfungsgesellschaften regulieren. In der Tat führt die PCAOB regelmäßige Audits der Auditoren durch, um sicherzustellen, dass die Qualität hoch bleibt und die Best Practices der Branche befolgt werden.

So sehr Unternehmen anfangs mit der Kosten- und Ressourcenbelastung durch Compliance zu kämpfen hatten, sehen sie im Laufe der Zeit, dass sich die Investitionen in die SOX-Compliance in mehrfacher Hinsicht auszahlen.

1. Verbesserte Corporate Governance: SOX-Compliance verbesserte die Corporate Governance durch die stärkere Regulierung von Prüfungsausschüssen. Vor SOX hatten 51 % der börsennotierten Unternehmen völlig unabhängige Prüfungsausschüsse. SOX schreibt vor, dass alle börsennotierten Unternehmen einen Prüfungsausschuss haben, dessen Mitglieder unabhängig vom Management sind und aus mindestens einem Finanzexperten bestehen. Infolgedessen sind Prüfungsausschüsse heute besser in der Lage, genaue und wahrheitsgemäße Finanzberichte zu erstellen. Unabhängige Prüfungsausschüsse haben ein anderes Mandat als andere und fügen dem Finanzberichterstattungsprozess eine weitere Governance-Ebene hinzu.

2. Erhöhte Rechenschaftspflicht: SOX-Compliance macht Führungskräfte rechenschaftspflichtiger und schützt Investoren. Führungskräfte sind verpflichtet, Finanzberichte persönlich zu bestätigen, wobei für betrügerische Aktivitäten erhebliche Strafen verhängt werden. Auch Wirtschaftsprüfer haben eine erhöhte Verantwortung, Integrität und Unabhängigkeit zu wahren, da die Betrugsskandale, die Sarbanes-Oxley befeuerten, auch zum Niedergang von Arthur Andersen führten, einer der größten Wirtschaftsprüfungsgesellschaften zu dieser Zeit.

3. Verbesserte Unabhängigkeit und Qualität der Abschlussprüfer: Die SOX-Compliance erhöht die Unabhängigkeit der

Abschlussprüfer, indem sie es Prüfungsgesellschaften verbietet, Buchhaltungs-, Versicherungsmathematik- oder Managementfunktionen für die von ihnen geprüften Unternehmen zu übernehmen. Externe Revisionsstellen müssen nach Erscheinungsbild und in der Tat Unabhängigkeit wahren. Dies verbessert die Prüfungsqualität und die Strenge der Prüfung.

4. Weniger finanzielle Anpassungen: Nach der SOX-Einführung ist die Anzahl der Anpassungen von Finanzunterlagen im Vergleich zum Vorjahr weiter rückläufig und ging von 1.784 im Jahr 2006 auf 738 im Jahr 2012 zurück.

5. Verbessertes Risikomanagement und verbesserte Cybersicherheit: Viele der Best Practices, die von heutigen Unternehmen im Rahmen der SOX-Compliance implementiert werden, insbesondere IT General Controls, überschneiden sich mit den Leitlinien von Cybersicherheits-Frameworks wie dem NIST CSF. Ein Beispiel für diese Überschneidung ist die Forderung nach einer starken, eingeschränkten Zugriffskontrolle und Zugriffsverwaltung, um sensible Systeme und Informationen vor unbefugtem Zugriff zu schützen – die meisten SOX 404-Audits verlangen dies für finanziell wesentliche Informationssysteme, und das NIST CSF empfiehlt dies dringend als Teil seiner "Protect"-Säule.

Zusammenfassend lässt sich sagen, dass einige der wichtigsten Vorteile der Aufrechterhaltung und Iteration der SOX-Compliance in Ihrem Unternehmen, abgesehen von der einfachen Einhaltung der Compliance, sind: 1) verbesserte Corporate Governance, 2) erhöhte Rechenschaftspflicht, 3) verbesserte Unabhängigkeit und Qualität der Prüfer, 4) weniger finanzielle Neudarstellungen

und 5) verbessertes Risikomanagement und Cybersicherheitslage.

Die Entwicklung von SOX: Technologieakzeptanz und Kostenfokus inmitten von Geschäftsveränderungen, Cyber- und ESG-Mandaten

Der SOX-Audit-Prozess

SOX-Audits können in eine beliebige Anzahl von Schritten unterteilt werden, von der Durchführung von Risikobewertungen bis hin zu den Bestandteilen eines Berichts des Prüfungsausschusses. Wir haben unseren Überblick über den SOX-Auditprozess auf die folgenden acht Schritte eingegrenzt:

Definition des Prüfungsumfangs mit Hilfe eines Risikobewertungsansatzes

Bestimmung von Wesentlichkeit und Risiken – Konten, Kontoauszüge, Standorte, Prozesse, Systeme und wichtige Transaktionen

Identifizierung von SOX-Kontrollen – IT General Controls (ITGCs), Application Controls, Entity Level Controls (ELCs) usw.

Durchführung einer Betrugsrisikobewertung

Verwaltung der Prozess- und Steuerungsdokumentation

Testen von Schlüsselsteuerelementen

Bewertung von Mängeln

Erstellung des Managementberichts über die Kontrollen

1) Definition des SOX-Auditumfangs unter Verwendung eines Risikobewertungsansatzes

Für die Durchführung einer Risikobewertung heißt es im PCAOB Accounting Standard Nr. 5: "Ein Top-down-Ansatz beginnt auf der Ebene des Abschlusses und mit dem Verständnis des Abschlussprüfers für die Gesamtrisiken für die internen Kontrollen der Finanzberichterstattung. Der Prüfer konzentriert sich dann auf die Kontrollen auf Unternehmensebene und arbeitet sich bis hinunter zu bedeutenden Konten, Angaben und deren relevanten Behauptungen." Um dies auf den Punkt zu bringen, empfiehlt die PCAOB, dass das Audit auf der höchsten Ebene beginnt und detaillierter wird. Der Schwerpunkt des Prüfungsumfangs sollte auf den Vermögenswerten, Personen, Systemen und Prozessen liegen, die sich auf den Prozess der finanziellen Offenlegung auswirken – was bedeutet, dass nicht alles in der Organisation in den Geltungsbereich fällt. Ein SOX-Auditumfang sollte alle Risiken für die internen Kontrollen eines Unternehmens über die Finanzberichterstattung in einem risikoorientierten Ansatz für die SOX-Compliance umfassen und berücksichtigen.

Dieser Schritt in einer SOX-Complianceüberwachung sollte nicht zu einer Liste von Complianceverfahren führen. Dennoch sollte es dem Prüfer helfen, potenzielle Risiken und Ursachen zu identifizieren, wie sie sich auf das Geschäft auswirken könnten und ob die internen Kontrollen eine angemessene Sicherheit bieten, dass ein wesentlicher Fehler vermieden, verhindert oder aufgedeckt wird.

2) Bestimmung der Wesentlichkeit in SOX – Konten, Kontoauszüge, Standorte, Prozesse und wichtige Transaktionen

Schritt 1 – Bestimmen Sie, was für die GuV und die Bilanz als wesentlich angesehen wird. Wie: Abschlussposten gelten als

"wesentlich", wenn sie die wirtschaftlichen Entscheidungen der Adressaten beeinflussen können. Wirtschaftsprüfer können in der Regel bestimmen, was wesentlich ist, indem sie einen bestimmten Prozentsatz der wichtigsten Abschlusskonten berechnen. Zum Beispiel 5 % des Gesamtvermögens, 3-5 % des Betriebsergebnisses oder eine Analyse mehrerer wichtiger GuV- und BS-Konten.

Schritt 2 – Ermitteln Sie alle Standorte mit Materialkontensalden. Wie: Analysieren Sie die Finanzdaten für alle Standorte, an denen Sie geschäftlich tätig sind. Wenn einer der Salden des Jahresabschlusses an diesen Standorten den Betrag übersteigt, der (in Schritt 1) als wesentlich eingestuft wurde, besteht die Möglichkeit, dass er im kommenden Jahr als wesentlich und in den Geltungsbereich von SOX fallend angesehen wird. Schritt 3 – Identifizieren Sie Transaktionen, die die Salden der materiellen Konten füllen Wie: Treffen Sie sich mit Ihrem Controller und den jeweiligen Prozessverantwortlichen, um die Transaktionen (d. h. Belastungen und Haben) zu ermitteln, die dazu führen, dass das Bilanzkonto steigt oder sinkt. Wie diese Transaktionen ablaufen und wie sie aufgezeichnet werden, sollte in einer Erzählung, einem Flussdiagramm oder beidem dokumentiert werden.

Schritt 4 – Identifizieren Sie die Risiken der Finanzberichterstattung für wesentliche Konten. Wie: Versuchen Sie zu verstehen, was die korrekte Aufzeichnung der Transaktion oder das Risikoereignis verhindern könnte. Dokumentieren Sie dann die Auswirkungen, die das Risikoereignis auf die Art und Weise haben könnte, wie der Kontostand falsch erfasst werden könnte, oder auf die Aufschlüsselung der Behauptung des Jahresabschlusses.

3) Identifizierung von SOX-Kontrollen – Schlüssel- und Nicht-Schlüsselkontrollen, ITGCs und andere Kontrollen auf Entitätsebene (ELCs)

Während Ihrer Wesentlichkeitsanalyse identifizieren und dokumentieren Auditoren SOX-Kontrollen, die verhindern oder aufdecken können, dass Transaktionen falsch erfasst werden. Sie werden versuchen, die Checks and Balances im Finanzberichterstattungsprozess zu identifizieren, die sicherstellen, dass die Transaktionen korrekt erfasst und die Kontostände genau berechnet werden. Einige Beispiele für präventive oder detektive SOX-Kontrollen sind:

Trennung von widersprüchlichen und unvereinbaren Aufgaben (z. B. die Möglichkeit, Rechnungen zu buchen und zu genehmigen),

Überprüfungen einzelner oder mehrerer Transaktionen, die in der Periode erfasst wurden, und

Kontenabstimmungen.

Darüber hinaus müssen bei wesentlichen Konten häufig mehrere Kontrollen eingerichtet werden, um zu verhindern, dass wesentliche falsche Angaben gemacht werden. Sie müssen alle Kontrollen analysieren, um festzustellen, welche am besten Sicherheit bieten, wobei Sie die vorhandenen Mitarbeiter, Prozesse und Technologien im Auge behalten.

Audit-Teams werden davor gewarnt, einen Brute-Force-Ansatz anzuwenden und eine neue SOX-Kontrolle zu erstellen, wenn ein neues Risiko identifiziert wird. Versehentlich wird jede neue Kontrolle oft als "Schlüssel" eingestuft, ohne dass eine echte Risikobewertung durchgeführt wird, was zu der ständig steigenden Anzahl von Kontrollen beiträgt. Durch das

Verständnis der Unterschiede zwischen wichtigen und nicht-zentralen Kontrollen können interne Auditteams die steigende Anzahl von Kontrollen und die Ausweitung des "Scope Creep" wirksam bekämpfen.

Um die Dinge einfach zu halten, besteht die schnellste Methode zur Unterscheidung einer nicht schlüsselrelevanten vs. key Kontrolle darin, sich auf das Niveau des Risikos zu beziehen, das angesprochen wird. Ist die Kontrolle ein geringes oder hohes Risiko? Durch das Verständnis der Risiken, die sich auf den SOX-Compliance-Prozess auswirken, können Audit-Teams ihre Prioritäten besser setzen und ihre Bemühungen auf wichtige Kontrollen konzentrieren.

Um ein effektives System interner Kontrollen abzuschließen und zu planen, muss Ihr Prüfungsteam schließlich manuelle und automatisierte Kontrollen identifizieren. Für die identifizierten automatisierten Kontrollen sollten Sie bewerten, ob das zugrunde liegende System in den Geltungsbereich von ITGC-Tests (IT General Controls) fällt, was sich auf Ihre gesamte Teststrategie für die Kontrolle auswirkt. Wenn Sie ITGC-Komfort über das zugrunde liegende System haben, können Sie den Umfang der durchzuführenden Kontrolltests erheblich reduzieren. Der Betrieb starker ITGCs und Cybersicherheitskontrollen sind ein weiterer Vorteil der SOX-Compliance.

4) Durchführung einer Betrugsrisikobewertung

Zu einem wirksamen internen Kontrollsystem gehört auch die Bewertung möglicher betrügerischer Aktivitäten. Prävention und Früherkennung sind entscheidend, um Betrugsfälle in einem Unternehmen zu reduzieren. Interne Kontrollen spielen eine Schlüsselrolle bei der Verringerung der verfügbaren

Betrugsmöglichkeiten und der wesentlichen Auswirkungen eines Betrugs, einschließlich einer manuellen Überschreibung der internen Kontrollen.

Im Folgenden finden Sie Beispiele für interne Kontrollen und Praktiken zur Betrugsbekämpfung, die Unternehmen implementieren können, um Verluste durch Betrug erheblich zu senken.

Aufgabentrennung: Das Institute of Internal Auditors (IIA) beschreibt die Grundidee der Aufgabentrennung wie folgt: "Kein Mitarbeiter oder eine Gruppe von Mitarbeitern sollte in der Lage sein, Fehler oder Betrug im normalen Rahmen seiner Aufgaben zu begehen und zu verbergen." Das heißt, die Arbeit eines Individuums sollte entweder unabhängig von der Arbeit eines anderen sein oder dazu dienen, sie zu kontrollieren. Beispiele:

Verwahrung von Vermögenswerten

Genehmigung/Genehmigung von damit verbundenen Transaktionen, die diese Vermögenswerte betreffen

Erfassung und Berichterstattung über damit verbundene Transaktionen

Spesenerstattungen: Laut dem ACFE-Bericht von 2014 handelt es sich bei einem erheblichen Teil der Veruntreuungsprogramme um Situationen, in denen ein Mitarbeiter einen Anspruch auf Erstattung fiktiver oder überhöhter Geschäftsausgaben geltend macht. Um solche Systeme zu verhindern, sollte das Management sicherstellen, dass die relevanten Richtlinien und Verfahren für Mitarbeitererstattungen den Mitarbeitern mitgeteilt und bei Bedarf aktualisiert werden. Darüber hinaus sollte der Genehmigungsprozess für solche Erstattungen neben dem

direkten Vorgesetzten auch andere wichtige Stakeholder umfassen, wie z. B. betroffene Mitglieder des Geschäftsteams, die Gehaltsabrechnung oder die interne Revision.

Whistleblower-Hotline: Trotz bundesstaatlicher Vorschriften liegt die letztendliche Verantwortung für die Implementierung eines starken Whistleblower-Programms beim Management. In der Vergangenheit waren interne Mitarbeiterhinweise das beste Mittel zur Betrugserkennung. Daher kann es sich das Management nicht leisten, einen internen Whistleblower-Mechanismus innerhalb der Organisation zu vernachlässigen.

Periodische Abstimmung von Bankkonten: Bankabstimmungen heben die Unterschiede zwischen der Kasse pro Bilanz und dem Kontoauszug hervor und bestätigen gleichzeitig die Richtigkeit der im Kassenbuch der Organisation aufgezeichneten Daten. Die Kernaufgabe bei der Durchführung einer Bankabstimmung besteht nicht nur darin, unerwartete Unterschiede zu identifizieren, sondern auch darin, zukünftige Ereignisse zu verhindern, wie z. B. Buchhaltungsverzögerungen, die Beschränkung von automatischen Lastschriften auf Lieferanten usw. Je nach Größe des Unternehmens sollten Bankabstimmungen täglich, wöchentlich oder monatlich durchgeführt werden, um betrügerische Aktivitäten zu überwachen und zu erkennen.

Es ist der proaktive Ansatz des Managements zur Betrugserkennung und -prävention, gepaart mit starken internen Kontrollen, die letztendlich die Möglichkeiten zur Begehung von Betrug verringern und eine ethische Kultur in einem Unternehmen einführen.

5) Verwaltung der Dokumentation zu Prozessen und SOX-Kontrollen

Die Kontrollbeschreibung und -dokumentation enthalten Details zur Funktionsweise der wichtigsten Kontrollen, wie z. B. Beschreibungen der Kontrollen, Häufigkeit, Testverfahren, damit verbundene Risiken, Grundgesamtheit und Nachweise. Die Risiko- und Kontrollzuordnung hat oft eine m:n-Beziehung, was die manuelle Dokumentation erschwert. Einige Beispiele sind Risiken, die über mehrere Prozesse oder Geschäftseinheiten hinweg auftreten, Audit-Probleme, die sich auf mehrere Kontrollen oder Prozesse auswirken, und COSO-Prinzipien, die vielen Kontrollen zugeordnet sind. Wie ein Audit-Manager bestätigen kann, kann der nachgelagerte Dominoeffekt die Manager Stunden und Stunden der Bereinigung kosten, wenn ein Mitglied des Teams es versäumt, rechtzeitig eine Bearbeitung vorzunehmen oder zu vergessen, Aktualisierungen für alle Testblätter vorzunehmen. Die Lösung besteht darin, eine zugrunde liegende relationale Datenbank zu nutzen, die als zentrales Repository und als Grundlage des Auditprogramms fungiert. SOX-Software, die auf speziell entwickelten Datenbankstrukturen basiert, kann es Auditoren ermöglichen, Informationen schnell in eine Datenbank zu ziehen oder zu übertragen, und diese Ergebnisse sofort im gesamten SOX-Programm kaskadieren zu lassen. Die Dokumentation der Steuerelemente ist einfach und erfordert keine Änderungen an mehreren eigenständigen Tabellenkalkulationsdateien. Darüber hinaus kann eine Tabelle keine großen Datenmengen verarbeiten, damit die Ergebnisse der jährlichen Prüfung von Jahr zu Jahr verwendet werden können. Die Geschwindigkeit, Genauigkeit

und Skalierbarkeit einer Datenbanklösung wird die Vorteile der "Vertrautheit mit Tabellenkalkulationen" übertreffen.

6) Testen der wichtigsten Bedienelemente

Das übergeordnete Ziel von SOX-Kontrolltests ist dreierlei: 1) sicherzustellen, dass der Prozess oder die Testverfahren, wie beschrieben, eine effektive Methode zum Testen der Kontrolle sind, 2) die Kontrolle über den gesamten Zeitraum und vom zugewiesenen Prozessverantwortlichen durchgeführt wird, und 3) die Kontrolle war erfolgreich bei der Vermeidung oder Aufdeckung wesentlicher falscher Angaben. Kurz gesagt, Kontrolltests validieren das Design und die Betriebswirksamkeit von Kontrollen.

Der eigentliche Testprozess für SOX-Kontrollen kann eine Vielzahl oder Kombination von Testverfahren umfassen, einschließlich laufender Bewertung, Beobachtung, Anfragen bei Prozessverantwortlichen, Walkthrough der Transaktion, Inspektion des Dokumentationspfads und/oder einer erneuten Durchführung des Prozesses.

7) Bewertung von Mängeln in SOX

Kontinuierliche Investitionen in ein SOX-Programm führen natürlich zu einer Verbesserung Ihrer Maßnahmen, Richtlinien und Verfahren. Mit der Verbesserung des Kontrollumfelds werden die Unternehmen wahrscheinlich auch einen deutlichen Anstieg des Automatisierungsgrades und einen entsprechenden Rückgang des Umfangs der manuellen Tests feststellen, die von Auditoren verlangt werden. Letztendlich wird dies dazu führen, dass Ihr Team weniger Zeit mit der Verwaltung von Problemen verbringt. Mängel sollten auf ein akzeptables und vorhersehbares

Maß reduziert werden, und es sollte wenig bis gar keine Überraschungen geben.

Während des Testprozesses und der Analyse der SOX-Kontrolle kann der Prüfer eine Ausnahme, einen Mangel oder eine Lücke in der getesteten Probe feststellen. In diesem Fall wird ein "Problem" erstellt. Neben der Behebung und Korrektur des Problems beurteilt das Auditteam, ob es sich um einen Konstruktionsfehler in der Steuerung oder einen Betriebsfehler handelte, bei dem Schulungen, Verantwortlichkeiten oder Prozesse angepasst werden müssen. Schließlich beurteilen das Management und das Prüfungsteam, ob es sich um eine wesentliche Schwäche handelt (wie oben beschrieben, handelt es sich in der Regel um einen Prozentsatz der Abweichung und mit einem hohen Risikoniveau) und ob es sich um eine wesentliche Schwäche handelt, oder ob es sich nur um eine wesentliche Schwäche handelt.

8) Erstellung des Berichts des Managements über die Kontrollen

Das Endprodukt der SOX-Kontrolltests ist der Bericht des Managements über die Kontrollen der Finanzberichterstattung, der dem Prüfungsausschuss vorgelegt wird. Während des Prozesses wird zwar eine beträchtliche Menge an Dokumentationen und Daten gesammelt, aber der Bericht sollte Folgendes enthalten:

Zusammenfassung der Meinung des Managements und Unterstützung dieser Schlussfolgerungen.

Überprüfung des verwendeten Rahmens, der gesammelten Nachweise und der Zusammenfassung der Ergebnisse.

Ergebnisse aus jedem der Tests – Entitätsebene, IT, Schlüsselkontrollen.

Identifizierung der Steuerungsfehler, Lücken und entsprechenden Ursachen.

Bewertung durch den unabhängigen, externen Wirtschaftsprüfer des Unternehmens.

SOX-ITGCs und Sicherheitskontrollen

Da sich die Technologielandschaft schnell weiterentwickelt, wirkt sich die Abhängigkeit von Unternehmen auf Informationstechnologie und -systeme für die Verwaltung von Finanzinformationen erheblich darauf aus, wie ein Unternehmen seine Berichte der Securities and Exchange Commission (SEC) erstellt und bereitstellt. Da die meisten Unternehmen finanziell bedeutende Funktionen und Abläufe auf Informationssysteme verlagert haben, einschließlich Buchhaltungsfunktionen, Finanzfunktionen und sogar Einzelhandels-/E-Commerce-Funktionen, können die Auswirkungen erfolgreicher Cyberangriffe auf ein Unternehmen schwerwiegend sein. Auch ohne Auswirkungen auf die SOX-Compliance-Aktivitäten eines Unternehmens können Sicherheitsvorfälle zu Datenschutzverletzungen und Datenverlusten führen, was eine weitere Reihe von Herausforderungen für ein Unternehmen mit sich bringt.

Einige der grundlegenden ITGCs, die im Rahmen von SOX getestet werden, können dazu beitragen, Sicherheitsverletzungen und die Manipulation finanziell wesentlicher Informationen zu verhindern. Durch die Einrichtung effektiver Sicherheitskontrollen in Bezug auf Datenschutz,

Änderungsmanagement und sensible Daten können IT-Abteilungen potenzielle Sicherheitsvorfälle besser erkennen, verhindern und beheben. Selbst Unternehmen, die Cloud-Dienste stark nutzen und keine eigenen Rechenzentren haben, sollten die Compliance-Berichte ihrer Drittanbieter regelmäßig überprüfen, um zu überprüfen, ob die Standards der Anbieter für die Datensicherheit mit Ihren Unternehmen übereinstimmen. Die Nichteinhaltung durch einen Lieferanten kann immer noch ein erhebliches Risiko für die Kunden dieses Lieferanten darstellen.

Häufige Herausforderungen bei der SOX-Compliance

Probleme mit Tabellenkalkulationen und Endbenutzern

Die einfache Tabellenkalkulation hat sich zu mehr als nur einem Buchhaltungstool entwickelt. Im Laufe der Zeit hat sich die einfache Tabellenkalkulation zu einem Grundnahrungsmittel für SOX-Workflows entwickelt, was zum Teil auf ihre Fähigkeit zurückzuführen ist, Daten über verschiedene Dokumente hinweg zu verknüpfen und grundlegende Aufgaben zu automatisieren. Gleichzeitig benötigen moderne Audit-Projekte heute mehr Attribute und Details zur Steuerung. Unabhängig davon, ob es um die Dokumentation der Vollständigkeit und Genauigkeit von Nachweisen oder die Validierung der Integrität eines wichtigen Berichts geht, haben sich die Testverfahren über das einfache Ticken und Verknüpfen von Attributen hinaus entwickelt. Die moderne Tabellenkalkulation kann diesen robusten Testprozess bewältigen, aber es mangelt ihnen an Geschwindigkeit, Effizienz und Konsistenz.

Zusätzlich zu den oben genannten Risiken gibt es bestimmte Risiken im Zusammenhang mit der Verwendung von Tabellenkalkulationen für Ihr SOX-Programm, einschließlich, aber nicht beschränkt auf:

Falsche Eingabe durch einen Benutzer oder gelöschte Daten

Analyse eines inkonsistenten Datensatzes – d. h. die Grundgesamtheit ist falsch

Prozessverantwortliche im Dunkeln gelassen

Prozessverantwortliche, die für die täglichen Kontrollaktivitäten verantwortlich sind, werden oft im Dunkeln gelassen, wenn es um ihre eigenen Kontrollen geht. Interne Audit-Teams verlassen sich auf Tabellenkalkulationen und freigegebene Ordner, um ihre Kontrollen zu verwalten, sodass die Dokumentation oft auf dem Desktop der internen Audit-Teams verbleibt – weit weg von den Prozessverantwortlichen.

Wenn die Kontrolldokumentation bei der internen Revision angesiedelt ist, erhalten die Prozessverantwortlichen nur einmal im Quartal Einblick in ihre Kontrollen und erstellen so ihre eigenen täglichen Aktivitäten, die von ihrer eigenen Version der Aufgaben gesteuert werden, und nicht unbedingt im Kontext ihrer eigenen Kontrollen.

Steigende Kosten und Ressourcen

Obwohl sich SOX positiv auf die Finanzberichterstattung ausgewirkt hat, bestehen nach wie vor Bedenken hinsichtlich der steigenden Kosten für die SOX-Compliance und der hohen Ressourcenbelastung. Die SOX-Kosten steigen bei vielen Unternehmen im Vergleich zum Vorjahr weiter an, so die jährliche Sarbanes Oxley Survey von Protiviti. Zu den Gründen gehören die

Einführung neuer Rahmenwerke wie COSO und die sich entwickelnden Anforderungen externer Prüfer an die Einhaltung von Section 404. Unternehmen geben heute jährlich durchschnittlich eine Million bis zwei Millionen Dollar und bis zu 10.000 Stunden für SOX-Programme aus.

Vereinfachen Sie die SOX-Compliance mit speziell entwickelter Technologie

Ein Schlüssel zur Verringerung der kostspieligen und zeitaufwändigen SOX-Compliance und zur Maximierung der SOX-Ressourcen liegt in der Nutzung speziell entwickelter Technologien zur Automatisierung von Prozessen. Vorausschauende SOX-Teams nutzen SOX-Automatisierungstools, um den Verwaltungsaufwand und den Aufwand für SOX zu reduzieren. SOX-Compliance-Software ermöglicht es Teams, Zeit für wertschöpfendere Audits zu gewinnen, die Qualität der internen Kontrollen zu erhöhen, die Echtzeit-Transparenz in SOX-Umgebungen zu verbessern, die Zusammenarbeit mit externen Prüfern zu fördern – und letztendlich finanzielle Anpassungen zu vermeiden.

Häufig gestellte Fragen zur SOX-Compliance

Was ist der Sarbanes-Oxley Act (SOX) und warum wurde er erlassen?

Der Sarbanes-Oxley Act, allgemein bekannt als SOX, ist ein US-Bundesgesetz, das im Jahr 2002 erlassen wurde, um Anleger zu schützen, indem die Genauigkeit und Zuverlässigkeit von Unternehmensangaben verbessert wird. Es wurde als Reaktion auf große Unternehmens- und Bilanzskandale, einschließlich derjenigen, in die Enron und WorldCom verwickelt waren,

verabschiedet, um das Vertrauen der Öffentlichkeit in die Finanzmärkte wiederherzustellen.

Was sind die wichtigsten Anforderungen an die SOX-Compliance?

Die SOX-Compliance verlangt von Unternehmen, dass sie robuste interne Kontrollen für die Finanzberichterstattung implementieren und aufrechterhalten. Zu den wichtigsten Anforderungen gehören die Bescheinigung von Jahresabschlüssen durch CEOs und CFOs (§ 302), die Einrichtung eines internen Kontrollrahmens (§ 404) und die Unabhängigkeit der externen Revisionsstelle (§ 301). Unternehmen müssen außerdem regelmäßige SOX-Audits durchführen, um die Einhaltung dieser Standards sicherzustellen.

Wie kann ein Unternehmen eine erfolgreiche SOX-Compliance sicherstellen?

Um eine erfolgreiche SOX-Compliance zu gewährleisten, sollten Unternehmen ein eigenes SOX-Compliance-Team einrichten, umfassende interne Kontrollen implementieren und regelmäßige Schulungen für die Mitarbeiter durchführen. Der Einsatz von Audit-Management-Software wie Audit Board kann Compliance-Prozesse rationalisieren, indem Workflows automatisiert, Echtzeit-Datenanalysen bereitgestellt und detaillierte Compliance-Berichte erstellt werden. Regelmäßige Audits und kontinuierliche Überwachung sind ebenfalls unerlässlich, um die Einhaltung der Vorschriften zu gewährleisten und Probleme umgehend zu beheben.

Laster

Vice Vicente begann seine Karriere bei EY und war in den letzten 10 Jahren in den Bereichen IT-Compliance, Risikomanagement

und Cybersicherheit tätig. Vice hat über 120 Kunden betreut, geprüft oder beraten, Sicherheits- und Compliance-Programme und -Technologien implementiert, Engagements rund um SOX 404, SOC 1, SOC 2, PCI DSS und HIPAA durchgeführt und Unternehmen bei der Sicherheits- und Compliance-Bereitschaft begleitet. Verbinden Sie sich mit Vice auf LinkedIn.