ساربينز أوكسلي

في عام 2002، أقر الكونجرس قانون ساربينز أوكسلي (SOX) استجابة للتداعيات وعدم اليقين في أعقاب أحداث الاحتيال والفضائح المالية في العديد من الشركات، بما في ذلك WorldCom و Enron. أدخل قانون SOX العديد من الإصلاحات الرئيسية لتنظيم الإفصاحات المالية وإدارة الشركات بهدف استعادة ثقة الجمهور في مراجعة الحسابات والإبلاغ المالي. تم تسمية قانون SOX ، المعروف أيضا باسم "قانون إصلاح محاسبة الشركات العامة وحماية المستثمرين" أو "قانون مساءلة ومسؤولية الشركات والتدقيق" ، على اسم مهندسيه الرئيسيين ، السناتور بول ساربانيس والنائب مايكل أوكسلي.

تنطبق متطلبات الامتثال الجديدة أو الموسعة على جميع مجالس إدارة الشركات العامة الأمريكية وإدارتها وشركات المحاسبة. قد تجد الشركات الخاصة التي تفكر في الاكتتاب العام أو تستعد للاندماج أو الاستحواذ أيضا مراجعة ضوابطها الداخلية في SOX أمرا حكيما. من بين الأحكام الأخرى ، يفرض SOX:

تتضمن جميع التقارير المالية للشركات تقرير الضوابط الداخلية.

بيانات مالية دقيقة وضوابط لحماية البيانات المالية.

إصدار تقارير الإفصاح المالي لنهاية العام.

الإفصاح عن احتيال الشركات من خلال حماية الموظفين المبلغين عن المخالفات.

يقدم كيم فام لمحة عامة عن امتثال SOX وتأثيره وتحدياته ومخاوفه والاستفادة من الحلول التكنولوجية للامتثال ل SOX.

أضافت ساربينز أوكسلي متطلبات المساءلة للقادة والإدارة ، مما يجعلهم مسؤولين عن دقة البيانات المالية لمنظمتهم. لعب سوء السلوك التنفيذي دورا رئيسيا في فضائح إنرون وورلدكوم وتايكو ، من بين أمور أخرى ، ولا يزال يؤثر على مواقف المنظمات تجاه الإفصاحات المالية والممارسات المحاسبية. وهكذا ، فتحت SOX الباب لتحميل المديرين التنفيذيين المسؤولية عن الاحتيال في التقارير المالية. TL. يضمن الامتثال ل DR SOX التزام الشركات بمعايير التقارير المالية الصارمة والضوابط الداخلية ، مما يعزز الشفافية وثقة المستثمرين. تغطي هذه المقالة أساسيات الامتثال ل SOX وتنفيذه والفوائد التي يوفرها بما يتجاوز مجرد الالتزام التنظيمي.

ستوضح هذه المقالة متطلبات الامتثال المختلفة ل SOX ، وتحديات SOX ، وفوائد التوافق مع SOX ، وما يمكن توقعه أثناء عملية تدقيق SOX.

يتم فرض الامتثال ل SOX من قبل لجنة الأوراق المالية والبورصات (SEC) بصفتها الوكالة الفيدرالية الرئيسية المسؤولة عن حماية المستثمرين والحفاظ على أسواق عادلة وفعالة ، تضمن هيئة الأوراق المالية والبورصات التزام الشركات بالمتطلبات الصارمة المنصوص عليها في قانون ساربينز أوكسلي. وتساعد رقابة هيئة الأوراق المالية والبورصات على تعزيز الشفافية والمساءلة والنزاهة في إعداد التقارير المالية، وبالتالي تعزيز ثقة المستثمرين واستقرار السوق. كان مجلس الإشراف على محاسبة الشركات العامة (PCAOB) وكالة جديدة أنشأتها SOX وهي مسؤولة عن الإشراف على شركة المحاسبة العامة وجودة عمليات تدقيق الشركات العامة. يتكون قانون ساربينز أوكسلي لعام 2002 من 11 عنوانا ، ولكن هناك حكمان رئيسيان يتعلقان بمتطلبات الامتثال: القسمان 302 و 404.

القسم 302: مسؤولية الشركات عن التقارير المالية

ينص القسم 302 من SOX على أن الرؤساء التنفيذيين (CEOs) وكبار المسؤولين الماليين (CFOs) مسؤولون بشكل مباشر عن دقة التقارير المالية. يجب على مسؤولي التوقيع مراجعة دقة البيانات المالية والتصديق عليها ، وإنشاء ضوابط داخلية والحفاظ عليها ، والكشف عن جميع أوجه القصور الهامة والاحتيال والتغييرات المهمة في الضوابط الداخلية.

يسمح هذا التفويض للمديرين التنفيذيين والمديرين الماليين بالمساءلة عن عدم الدقة في البيانات المالية لمنظماتهم ، بما في ذلك العقوبات الجنائية. يمكن أن يؤدي عدم الامتثال لقسم SOX 302 إلى عقوبات مدنية وجنائية كبيرة ، بما في ذلك غرامات تصل إلى 5 ملايين دولار والسجن لمدة تصل إلى 20 عاما للمديرين التنفيذيين الذين يصادقون عن عمد على التقارير المالية الكاذبة.

القسم 404: التقييم الإداري للضوابط الداخلية

ينص القسم 404 على أن جميع التقارير السنوية يجب أن تتضمن تقريرا عن الرقابة الداخلية يحدد صراحة مسؤولية الإدارة عن الحفاظ على هيكل رقابة داخلية مناسب ، وتقييم فعاليته ، وأي أوجه قصور في تلك الضوابط. كما يجب أن يشهد المدققون الخارجيون المستقلون على دقة بيان الشركة بأن الضوابط الداخلية موجودة وفعالة. يتضمن القسم 404 متطلبات إضافية مثل مراجعة الضوابط الداخلية للشركة من قبل مراجعي الحسابات الخارجيين ويوفر إعفاءات لبعض الشركات. تقدم مراجعة مجلس التدقيق ل SOX 404 معلومات أكثر تفصيلا حول قسم SOX هذا.

للحد من تضارب المصالح ، يجب إجراء التدقيق الخارجي 404 من قبل مدققين مستقلين يمارسون الشك المهني والحكم لفحص حالة الضوابط الداخلية في الشركات المتداولة علنا.

فوائد الامتثال SOX 404

كانت إحدى النتائج الحاسمة ل ساربينز أوكسلي هي إنهاء التنظيم الذاتي وإنشاء إشراف مستقل على عملية التدقيق من خلال مجلس الإشراف على محاسبة الشركات العامة (PCAOB). يمكن ل PCAOB وضع معايير الصناعة ، والتحقيق في مزاعم الاحتيال ، وتنظيم شركات التدقيق. في الواقع، يقوم PCAOB بإجراء عمليات تدقيق منتظمة للمراجعين لضمان بقاء الجودة عالية واتباع أفضل الممارسات الصناعية.

بقدر ما كافحت الشركات في البداية مع عبء التكلفة والموارد للامتثال ، بمرور الوقت ، فإنها ترى أن الاستثمار في الامتثال ل SOX يؤتي ثماره بعدة طرق مهمة.

1. تحسين حوكمة الشركات: أدى الامتثال ل SOX إلى تحسين حوكمة الشركات من خلال زيادة تنظيم لجان التدقيق. قبل SOX ، كان لدى 51٪ من الشركات العامة لجان تدقيق مستقلة تماما عن الإدارة. وفرضت سوكس على جميع الشركات المدرجة أن يكون لديها لجنة تدقيق يكون أعضاؤها مستقلين عن الإدارة ولديهم خبير مالي واحد على الأقل. ونتيجة لذلك، أصبحت لجان مراجعة الحسابات اليوم مجهزة بشكل أفضل لتقديم تقارير مالية دقيقة وصادقة. وللجان المستقلة لمراجعة الحسابات ولاية مختلفة عن غيرها، مما يضيف طبقة أخرى من الإدارة إلى عملية الإبلاغ المالي.

2. زيادة المساءلة: الامتثال ل SOX يجعل المديرين التنفيذيين أكثر عرضة للمساءلة ويحمي المستثمرين. يطلب من المديرين التنفيذيين التصديق شخصيا على التقارير المالية ، مع فرض عقوبات كبيرة على الأنشطة الاحتيالية. يتحمل المدققون أيضا مسؤولية كبيرة للحفاظ على النزاهة والاستقلالية حيث أدت فضائح الاحتيال التي غذت ساربينز أوكسلي أيضا إلى سقوط آرثر أندرسن ، واحدة من أكبر شركات المحاسبة في ذلك الوقت.

3. تحسين استقلالية المدقق وجودته: يعزز امتثال SOX استقلالية المدقق من خلال منع شركات التدقيق من توفير وظائف مسك الدفاتر أو الاكتوارية أو الإدارية للشركات التي تقوم بتدقيقها. يجب على المدققين الخارجيين الحفاظ على الاستقلالية في المظهر وفي الواقع. هذا يحسن جودة التدقيق ودقة التدقيق.

4. عدد أقل من عمليات إعادة البيانات المالية: بعد SOX ، يستمر عدد عمليات إعادة صياغة السجلات المالية في الانخفاض على أساس سنوي ، حيث انخفض من 1,784 في عام 2006 إلى 738 في عام 2012.

5. تحسين إدارة المخاطر ووضع الأمن السيبراني: تتداخل العديد من أفضل الممارسات التي تنفذها المؤسسات الحالية كجزء من الامتثال ل SOX ، وخاصة الضوابط العامة لتكنولوجيا المعلومات ، مع إرشادات من أطر الأمن السيبراني مثل NIST CSF. أحد الأمثلة على هذا التداخل هو الدعوة إلى التحكم القوي والمقيد في الوصول وإدارة الوصول لحماية الأنظمة والمعلومات الحساسة من الوصول غير المصرح به - تتطلب معظم عمليات تدقيق SOX 404 ذلك لأنظمة المعلومات المادية ماليا ، ويوصي NIST CSF بشدة بهذا كجزء من ركيزة "الحماية" الخاصة بهم.

للتلخيص ، فإن بعض الفوائد الرئيسية للحفاظ على الامتثال ل SOX وتكراره في مؤسستك ، بخلاف مجرد البقاء في الامتثال هي: 1) تحسين حوكمة الشركات ، 2) زيادة المساءلة ، 3) تحسين استقلالية المدقق وجودته ، 4) عدد أقل من عمليات إعادة البيانات المالية ، و 5) تحسين إدارة المخاطر ووضع الأمن السيبراني.

تطور SOX: اعتماد التكنولوجيا والتركيز على التكلفة وسط تغييرات الأعمال ، والإنترنت ، وتفويضات ESG

عملية تدقيق SOX

يمكن تقسيم عمليات تدقيق SOX إلى أي عدد من الخطوات ، من إجراء تقييمات المخاطر إلى ما يجب تضمينه في تقرير لجنة التدقيق. لقد قمنا بتضييق مخططنا لعملية تدقيق SOX إلى الخطوات الثماني التالية:

تحديد نطاق التدقيق باستخدام نهج تقييم المخاطر

تحديد الأهمية النسبية والمخاطر - الحسابات والبيانات والمواقع والعمليات والأنظمة والمعاملات الرئيسية

تحديد عناصر تحكم SOX - الضوابط العامة لتكنولوجيا المعلومات (ITGCs) ، وضوابط التطبيق ، وعناصر التحكم على مستوى الكيان (ELCs) ، وما إلى ذلك.

إجراء تقييم مخاطر الاحتيال

إدارة وثائق العمليات والتحكم

اختبار عناصر التحكم الرئيسية

تقييم أوجه القصور

تقديم تقرير الإدارة حول الضوابط

1) تحديد نطاق تدقيق SOX باستخدام نهج تقييم المخاطر

لإجراء تقييم للمخاطر ، ينص المعيار المحاسبي PCAOB رقم 5 على أن "النهج من أعلى إلى أسفل يبدأ على مستوى البيانات المالية وبفهم المدقق للمخاطر الإجمالية للضوابط الداخلية على التقارير المالية. ثم يركز المدقق على الضوابط على مستوى الكيان ويعمل وصولا إلى الحسابات المهمة والإفصاحات والتأكيدات ذات الصلة ". باختصار ، يوصي PCAOB بأن يبدأ التدقيق على أعلى مستوى ، ليصبح أكثر دقة. يجب أن يكون تركيز نطاق التدقيق على تلك الأصول والأشخاص والأنظمة والعمليات التي تؤثر على عملية الإفصاح المالي - مما يعني أنه لن يكون كل شيء في المنظمة في النطاق. يجب أن يتضمن نطاق تدقيق SOX وينظر في جميع المخاطر التي تتعرض لها الضوابط الداخلية للمؤسسة على التقارير المالية في نهج المخاطر أولا للامتثال ل SOX.

يجب ألا تؤدي هذه الخطوة في تدقيق امتثال SOX إلى قائمة بإجراءات الامتثال. ومع ذلك ، يجب أن يساعد المدقق على تحديد المخاطر والمصادر المحتملة ، وكيف يمكن أن تؤثر على الأعمال ، وما إذا كانت الضوابط الداخلية ستوفر تأكيدا معقولا بأنه سيتم تجنب الخطأ المادي أو منعه أو اكتشافه.

2) تحديد الأهمية النسبية في SOX - الحسابات والبيانات والمواقع والعمليات والمعاملات الرئيسية

الخطوة 1 - تحديد ما يعتبر جوهريا للربح والخسارة والميزانية العمومية. كيف: تعتبر بنود البيانات المالية "جوهرية" إذا كان بإمكانها التأثير على القرارات الاقتصادية للمستخدمين. يمكن للمدققين عادة تحديد ما هو جوهري عن طريق حساب نسبة معينة من حسابات البيانات المالية الرئيسية. على سبيل المثال ، 5٪ من إجمالي الأصول ، 3-5٪ من الدخل التشغيلي ، أو بعض التحليلات لحسابات الربح والخسارة الرئيسية المتعددة و BS.

الخطوة 2 - تحديد جميع المواقع ذات أرصدة حسابات المواد. كيف: تحليل البيانات المالية لجميع المواقع التي تعمل فيها. إذا تجاوز أي من أرصدة حسابات البيانات المالية في هذه المواقع ما تم تحديده على أنه مادي (في الخطوة 1) ، فمن المحتمل أن يتم اعتبارها جوهرية وفي نطاق SOX في العام المقبل. الخطوة 3 - تحديد المعاملات التي تملأ أرصدة الحسابات المادية كيف: اجتمع مع المراقب المالي الخاص بك ومالكي العمليات المحددة لتحديد المعاملات (أي الديون والائتمانات) التي تتسبب في زيادة أو نقصان حساب البيانات المالية. يجب توثيق كيفية حدوث هذه المعاملات وكيفية تسجيلها في سرد أو مخطط انسيابي أو كليهما.

الخطوة 4 - تحديد مخاطر التقارير المالية للحسابات المادية. كيف: حاول فهم ما يمكن أن يمنع تسجيل المعاملة بشكل صحيح ، أو حدث المخاطرة. بعد ذلك ، قم بتوثيق التأثير الذي يمكن أن يحدثه حدث المخاطر على كيفية تسجيل رصيد الحساب بشكل غير صحيح ، أو تفصيل تأكيد البيان المالي.

3) تحديد عناصر تحكم SOX - الضوابط الرئيسية وغير الرئيسية ، و ITGCs ، والضوابط الأخرى على مستوى الكيان (ELCs)

أثناء تحليل الأهمية النسبية ، سيقوم المدققون بتحديد وتوثيق ضوابط SOX التي قد تمنع أو تكتشف المعاملات من التسجيل بشكل غير صحيح. سيسعون إلى تحديد الضوابط والأرصدة في عملية إعداد التقارير المالية التي تضمن تسجيل المعاملات بشكل صحيح ، ويتم حساب أرصدة الحسابات بدقة. تتضمن بعض الأمثلة على عناصر التحكم الوقائية أو المخبرية SOX ما يلي:

فصل الواجبات المتضاربة وغير المتوافقة (على سبيل المثال ، القدرة على نشر الفواتير والموافقة عليها) ،

مراجعات المعاملات الفردية أو المتعددة المسجلة في الفترة ، و

تسويات الحساب.

بعد ذلك ، غالبا ما تحتاج حسابات المواد إلى عناصر تحكم متعددة لمنع حدوث خطأ جوهري. سيتعين عليك تحليل جميع عناصر التحكم لتحديد أي منها يوفر الضمان بشكل أفضل ، مع الأخذ في الاعتبار الأشخاص والعملية والتكنولوجيا المعمول بها.

يتم تحذير فرق التدقيق من تطبيق نهج القوة الغاشمة وإنشاء عنصر تحكم SOX جديد كلما تم تحديد خطر جديد. عن غير قصد ، غالبا ما يتم تصنيف كل عنصر تحكم جديد على أنه "مفتاح" دون إجراء تقييم حقيقي للمخاطر ، مما يساهم في زيادة عدد عناصر التحكم باستمرار. من خلال فهم الاختلافات بين الضوابط الرئيسية وغير الرئيسية، يمكن لفرق التدقيق الداخلي مكافحة ارتفاع عدد الضوابط و"زحف النطاق" بشكل فعال.

لتبسيط الأمور ، فإن أسرع طريقة للتمييز بين عنصر التحكم في key vs. غير المفتاح هي الإشارة إلى مستوى المخاطر التي تتم معالجتها. هل تخفف السيطرة من مخاطر منخفضة أم عالية؟ من خلال فهم المخاطر التي تؤثر على عملية الامتثال ل SOX ، يمكن لفرق التدقيق تحديد الأولويات بشكل أفضل وتركيز جهودها على الضوابط الرئيسية.

وأخيرا، لوضع اللمسات الأخيرة على نظام فعال للضوابط الداخلية والتخطيط له، يجب على فريق التدقيق الخاص بك تحديد الضوابط اليدوية والآلية. بالنسبة لعناصر التحكم التلقائية المحددة ، يجب عليك تقييم ما إذا كان النظام الأساسي في نطاق اختبار عناصر التحكم العامة لتكنولوجيا المعلومات (ITGC) ، مما سيؤثر على استراتيجية الاختبار الشاملة لعنصر التحكم. إذا كان لديك راحة ITGC على النظام الأساسي ، فيمكنك تقليل كمية اختبار التحكم المطلوب إجراؤها بشكل كبير. يعد تشغيل ITGCs القوية والضوابط المتعلقة بالأمن السيبراني فائدة أخرى للامتثال ل SOX.

4) إجراء تقييم مخاطر الاحتيال

يتضمن النظام الفعال للضوابط الداخلية تقييما للنشاط الاحتيالي المحتمل. الوقاية والكشف المبكر أمران حاسمان للحد من حالات الاحتيال في المنظمة. تلعب الضوابط الداخلية دورا رئيسيا في الحد من الفرص المتاحة لارتكاب الاحتيال وما سيكون عليه الأثر المادي إذا حدث الاحتيال ، بما في ذلك التجاوز اليدوي للضوابط الداخلية.

فيما يلي أمثلة على الضوابط والممارسات الداخلية لمكافحة الاحتيال التي يمكن للمؤسسات تنفيذها لتقليل الخسائر الناجمة عن الاحتيال بشكل كبير.

الفصل بين الواجبات: يصف معهد المدققين الداخليين (IIA) الفكرة الأساسية الكامنة وراء الفصل بين الواجبات على أنها "لا ينبغي أن يكون أي موظف أو مجموعة من الموظفين في وضع يسمح لهم بارتكاب وإخفاء الأخطاء أو الاحتيال في السياق العادي لواجباتهم". أي أن عمل فرد ما يجب أن يكون إما مستقلا عن عمل فرد آخر أو يعمل على التحقق منه. امثله:

حراسة الأصول

الإذن/الموافقة على المعاملات ذات الصلة التي تؤثر على تلك الأصول

تسجيل المعاملات ذات الصلة والإبلاغ عنها

سداد النفقات: وفقا لتقرير ACFE لعام 2014 ، فإن جزءا كبيرا من مخططات اختلاس الأصول ينطوي على حالات يقدم فيها الموظف مطالبة بسداد نفقات الأعمال الوهمية أو المتضخمة. لمنع مثل هذه المخططات ، يجب على الإدارة ضمان إبلاغ الموظفين بالسياسات والإجراءات ذات الصلة المحيطة بتعويضات الموظفين وتحديثها عند الضرورة. علاوة على ذلك ، يجب أن يشمل تدفق الموافقة على عمليات السداد هذه ، إلى جانب المشرف المباشر ، أصحاب المصلحة الرئيسيين الآخرين ، مثل أعضاء فريق العمل المتأثرين أو كشوف المرتبات أو التدقيق الداخلي.

الخط الساخن للمبلغين عن المخالفات: على الرغم من اللوائح الفيدرالية ، فإن المسؤولية النهائية عن تنفيذ برنامج قوي للمبلغين عن المخالفات تقع على عاتق الإدارة. تاريخيا ، قدمت معلومات الموظفين الداخلية أفضل وسيلة للكشف عن الاحتيال. وبالتالي ، لا يمكن للإدارة أن تهمل آلية داخلية للمبلغين عن المخالفات داخل المنظمة.

التسوية الدورية للحسابات المصرفية: تسلط التسويات المصرفية الضوء على الاختلافات بين النقد لكل ميزانية عمومية وكشف الحساب المصرفي ، مع تأكيد دقة البيانات المسجلة في دفتر الأستاذ النقدي للمؤسسة. لا يقتصر الواجب الأساسي لإجراء التسوية المصرفية على تحديد الاختلافات غير المتوقعة فحسب ، بل يستلزم أيضا منع الحوادث المستقبلية ، مثل التأخيرات المحاسبية ، وتقييد الخصم التلقائي للبائعين ، وما إلى ذلك. اعتمادا على حجم المنظمة ، يجب إجراء التسويات المصرفية يوميا أو أسبوعيا أو شهريا لمراقبة النشاط الاحتيالي واكتشافه.

إن نهج الإدارة الاستباقي تجاه اكتشاف الاحتيال ومنعه ، إلى جانب الضوابط الداخلية القوية ، هو الذي سيقلل في النهاية من فرص ارتكاب الاحتيال ويغرس ثقافة أخلاقية داخل المنظمة.

5) إدارة العملية ووثائق ضوابط SOX

يحدد سرد التحكم والوثائق تفاصيل تشغيل الضوابط الرئيسية ، مثل أوصاف التحكم والتكرار وإجراءات الاختبار والمخاطر المرتبطة بها والسكان والأدلة. غالبا ما يكون لرسم خرائط المخاطر والتحكم علاقة متعدد إلى متعدد ، مما يجعل التوثيق اليدوي صعبا. تتضمن بعض الأمثلة المخاطر التي تظهر عبر عمليات أو وحدات أعمال متعددة ، ومشكلات التدقيق التي تؤثر على ضوابط أو عمليات متعددة ، وتعيين مبادئ COSO للعديد من الضوابط. كما يمكن لمدير التدقيق أن يشهد ، إذا فشل أحد أعضاء الفريق في إجراء تعديل في الوقت المناسب أو نسي إجراء تحديثات عبر جميع أوراق الاختبار ، فإن تأثير التموج النهائي يمكن أن يكلف المديرين ساعات وساعات من التنظيف. الحل هو الاستفادة من قاعدة بيانات علائقية أساسية لتكون بمثابة مستودع مركزي وكأساس لبرنامج التدقيق. يمكن لبرنامج SOX المبني على هياكل قواعد البيانات المصممة لهذا الغرض أن يسمح للمدققين بسحب أو دفع المعلومات من وإلى قاعدة البيانات بسرعة والحصول على هذه النتائج المتتالية في جميع أنحاء برنامج SOX بأكمله على الفور. وثائق عناصر التحكم بسيطة ولا تتطلب إجراء تعديلات عبر العديد من ملفات جداول البيانات المستقلة. بالإضافة إلى ذلك ، بالنسبة لنتائج التدقيق السنوية التي سيتم استخدامها عاما بعد عام ، لا يمكن لجدول البيانات معالجة كميات كبيرة من البيانات. ستتجاوز سرعة حل قاعدة البيانات ودقته وقابليته للتوسع فوائد "الإلمام بجدول البيانات".

6) اختبار الضوابط الرئيسية

الهدف العام من اختبار التحكم في SOX هو ثلاثة أضعاف - 1) التأكد من أن العملية أو إجراءات الاختبار كما هو موضح هي طريقة فعالة لاختبار التحكم ، 2) يتم تنفيذ التحكم طوال الفترة بأكملها ومن قبل مالك العملية المعين ، و 3) نجح التحكم في منع أو اكتشاف أي أخطاء جوهرية. باختصار ، يتحقق اختبار التحكم من صحة التصميم والفعالية التشغيلية لعناصر التحكم.

قد تتضمن عملية اختبار ضوابط SOX الفعلية مجموعة متنوعة أو مجموعة من إجراءات الاختبار بما في ذلك التقييم المستمر والملاحظة والاستفسارات مع مالكي العملية وتجول المعاملة وفحص مسار التوثيق و / أو إعادة أداء العملية.

7) تقييم أوجه القصور في SOX

سيؤدي الاستثمار المستمر في برنامج SOX بطبيعة الحال إلى تحسين إجراءاتك وسياساتك وإجراءاتك. مع تحسن بيئة التحكم ، من المرجح أن تشهد الشركات أيضا زيادة واضحة في مستوى الأتمتة وانخفاضا مقابلا في كمية الاختبار اليدوي المطلوب من قبل المدققين. في النهاية ، سيؤدي ذلك إلى قضاء فريقك وقتا أقل في إدارة عدد أقل من المشكلات الإجمالية. يجب تقليل أوجه القصور إلى مستوى مقبول ويمكن التنبؤ به ، ويجب أن تكون هناك مفاجآت قليلة أو معدومة.

أثناء عملية اختبار وتحليل التحكم في SOX ، قد يحدد المدقق إعفاء أو نقصا أو فجوة في العينة المختبرة. إذا حدث هذا ، يتم إنشاء "مشكلة". إلى جانب معالجة المشكلة وتصحيحها ، يقوم فريق التدقيق بعد ذلك بتقييم ما إذا كان فشل التصميم في التحكم أو فشل التشغيل حيث يحتاج التدريب أو المسؤوليات أو العملية إلى تعديل. وأخيرا، تقوم الإدارة وفريق التدقيق بتقييم ما إذا كان ضعفا جوهريا أم لا (كما هو موضح أعلاه هو عادة نسبة مئوية من التباين وبمستوى مخاطر مرتفع) وسيتم الإبلاغ عنه في البيانات المالية لنهاية العام أو إذا كان مجرد ضعف كبير.

8) تقديم تقرير الإدارة عن الضوابط

المنتج النهائي لاختبار التحكم SOX هو تقرير الإدارة حول الضوابط على التقارير المالية التي يتم تسليمها إلى لجنة التدقيق. وفي حين يتم جمع قدر كبير من الوثائق والبيانات أثناء العملية، ينبغي أن يتضمن التقرير ما يلي:

موجز رأي الإدارة ودعمها لتلك الاستنتاجات.

مراجعة الإطار المستخدم والأدلة التي تم جمعها وملخص النتائج.

النتائج من كل اختبار - على مستوى الكيان ، وتكنولوجيا المعلومات ، والضوابط الرئيسية.

تحديد إخفاقات التحكم والثغرات والأسباب الجذرية المقابلة.

التقييم الذي أجراه مدقق الحسابات الخارجي المستقل للشركة.

SOX ITGCs والضوابط الأمنية

مع تطور المشهد التكنولوجي بسرعة ، يؤثر اعتماد الشركات على تكنولوجيا المعلومات والأنظمة لإدارة المعلومات المالية بشكل كبير على كيفية قيام الشركة بتجميع وتقديم تقارير لجنة الأوراق المالية والبورصات (SEC). نظرا لأن معظم الشركات قد نقلت وظائف وعمليات مهمة ماليا إلى أنظمة المعلومات ، بما في ذلك وظائف المحاسبة والوظائف المالية وحتى وظائف البيع بالتجزئة / التجارة الإلكترونية ، فإن تأثير الهجمات الإلكترونية الناجحة على المؤسسة يمكن أن يكون شديدا. حتى بدون التأثير على أنشطة الامتثال ل SOX الخاصة بالشركة ، يمكن أن تؤدي الحوادث الأمنية إلى خروقات البيانات وفقدان البيانات ، مما يخلق مجموعة أخرى من التحديات للشركة.

يمكن أن تساعد بعض ITGCs التأسيسية التي يتم اختبارها كجزء من SOX في تجنب الانتهاكات الأمنية والتلاعب بالمعلومات المادية المالية. من خلال إنشاء ضوابط أمنية فعالة حول حماية البيانات وإدارة التغيير والبيانات الحساسة ، يمكن لأقسام تكنولوجيا المعلومات اكتشاف أي حوادث أمنية محتملة ومنعها وتنفيذها بشكل أفضل. حتى الشركات التي تستفيد بشكل كبير من الخدمات السحابية وليس لديها مراكز بيانات خاصة بها يجب أن تراجع بانتظام تقارير امتثال موردي الجهات الخارجية للتحقق من أن معايير البائعين لأمن البيانات تتوافق مع مؤسستك. لا يزال عدم الامتثال من جانب البائع ينطوي على مخاطر كبيرة لعملاء ذلك البائع.

تحديات الامتثال SOX الشائعة

مشاكل جداول البيانات والمستخدم النهائي

لقد تطور جدول البيانات المتواضع ليكون أكثر من مجرد أداة مسك الدفاتر. بمرور الوقت ، تحول جدول البيانات البسيط إلى عنصر أساسي في سير عمل SOX ، ويرجع ذلك جزئيا إلى قدرته على ربط البيانات عبر مستندات مختلفة وأتمتة المهام الأساسية. في الوقت نفسه ، تتطلب مشاريع التدقيق الحديثة الآن المزيد من السمات والتفاصيل حول التحكم. سواء كان الأمر يتعلق بتوثيق اكتمال الأدلة ودقتها ، أو التحقق من سلامة تقرير رئيسي ، فقد تطورت إجراءات الاختبار إلى ما هو أبعد من مجرد تحديد السمات وربطها. يمكن لجدول البيانات الحديث التعامل مع عملية الاختبار القوية هذه ولكنه يفتقر إلى السرعة والكفاءة والاتساق.

بالإضافة إلى ما هو مذكور أعلاه ، هناك بعض المخاطر المتعلقة باستخدام جداول البيانات لبرنامج SOX الخاص بك ، بما في ذلك ، على سبيل المثال لا الحصر:

خطأ من قبل مستخدم أو بيانات محذوفة

تحليل مجموعة البيانات غير المتسقة - أي أن السكان غير صحيح

ترك أصحاب العمليات في الظلام

غالبا ما يترك مالكو العمليات الذين يمتلكون أنشطة التحكم اليومية في الظلام عندما يتعلق الأمر بعناصر التحكم الخاصة بهم. تعتمد فرق التدقيق الداخلي على جداول البيانات والمجلدات المشتركة لإدارة عناصر التحكم الخاصة بها، لذلك غالبا ما تظل الوثائق على سطح مكتب فرق التدقيق الداخلي - بعيدا عن مالكي العمليات.

عندما تعمل وثائق التحكم مع التدقيق الداخلي، يحصل مالكو العمليات على رؤية لعناصر التحكم الخاصة بهم مرة واحدة فقط كل ثلاثة أشهر، وبالتالي ينشئون أنشطتهم اليومية الخاصة مدفوعة بنسختهم الخاصة من المهام، وليس بالضرورة في سياق عناصر التحكم الخاصة بهم.

ارتفاع التكاليف والموارد

بينما أثرت SOX بشكل إيجابي على التقارير المالية ، لا تزال هناك مخاوف بشأن التكلفة المتزايدة للامتثال ل SOX وأعباء الموارد الثقيلة. تستمر تكاليف SOX في الارتفاع على أساس سنوي للعديد من الشركات ، وفقا لمسح Sarbanes Oxley السنوي لشركة Protiviti. تشمل الأسباب إدخال أطر جديدة مثل COSO ومتطلبات المدقق الخارجي المتطورة للامتثال للقسم 404. تنفق الشركات اليوم ما معدله مليون إلى مليوني دولار وما يصل إلى 10000 ساعة على برامج SOX سنويا.

تبسيط امتثال SOX للتكنولوجيا المصممة لهذا الغرض

يكمن أحد مفاتيح تقليل الطبيعة المكلفة والمستهلكة للوقت لامتثال SOX وتعظيم موارد SOX في الاستفادة من التكنولوجيا المصممة لهذا الغرض لأتمتة العمليات. تستفيد فرق SOX ذات التفكير المستقبلي من أدوات أتمتة SOX لتقليل الساعات الإدارية والجهود المبذولة في SOX. يمكن برنامج الامتثال SOX الفرق من توفير الوقت لإجراء المزيد من عمليات تدقيق القيمة المضافة ، وزيادة جودة الضوابط الداخلية ، وتحسين الرؤية في الوقت الفعلي في بيئات SOX ، وتعزيز تعاون المدقق الخارجي - وفي النهاية تجنب إعادة البيانات المالية.

الأسئلة المتداولة حول امتثال SOX

ما هو قانون ساربينز أوكسلي (SOX) ولماذا تم سنه؟

قانون ساربينز أوكسلي ، المعروف باسم SOX ، هو قانون فيدرالي أمريكي تم سنه في عام 2002 لحماية المستثمرين من خلال تحسين دقة وموثوقية إفصاحات الشركات. تم تمريره استجابة لفضائح الشركات والمحاسبة الكبرى ، بما في ذلك تلك التي تورطت فيها إنرون وورلدكوم ، لاستعادة ثقة الجمهور في الأسواق المالية.

ما هي المتطلبات الرئيسية للامتثال ل SOX؟

يتطلب الامتثال ل SOX من الشركات تنفيذ ضوابط داخلية قوية على التقارير المالية والحفاظ عليها. وتشمل المتطلبات الرئيسية التصديق على البيانات المالية من قبل الرؤساء التنفيذيين والمديرين الماليين (القسم 302)، وإنشاء إطار للرقابة الداخلية (القسم 404)، واستقلال المدققين الخارجيين (القسم 301). يجب على الشركات أيضا إجراء عمليات تدقيق SOX منتظمة لضمان الامتثال لهذه المعايير.

كيف يمكن للشركة ضمان الامتثال الناجح ل SOX؟

لضمان الامتثال الناجح ل SOX ، يجب على الشركات إنشاء فريق امتثال SOX مخصص ، وتنفيذ ضوابط داخلية شاملة ، وإجراء تدريب منتظم للموظفين. يمكن أن يؤدي استخدام برامج إدارة التدقيق مثل Audit Board إلى تبسيط عمليات الامتثال عن طريق أتمتة سير العمل وتوفير تحليلات البيانات في الوقت الفعلي وإنشاء تقارير امتثال مفصلة. تعد عمليات التدقيق المنتظمة والمراقبة المستمرة ضرورية أيضا للحفاظ على الامتثال ومعالجة أي مشكلات على الفور.

نائب

بدأ Vice Vicente حياته المهنية في EY وقضى السنوات ال 10 الماضية في مجال الامتثال لتكنولوجيا المعلومات وإدارة المخاطر والأمن السيبراني. خدمت Vice أو راجعت أو استشارت لأكثر من 120 عميلا ، ونفذت برامج وتقنيات الأمان والامتثال ، ونفذت ارتباطات حول SOX 404 و SOC 1 و SOC 2 و PCI DSS و HIPAA ، وتوجيه الشركات من خلال الاستعداد للأمان والامتثال. تواصل مع نائب على لينكد إن.