المعايير الخاصة
Topical Requirement
بموضوع
الأمن السيبراني

The Institute of
Internal Auditors

المعايير الخاصة بموضوع الأمن السيبراني

تعد **المعايير الخاصة بمواضيع معينة** مكونا إلزاميا في الإطار الدولي للممارسات المهنية (International Professional Practices Framework®)، إلى جانب المعايير العالمية للتدقيق الداخلي (Global Internal Audit Standards™) والإرشادات العالمية. يجب استخدام **المعايير الخاصة بمواضيع معينة** بالاقتران مع المعايير العالمية للتدقيق الداخلي، والتي توفر الأساس الرسمي للممارسات المطلوبة.

توفر **المعايير الخاصة بمواضيع معينة** توقعات واضحة للمدققين الداخليين من خلال تحديد حد أدنى من خط الأساس لتدقيق موضوعات المخاطر المحددة. قد يتطلب ملف بيانات المخاطر في المؤسسة من المدققين الداخليين النظر في جوانب إضافية من الموضوع.

سيؤدي التوافق مع المعايير الخاصة بمواضيع معينة إلى زيادة الاتساق الذي يتم به تقديم خدمات التدقيق الداخلي وتحسين جودة وموثوقية خدمات التدقيق الداخلي ونتائجه. في النهاية، ترفع المعايير الخاصة بمواضيع معينة مهنة التدقيق الداخلي.

يجب على المدققين الداخليين تطبيق المعايير الخاصة بمواضيع معينة بما يتفق مع معايير التدقيق الداخلي العالمية. التوافق مع المعايير الخاصة بمواضيع معينة إلزامي لخدمات التأكيد ويوصى به للخدمات الاستشارية.

تنطبق المعايير الخاصة عندما يكون الموضوع واحدا مما يلي:

أ. موضوع مهمة محددة في خطة التدقيق الداخلي.

ب. موضوع تم تحديده أثناء أداء المهمة.

ت. موضوع تم طلبه لاحقا ولم يكن مدرجا في خطة التدقيق الداخلي الأصلية.

يجب توثيق وحفظ الأدلة على أن كل شرط في المعايير الخاصة بمواضيع معينة قد تم تقييمه من أجل قابلية التطبيق. قد لا تنطبق بعض المتطلبات الفردية في بعض المهام. ولكن، إذا تم استبعاد بعض المتطلبات، فيجب توثيق الأساس المنطقي لذلك والاحتفاظ به كدليل علما أن التوافق مع المعايير الخاصة بمواضيع معينة إلزامي وسيتم تقييمه أثناء تقييمات الجودة.

لمزيد من المعلومات، راجع " دليل استخدام المعايير الخاصة بموضوع للأمن السيبراني".

الأمن السيبراني

يعرف المعهد الوطني للمعايير والتكنولوجيا (NIST) الأمن السيبراني ببساطة بأنه "القدرة على حماية أو الدفاع عن استخدام الفضاء السيبراني من الهجمات الإلكترونية". الأمن السيبراني هو مجموعة فرعية من أمن المعلومات الشامل ، والذي يعرفه NIST على أنه "حماية المعلومات وأنظمة المعلومات من الوصول غير المصرح به أو الاستخدام أو الإفصاح أو التعطيل أو التعديل أو التدمير من أجل توفير السرية والنزاهة والتوافر".

يقلل الأمن السيبراني من المخاطر من خلال تعزيز بيئة التحكم الشاملة وحماية أصول معلومات المؤسسة من الوصول غير المصرح به أو التعطيل أو التغيير أو التدمير. يمكن أن تؤدي الهجمات الإلكترونية إلى تأثيرات مباشرة وغير مباشرة غالبا ما تكون كبيرة ، حيث تعد أجهزة الكمبيوتر والشبكات والبرامج والبيانات والمعلومات الحساسة مكونات مهمة لمعظم المؤسسات.

تقييم وتقدير حوكمة الأمن السيبراني وإدارة المخاطر وعمليات الرقابة

توفر **المعايير الخاصة بموضوع الأمن السيبراني** نهجا متسقا وشاملا لتقييم تصميم وتنفيذ حوكمة الأمن السيبراني وإدارة المخاطر وعمليات الرقابة. تمثل المتطلبات حدا أدنى من خط الأساس لتقييم الأمن السيبراني في المؤسسة.

الحوكمة: تقييم وتقدير حوكمة الأمن السيبراني

المتطلبات:

يجب على المدققين الداخليين تقييم ما يلي فيما يتعلق بحوكمة الأمن السيبراني للمؤسسة:

أ. وجود استراتيجية وأهداف رسمية للأمن السيبراني يتم تحديثها بشكل دوري. يتم إرسال التحديثات حول تحقيق أهداف الأمن السيبراني ومراجعتها بشكل دوري من قبل مجلس الإدارة ، بما في ذلك اعتبارات الموارد والميزانية لدعم استراتيجية الأمن السيبراني.

ب. وجود السياسات والإجراءات المتعلقة بالأمن السيبراني وتحديثها بشكل دوري لتعزيز بيئة الرقابة.

ت. يوجد تحديد للأدوار والمسؤوليات التي تدعم أهداف الأمن السيبراني ، وتوجد عملية لتقييم المعرفة والمهارات والقدرات بشكل دوري للأفراد الذين يشغلون الأدوار.

ث. إشراك أصحاب المصلحة المعنيين لمناقشة نقاط الضعف الحالية والتهديدات الناشئة في بيئة الأمن السيبراني والعمل بشأنها. والمصود بأصحاب المصلحة الإدارة العليا والعمليات وإدارة المخاطر والموارد البشرية والقانونية والامتثال والموردين وغيرهم.

إدارة المخاطر: تقييم وتقدير إدارة مخاطر الأمن السيبراني

المتطلبات:

يجب على المدققين الداخليين تقييم ما يلي فيما يتعلق بإدارة مخاطر الأمن السيبراني في المؤسسة:

أ. شمول عمليات تقييم المخاطر وإدارة المخاطر في المؤسسة لموضوع تحديد تهديدات الأمن السيبراني وتحليلها والتخفيف من حدتها ومراقبتها وتأثيرها على تحقيق الأهداف الاستراتيجية.

ب. يتم إجراء إدارة مخاطر الأمن السيبراني في جميع أنحاء المؤسسة وقد تشمل المجالات التالية: تكنولوجيا المعلومات ، وإدارة مخاطر المؤسسة ، والموارد البشرية ، والقانونية ، والامتثال ، والعمليات ، وسلسلة التوريد ، والمحاسبة ، والتمويل ، وغيرها.

ت. يتم تحديد المساءلة والمسؤولية عن إدارة مخاطر الأمن السيبراني. يتم تحديد فرد أو فريق لمراقبة كيفية إدارة مخاطر الأمن السيبراني والإبلاغ عنها بشكل دوري ، بما في ذلك الموارد المطلوبة للتخفيف من المخاطر وتحديد تهديدات الأمن السيبراني الناشئة.

ث. يتم إنشاء عملية لتصعيد أي مخاطر للأمن السيبراني بسرعة (ناشئة أو محددة مسبقا) تصل إلى مستوى غير مقبول وفقا لإرشادات إدارة المخاطر المعمول بها في المؤسسة أو المتطلبات القانونية والتنظيمية المعمول بها. يجب مراعاة الآثار المالية وغير المالية لمخاطر الأمن السيبراني.

ج. يتم إنشاء عملية لإيصال الوعي بمخاطر الأمن السيبراني إلى الإدارة والموظفين وللإدارة لمراجعة المشكلات أو الفجوات أو أوجه القصور أو إخفاقات التحكم بشكل دوري مع الإبلاغ والمعالجة في الوقت المناسب.

ح. نفذت المؤسسة عملية الاستجابة لحوادث الأمن السيبراني والتعافي منها والتي تشمل الكشف والاحتواء والاسترداد وتحليل ما بعد الحادث. يتم اختبار عملية الاستجابة للحوادث والتعافي بشكل دوري.

الضوابط: تقييم وتقييم عمليات التحكم في الأمن السيبراني

المتطلبات:

يجب على المدققين الداخليين تقييم ما يلي فيما يتعلق بعمليات الرقابة على الأمن السيبراني في المؤسسة:

أ. وجود عملية لضمان وجود كل من الضوابط الداخلية والضوابط المستندة إلى المورد لحماية سرية وسلامة وتوافر أنظمة وبيانات المؤسسة. يتم إجراء التقييمات بشكل دوري لتحديد ما إذا كانت الضوابط تعمل بطريقة تعزز تحقيق أهداف الأمن السيبراني التنظيمي والحل الفوري للمشكلات.

ب. وجود عملية لإدارة المواهب التي تشمل التدريب لتطوير الكفاءات الفنية المتعلقة بعمليات الأمن السيبراني والحفاظ عليها. تتم مراجعة العملية بشكل دوري.

ت. وجود عملية لمراقبة تهديدات ونقاط الضعف الناشئة في مجال الأمن السيبراني والإبلاغ عنها باستمرار وتحديد الفرص لتحسين عمليات الأمن السيبراني وتحديد أولوياتها وتنفيذها.

ث. يتم تضمين الأمن السيبراني في إدارة دورة الحياة (الاختيار والاستخدام والصيانة وإيقاف التشغيل) لجميع أصول تكنولوجيا المعلومات ، بما في ذلك الأجهزة والبرامج وخدمات البائعين.

ج. وجود عمليات لتعزيز الأمن السيبراني ، بما في ذلك التكوين وإدارة جهاز المستخدم النهائي والتشفير والتصحيح وإدارة وصول المستخدم ومراقبة التوافر والأداء. يتم تضمين اعتبارات الأمن السيبراني في تطوير البرامج (DevSecOps).

ح. وجود ضوابط متعلقة بالشبكة، مثل ضوابط الوصول إلى الشبكة والتجزئة؛ استخدام ووضع جدران الحماية ؛ اتصالات محدودة من وإلى الشبكات الخارجية؛ الشبكة الافتراضية الخاصة (VPN)/الوصول إلى شبكة الثقة المعدومة (ZTNA)؛ ضوابط شبكة إنترنت الأشياء (IoT) ؛ وأنظمة الكشف عن التسلل ومنعه (IDS و IPS).

خ. وجود عناصر ضبط أمان اتصالات نقطة النهاية لخدمات معينة مثل البريد الإلكتروني ومتصفحات الإنترنت ومؤتمرات الفيديو والمراسلة والوسائط الاجتماعية والسحابة وبروتوكولات مشاركة الملفات.

نبذة عن معهد المدققين الداخليين

معهد المدققين الداخليين (IIA) هو جمعية مهنية دولية تخدم أكثر من 255,000 عضو عالمي وقد منحت أكثر من 200,000 شهادة مدقق® داخلي معتمد (CIA®) في جميع أنحاء العالم. تأسس معهد المدققين الداخليين في عام 1941 ، وهو معترف به في جميع أنحاء العالم كرائد في مهنة التدقيق الداخلي وفي المعايير والشهادات والتعليم والبحث والتوجيه الفني. لمزيد من المعلومات ، قم بزيارة www.theiia.org.

حقوق النشر

The Institute of Internal Auditors

Greenwood Blvd 1035
جناح 401
ليك ماري ، فلوريدا 32746
الولايات المتحدة الأمريكية
هاتف: +1-407-937-1111