المعايير الخاصة بموضوع الأمن السيبراني

ما هي المعايير الخاصة بمواضيع معينة ؟

تعد **المعايير الخاصة بمواضيع معينة** عنصرًا أساسيًا في الإطار الدولي للممارسات المهنية ®، والذي يتضمن أيضًا المعايير العالمية للتدقيق الداخلي ™ وملاحق الإرشادات العالمية. يتطلب المعهد الدولي للمدققين الداخليين، باعتباره واضع المعايير لمهنة التدقيق الداخلي، هذه **المعايير الخاصة** الإلزامية كمكمل للمعايير العالمية للتدقيق الداخلي، والتي تعمل بمثابة المرجع للممارسات المطلوبة الموضحة والمشار إليها في **المعايير الخاصة** للمواضيع المعينة.

توفر **المعايير الخاصة بمواضيع معينة** هيكلًا للموضوعات العالمية التي يتم تدقيقها بشكل متكرر والتي عادة ما تكون ذات مخاطر أعلى ومنتشرة بطبيعتها. في حين أن المعايير تنطبق على جميع خدمات التدقيق الداخلي المقدمة، إلا أن المعايير الخاصة بمواضيع معينة يجب اعتبارها متطلبات إلزامية إضافية يجب اتباعها عندما يكون هذا الموضوع هو محور مهمة التدقيق الداخلي.

يجب تطبيق المعايير الخاصة بمواضيع معينة على مستوى الكيان أو المؤسسة لمواضيع لها تأثير على جميع أنحاء المؤسسة. يجب أن يكون المدققون الداخليون على دراية بالمعايير الخاصة بمواضيع معينة وأن يكونوا مستعدين لتطبيقها عندما يتم إدراج الموضوع في خطط التدقيق السنوية الخاصة بهم أو إذا كان هذا الموضوع المحدد هو محور مهمة التدقيق الداخلي. يجب تقييم عناصر المعايير الخاصة بمواضيع معينة عند تحديد نطاق المهمة. يجب توثيق الأدلة على حدوث التقييم ومعالجة الموضوع والاحتفاظ بها. يجب أن تقوم المهام التي تتضمن أي جانب من جوانب الموضوع بتقييم المتطلبات ذات الصلة بالمهمة أو توثيق سبب عدم تطبيق متطلبات محددة. تتوفر أداة لمساعدة المدققين الداخليين في شرح الأساس المنطقي لإدراج أو استبعاد المتطلبات في الملحق ب.

لماذا تعتبر المعايير الخاصة بمواضيع معينة ضرورية؟

صممت المعايير الخاصة بمواضيع معينة لتعزيز الأهمية المستمرة لوظيفة التدقيق الداخلي في مشهد المخاطر العالمية المتطور وتعزيز قيمة خدمات التدقيق الداخلي عبر الصناعات والقطاعات. إن التوافق مع المعايير الخاصة بمواضيع معينة سيساعد المدققين الداخليين على رفع جودة واتساق المهام.

تم تصميم المعايير الخاصة بمواضيع معينة لتوفير التوجيه لأداء خدمات التدقيق الداخلي في ثلاث مجالات: الحوكمة، وإدارة المخاطر، وعمليات الرقابة. يتضمن كل مجال:

- المتطلبات، وهي إلزامية وتغطي الأهداف التنظيمية الأساسية.
- الاعتبارات، وهي ليست إلزامية، ولكنها بمثابة أفضل الممارسات لتقييم تصميم وتنفيذ الأهداف التنظيمية. يجب استخدام الاعتبارات الواردة في الملحق (أ) ببساطة كأمثلة للتحقق من صحة المتطلبات.

سيتم تقييم التوافق مع المعايير الخاصة بمواضيع معينة في تقييمات الجودة. ومن أجل إثبات المطابقة أثناء التحضير لمراجعة الجودة، يجب على المدققين الداخليين استخدام الأدوات المتوفرة في الملحق ب للإشارة إلى المطابقة مع المتطلبات أو لشرح سبب عدم تحقيق المطابقة.

المعايير الخاصة بموضوع الأمن السيبراني

تقدير وتقييم فعالية حوكمة الأمن السيبراني وإدارة المخاطر وعمليات الرقابة

يحمي الأمن السيبراني أصول المعلومات الخاصة بالمؤسسة من المستخدمين غير المصرح لهم، أو من التعطيل، أو التغيير، أو التدمير، ويعزز بيئة الضوابط الرقابية الشاملة لتقليل المخاطر. يمكن أن تؤدي الهجمات الإلكترونية إلى تأثيرات مباشرة وغير مباشرة غالبًا ما تكون كبيرة، حيث تعد أجهزة الحاسوب والشبكات والبرامج والبيانات والمعلومات الحساسة مكونات مهمة لمعظم المؤسسات. نظرًا لأن المؤسسات تعتمد بشكل كبير على موارد تكنولوجيا المعلومات، فإن تحديد خطة الأمن السيبراني والأهداف والمخاطر الكامنة والضوابط الفعالة بشكل واضح يجب أن يكون أولوية للإدارة.

يوفر هذا المعيار التكميلي نهجًا متسقًا وشاملاً لتقييم تصميم وتنفيذ حوكمة الأمن السيبراني وإدارة المخاطر وعمليات التحكم.

الحوكمة: تقييم وتقدير حوكمة الأمن السيبراني

المتطلبات:

عند تنفيذ مهمة تدقيق داخلي يتضمن نطاقها أهداف تتعلق بالأمن السيبراني، يجب على المدققين الداخليين تقييم ما إذا كانت عمليات حوكمة المؤسسة تعالج الأمن السيبراني بشكل مناسب. يجب على المدققين الداخليين تقييم ما إذا كان:

A. يتم وضع السياسات والإجراءات المتعلقة بعمليات إدارة مخاطر الأمن السيبراني وتحديثها دوريًا، بما في ذلك تعزيز الممارسات التي تعزز بيئة الرقابة بناءً على أطر العمل المعتمدة على نطاق واسع (NIST, COBIT, وغيرها)
B. الأدوار والمسؤوليات التي تدعم أهداف الأمن السيبراني للمنظمة محددة بوضوح ويتم شغل هذه الأدوار من قبل أفراد يتمتعون بالمعرفة والمهارات والقدرات المطلوبة.
C. يتم إرسال تحديثات لأهداف واستراتيجيات ومخاطر الأمن السيبراني وضوابط تقليل المخاطر إلى مجلس الإدارة بشكل دوري.
D. يشارك أصحاب المصلحة المعنيون (على سبيل المثال، القيادة والعمليات والموردين الاستراتيجيين وغيرهم) في مناقشة أفضل السبل لإنشاء وتحسين عمليات إدارة مخاطر الأمن السيبراني.
E. يتم إبلاغ مجلس الإدارة بالموارد المطلوبة (مثل القيادة والتمويل والموهبة والأجهزة والبرمجيات والتدريب) اللازمة لتنفيذ عمليات إدارة مخاطر الأمن السيبراني بشكل فعال.

إدارة المخاطر: تقييم وتقدير إدارة مخاطر الأمن السيبراني

المتطلبات:

عند تنفيذ مهمة تدقيق داخلي يتضمن نطاقها أهداف تتعلق بالأمن السيبراني، يجب على المدققين الداخليين تقييم ما إذا كانت عمليات إدارة المخاطر في المؤسسة تعالج الأمن السيبراني بشكل مناسب. يجب على المدققين الداخليين تقييم ما إذا كان:

A. تم إنشاء عملية لإدارة المخاطر على مستوى المؤسسة لتتضمن تحديد وتحليل وإدارة المخاطر المتعلقة بتكنولوجيا المعلومات والأمن، مع التركيز بشكل خاص على مخاطر الأمن السيبراني وكيف يمكن أن تؤثر تلك المخاطر على القدرة على تحقيق أهداف المنظمة.
B. يتم إجراء عمليات إدارة مخاطر الأمن السيبراني من قبل فريق متعدد الوظائف يتضمن قيادة تكنولوجيا المعلومات، وإدارة المخاطر على مستوى المؤسسة، والشؤون القانونية، والامتثال، والإدارة الأخرى (العمليات، والمحاسبة، والتمويل، وغيرها) وإشراك الأطراف الخارجية (البائعين، ومقدمي الخدمات الخارجية والموردين والعملاء وغيرهم) حسب الاقتضاء.

C. تم وضع سياسات وإجراءات إدارة مخاطر الأمن السيبراني ويتم تحديثها دوريًا، بما في ذلك تعزيز الممارسات التي تعزز عمليات إدارة مخاطر الأمن السيبراني بناءً على أطر إدارة المخاطر المعتمدة على نطاق واسع، أو التوجيهات الرسمية، أو أفضل الممارسات الأخرى.

D. يتم تحديد المساءلة والمسؤولية فيما يتعلق بإدارة مخاطر الأمن السيبراني وتحديد فرد أو فريق يقوم بشكل دوري بمراقبة وإبلاغ كيفية إدارة مخاطر الأمن السيبراني، بما في ذلك متطلبات الموارد للتخفيف من المخاطر وتحديد مخاطر الأمن السيبراني الناشئة التي لم يتم التعرف عليها من قبل.

E. يتم إنشاء عملية للتصعيد السريع لأي مخاطر تتعلق بالأمن السيبراني (الناشئة أو التي تم تحديدها مسبقًا) والتي ترتفع إلى مستويات غير مقبولة بناءً على إرشادات إدارة المخاطر المعمول بها في المؤسسة أو للامتثال للمتطلبات القانونية و/أو التنظيمية المعمول بها.

F. تتضمن إدارة مخاطر الأمن السيبراني التنسيق بين إدارة أمن المعلومات والإدارة القانونية وإدارة الامتثال وغيرها لتحديد جميع الالتزامات القانونية والتعاقدية والامتثال لها، مثل القوانين والانظمة. يتم الإبلاغ عن حالة الامتثال وعدم الامتثال للمتطلبات المعمول بها داخل المؤسسة بشكل دوري.

G. يتم إنشاء عملية لتحديد وإدارة مخاطر الأمن السيبراني المتعلقة بأطراف ثالثة. يُطلب من البائعين والموردين وغيرهم من مقدمي العمليات و/أو الخدمات الخارجية تنفيذ ضوابط فعالة للأمن السيبراني تحمي بشكل مناسب سرية وسلامة وتوافر أنظمة وبيانات المؤسسة التي يمكن لأطراف ثالثة الوصول إليها.

H. يتم تصميم السياسات والعمليات المتعلقة بتصنيف البيانات والاحتفاظ بها وتدميرها وتشفيرها بشكل مناسب ونشرها بشكل فعال لتوفير نهج منظم يضمن التسجيل الكامل والدقيق للبيانات ويحمي سرية وخصوصية المعلومات الحساسة.

I. يتم إنشاء عملية للإبلاغ عن المخاطر التشغيلية للأمن السيبراني لضمان نشر الوعي عند الإدارة والموظفين. يتم إبلاغ مجلس الإدارة والإدارة بأي مشكلة، أو ثغرات أو أوجه قصور أو فشل في التحكم، ويتم مراقبة حالة الإصلاح والإبلاغ عنها عن كثب. يتم تحديد حالات عدم الامتثال لسياسات الأمن السيبراني والتحقيق فيها والإبلاغ عنها ومعالجتها في الوقت المناسب.

عمليات الرقابة: تقييم وتقدير عمليات الضبط في الأمن السيبراني

المتطلبات:

عند تنفيذ مهمة تدقيق داخلي يتضمن نطاقها أهداف تتعلق بالأمن السيبراني، يجب على المدققين الداخليين تقييم ما إذا كانت عمليات الرقابة في المؤسسة تعالج الأمن السيبراني بشكل مناسب. يجب على المدققين الداخليين تقييم ما إذا كانت المؤسسة:

A. تعطي الأولوية لضوابط الأمن السيبراني والتأكد من تخصيص الميزانية والموارد ذات الصلة (مثل الموظفين والبرامج والأدوات وغيرها) لتحقيق أقصى قدر من الفوائد المتوقعة.

B. التأكد من أن ضوابط الأمن السيبراني تعمل بطريقة تعزز تحقيق أهداف الأمن السيبراني التنظيمي وحل المشاكل في الوقت المناسب.

C. توفر التدريب الكافي للموظفين المسؤولين عن عمليات الأمن السيبراني.

D. تضع سياسات وإجراءات كافية لإدارة كافة جوانب عمليات الأمن السيبراني والضوابط المرتبطة بها.

E. تضمن أن الإدارة لديها الموارد اللازمة للبقاء على اطلاع بقضايا الأمن السيبراني الناشئة من التقنيات الجديدة، وتحديد الفرص لتحسين العمليات، وفهم أفضل السبل لنشر جهود الأمن السيبراني للتأثير على الأهداف والغايات التنظيمية الواسعة.

F. دمجت الأمن السيبراني بشكل مناسب في دورة حياة تطوير النظام لتطبيقات الأعمال، بما في ذلك البرامج والتطبيقات المشتراة أو المطورة داخليا .

G. أدرجت الأمن السيبراني في إدارة الأجهزة (مثل أجهزة الكمبيوتر المحمولة وأجهزة الكمبيوتر المكتبية والأجهزة المحمولة).

H. قامت بتنفيذ ضوابط فعالة فيما يتعلق بدعم أجهزة الإنتاج، مثل التكوين والتصحيح ودعم إدارة وصول المستخدم ومراقبة التوفر والأداء. قامت المؤسسة بتقييم مدى كفاية التصميم والفعالية التشغيلية لهذه الضوابط.

I. تحسن الضوابط المتعلقة بالشبكة فيما يتعلق بتجزئة الشبكة، واستخدام جدران الحماية ووضعها، والاتصالات المحدودة بالشبكات و/أو الأنظمة الخارجية، واستخدام التقنيات الوقائية والكشفية مثل أنظمة كشف/منع التسلل.

J. قامت بتنفيذ ضوابط فعالة تحيط بخدمات الاتصالات الشائعة مثل البريد الإلكتروني ومتصفحات الإنترنت وتلك المستخدمة للاجتماعات بواسطة الفيديو والمراسلة وبروتوكولات مشاركة الملفات.

K. نفذت ضوابط مناسبة لتقديم الخدمات لضمان تكامل المجالات التالية مع مراقبة الأمن السيبراني: إدارة التغيير، ومكتب الخدمة/المساعدة، وإدارة جهاز المستخدم النهائي.

L. قامت بتنفيذ ضوابط الأمان المادي المناسبة لحماية مراكز المعلومات عالية المخاطر (مثل مراكز البيانات ومراكز عمليات الشبكة ومراكز العمليات الأمنية) من الهجمات.

M. قامت بتنفيذ ضوابط الاستجابة للحوادث والاسترداد.

المعايير ذات الصلة:

3.1 الكفاءة
4.2 العناية المهنية اللازمة
9.1 فهم عمليات الحوكمة وإدارة المخاطر والرقابة
9.4 خطة التدقيق الداخلي
12.3 الاشراف على اداء المهمة وتحسينها
13.1 اتصالات المهمة
13.2 تقييم مخاطر المهمة
13.3 أهداف المهمة ونطاقها
13.4 معيار التقييم
13.5 موارد المهمة
13.6 برنامج العمل
14.1 جمع المعلومات لأغراض التحليل والتقييم
14.2 التحليلات ونتائج المهمة المحتملة
14.3 تقييم النتائج
14.4 التوصيات وخطط العمل
14.5 استنتاجات المهمة
14.6 توثيق المهمة
15.1 إبلاغ المهمة النهائي
15.2 تأكيد تنفيذ التوصيات وخطط العمل

أدلة تدقيق التكنولوجيا العالمية ذات الصلة:(GTAGs)

تقييم مخاطر الأمن السيبراني: نموذج الخطوط الثلاثة
تدقيق تطبيقات الأعمال
تدقيق الاستجابة للحوادث السيبرانية والتعافي منها
تدقيق عمليات الأمن السيبراني: الوقاية والكشف
تدقيق الهوية وإدارة الوصول
تدقيق حوكمة تكنولوجيا المعلومات
تدقيق الحوسبة المتنقلة
تدقيق إدارة الشبكات والاتصالات

الملحق أ. الاعتبارات

اعتبارات لكل من متطلبات الحوكمة:

لتقييم كيفية تطبيق عمليات الحوكمة الأساسية على أهداف الأمن السيبراني، يمكن للمدققين الداخليين مراجعة ما يلي:

A. السياسات والإجراءات والوثائق الأخرى ذات الصلة التي تستخدمها المؤسسة لإدارة مسؤوليات الأمن السيبراني اليومية، بما في ذلك:
   1. التوثيق الواضح والموجز والمتسق والمحدث بشكل دوري، ومن الأفضل أن يتم تحديد مخاطر الأمن السيبراني الناشئة بشكل سنوي على الأقل.
   2. الإجراءات المتعلقة بتحديد وتحليل وحل والإبلاغ عن الانتهاكات أو غيرها من فقدان البيانات الحساسة.
   3. توثيق كيفية ضمان الإدارة أن السياسات والإجراءات كافية لدعم عمليات الأمن السيبراني.

B. الأدوار والمسؤوليات التي أنشأها مجلس الإدارة لدعم تحقيق استراتيجية الأمن السيبراني، بما في ذلك هيكل إعداد التقارير الذي يضمن رفع تقارير الأمن السيبراني إلى مستوى في المؤسسة يتمتع برؤية كافية لتحقيق الدعم التنظيمي.

C. المواد المقدمة إلى مجلس الإدارة حول استراتيجية الأمن السيبراني وأهدافه ومخاطره وضوابطه، بما في ذلك تحليل ما إذا كان:
   1. وتيرة الاتصالات كافية، ومن الأفضل أن يتم ذلك كل ثلاثة أشهر ويقدمها رئيس وظيفة أمن المعلومات، مثل كبير مسؤولي نظم المعلومات.
   2. أن تكون المعلومات المقدمة واضحة وموجزة ومتسقة؛ يتم الإبلاغ عن المخاطر والضوابط بطريقة يسهل على مجلس الإدارة فهمها.
   3. يتم تضمين مؤشرات الأداء الرئيسية أو مقاييس/إحصاءات الأمن السيبراني الهامة الأخرى.
   4. حيثما كان ذلك مناسبًا، يتم تلقي ملاحظات مجلس الإدارة من قبل الإدارة وتنفيذها، مع إرسال تحديثات حالة التغييرات إلى مجلس الإدارة.

D. أدلة على اتصالات الإدارة المتعلقة بالأمن السيبراني مع أصحاب المصلحة المعنيين (على سبيل المثال، القيادة والعمليات والموردين الاستراتيجيين وغيرهم)، بما في ذلك أن المعلومات المرسلة واضحة وموجزة ومتسقة ومصممة خصيصًا لجمهور أصحاب المصلحة:
   1. الموظفون.
   2. البائعون، الموردون، مقدمو الخدمات الخارجيون، والأطراف الثالثة.
   3. العملاء.
   4. الشركاء الاستراتيجيون.

E. تحليل وإيصال متطلبات الموارد من قبل الإدارة، بما في ذلك:
   1. فهم كيفية تحديد الفجوات وما هي المقاييس الرئيسية المستخدمة لتوقع التغييرات في المتطلبات.
   2. كيف تعمل الإدارة مع الموارد البشرية لتحليل احتياجات المواهب في مجال الأمن السيبراني.
   3. كيف تقوم الإدارة بتحليل مخزون الأجهزة والبرامج الحالي وتحديد ما إذا كانت هناك حاجة إلى استثمارات إضافية لدعم مبادرات الأمن السيبراني.
   4. ما إذا كان المدققون الداخليون يقومون بمراجعة كيفية إنشاء الإدارة وتحديث مواد التدريب على الأمن السيبراني وتحديد الثغرات، بما في ذلك التأكد من أن التدريب يغطي أهداف الأمن السيبراني الناشئة والمخاطر والضوابط.

اعتبارات لكل من متطلبات إدارة المخاطر:

لتقييم الجوانب المطلوبة لإدارة مخاطر الأمن السيبراني، يمكن للمدققين الداخليين مراجعة ما يلي:

A. كيفية تحديد الإدارة في البداية لمخاطر الأمن السيبراني، بما في ذلك:
   1. فهم الموظفين المسؤولين عن التهديدات اليومية التي تواجهها المؤسسة والمخاطر الناشئة في مجتمع أمن المعلومات.
      a. تحديد ما إذا كان هؤلاء الأفراد لديهم الخبرة المهنية ذات الصلة والتدريب اللازم للتعرف بشكل فعال على التهديدات وتصعيدها لفريق إدارة المخاطر الأوسع.
   2. تحديد التطبيقات البرمجية أو الموردين الذين تعتمد عليهم الإدارة لتحديد مخاطر الأمن السيبراني.
   3. الوثائق المتعلقة بعملية إدارة مخاطر الأمن السيبراني، بما في ذلك:
      a. محاضر الاجتماعات.
      b. خطوات العمل.
      c. قوائم الحضور أو أعضاء الفريق.
      d. التحقيق في ما بعد الحادث / تحليل السبب الجذري.

B. كيف تقوم الإدارة بتحديد أو ترشيح أعضاء فريق إدارة المخاطر ومبررات العمل أو المؤهلات ذات الصلة المستخدمة لتقييم العضوية. مراجعة الأدلة على المشاركة الدورية في مناقشات مخاطر الأمن السيبراني مع الأطراف الخارجية ذات الصلة.

C. العملية التي تستخدمها المؤسسة لإنشاء وتحديث السياسات والإجراءات بشكل دوري المتعلقة بإدارة مخاطر الأمن السيبراني، والتي قد تشمل:
   1. المراجعة السنوية والموافقة على السياسات والإجراءات.
   2. فهم كيفية ضمان المؤسسة للامتثال لسياسات وإجراءات إدارة المخاطر وطريقة تدريب الموظفين على تنفيذ السياسات والإجراءات.
      a. فهم الأطر المتبعة أو توجيهات الجهات الرسمية التي تستخدمها الإدارة للتعامل مع مخاطر الأمن السيبراني (NIST, COBIT, وغيرها) والطريقة التي تؤكد بها المؤسسة الالتزام بالإطار (الإطارات) المختارة.

D. الفرد (الأفراد) المسؤول عن تنفيذ إدارة مخاطر الأمن السيبراني، بما في ذلك التأكد من أن خلفيتهم المهنية وخبراتهم ومؤهلاتهم وبيانات اعتمادهم مناسبة لإدارة مخاطر وتهديدات أمن المعلومات. التحقق من أن الفرد المسؤول يتم وضعه على مستوى داخل المؤسسة لتسليط الضوء على مخاطر الأمن السيبراني وإبلاغ تلك المخاطر بشكل فعال.

E. عمليات التصعيد التي تستخدمها المؤسسة للإبلاغ عن مخاطر الأمن السيبراني، بما في ذلك كيفية تقييم مستوى التهديد أو الخطر وتعيينه وترتيب أولوياته. التحقق من أن المؤسسة قد حددت مستويات المخاطر، مثل عالية، متوسطة، منخفضة، بما في ذلك شرح تفصيلي لكل مستوى خطر وإجراءات التصعيد لكل فئة من فئات المخاطر. قم بمراجعة قائمة مخاطر الأمن السيبراني الحالية التي تم تحديدها وحالة التخفيف لكل حدث.

F. العملية التي تستخدمها المؤسسة لضمان التوافق مع جميع لوائح الأمن السيبراني المعمول بها، بما في ذلك:
   1. مدى تأثير اللوائح المقترحة أو المعتمدة مؤخرًا على المؤسسة.
   2. إذا كان هناك جرد للأنظمة المعمول بها والتي يتم مراقبتها وتحديثها والإبلاغ عنها بشكل دوري لضمان الوعي التنظيمي.
      a. بالنسبة لأي بنود عدم امتثال، التحقق من أن الإدارة على دراية بالمخاطر المرتبطة بها، بما في ذلك من خلال التقارير الدورية.

G. عملية المؤسسة لإدارة مخاطر الأمن السيبراني الخارجية. التأكد من مراجعة ضوابط الأمن السيبراني للبائعين قبل بدء علاقة العمل وأن العقود تضمن الحق في إجراء مراجعات دورية طوال العلاقة. تضمين الحصول على تقرير ضوابط مؤسسة الخدمة الخاصة بالطرف الثالث وتحليله والتحقق من قيام المؤسسة بتوثيق مراجعة تقرير SOC الخاص بها، والذي يجب أن يتضمن ضمان تنفيذ اعتبارات التحكم في المستخدم. اكتساب فهم لنهج الإدارة لتحديد ما إذا كانت الأطراف الثالثة لديها بيئة رقابية مناسبة تتناسب مع ضوابط المؤسسة.

a. إذا تم العثور على نقاط ضعف في الضوابط الرقابية لدى الطرف الثالث، فيجب فهم كيفية استخدام إدارة العملية للتأكد من أن نقاط الضعف لا تعرض الأمن السيبراني المتعلق بالعمليات للخطر، أو فهم كيفية إبلاغ المؤسسة بأن التغييرات مطلوبة للحفاظ على العلاقة المعمول بها مع المورد أو من المحتمل أن يكون موردا" بديلاً ينبغي العثور عليها.

H. السياسات والعمليات التي وضعتها المؤسسة تتعلق بما يلي:

1. تصنيف البيانات.
2. الاحتفاظ بالبيانات.
3. تدمير البيانات.
4. التشفير.
5. إدارة الوصول/التأكد من الهوية.
6. من يقوم بإعداد الوثائق ومراجعتها وتحديثها، والتي ينبغي أن تشمل بشكل مثالي الموظفين القانونيين وموظفي الامتثال لضمان التوافق مع اللوائح المعمول بها.
7. كيفية قيام المؤسسة بتصنيف البيانات لضمان تحديد البيانات السرية والخاصة والحصول على المستوى المناسب من الحماية، مثل تقييد وصول المستخدم.
8. كيف تقوم المؤسسة بشكل دوري بمراجعة العملية المستخدمة لتصنيف البيانات وما إذا كانت العملية مستمرة في دعم أهداف الأمن السيبراني التنظيمي والامتثال للسياسات التنظيمية واللوائح المعمول بها.

I. عملية إبلاغ المخاطر التشغيلية للأمن السيبراني إلى الإدارة والموظفين. ومن الناحية المثالية، ينبغي تضمين هذا التواصل مع التدريب الدوري على الأمن السيبراني (سنويًا على الأقل). فهم عملية الإدارة لتوصيل التحديثات بشأن المعالجة الحالية لمشكلات الأمن السيبراني إلى جانب تواريخ الانتهاء المتوقعة. التحقق من مراقبة عدم الامتثال عن كثب، وتقديم التحديثات إلى مجلس الإدارة والإدارة العليا.

اعتبارات لكل من متطلبات عملية الرقابة:

لتقييم الجوانب المطلوبة للرقابة على الأمن السيبراني، يمكن للمدققين الداخليين مراجعة ما يلي:

A. عملية الإدارة لتحديد كيفية نشر الموارد المدرجة في الميزانية لدعم بيئة مراقبة الأمن السيبراني، والتي ينبغي أن تشمل التخطيط الاستراتيجي سنويًا لضمان توفر مستوى مناسب من الموارد التنظيمية لتحقيق أهداف الأمن السيبراني. وينبغي مراجعة النتائج الرسمية والموثقة للتخطيط السنوي والرصد الدوري لإدارة الموارد.

B. عملية الإدارة للتقييم الدوري لضوابط الأمن السيبراني تعمل بطريقة تعزز تحقيق أهداف الأمن السيبراني التنظيمية. التحقق من أن الإدارة تراقب فعالية الرقابة وتقييم ما إذا كانت الضوابط الحالية مصممة بشكل مناسب أو أن هناك حاجة إلى ضوابط جديدة. في العديد من المؤسسات، تلعب وظيفة التدقيق الداخلي دورًا مهمًا في هذه العملية من خلال توفير ضمانات بشأن تصميم الضوابط وما إذا كانت الضوابط تعمل بفعالية من خلال الاختبارات الدورية (ربع السنوية، السنوية). التحقق من عمليات الإدارة لمعالجة أوجه القصور في الرقابة أو معالجة نتائج التقييمات التي تجريها وظيفة التدقيق الداخلي أو مقدمو خدمات الضمان الآخرون (على سبيل المثال، اختبار الاختراق).

C. عملية الإدارة لتقييم الاحتياجات التدريبية لموظفي الأمن السيبراني داخل المؤسسة وكيفية تخصيص الموارد لتقديم التعليم المناسب والتأكد من فهم تهديدات الأمن السيبراني الناشئة وإدارتها. فهم كيف تضمن الإدارة حصول الموظفين على تدريب كافٍ في مجال الأمن السيبراني، والذي قد يشمل أحداث تدريب حية، أو تعليمات مسجلة، أو إكمال وحدات التدريب.

D. عملية المؤسسة لإنشاء وتحديث سياسات وإجراءات الأمن السيبراني وكيفية تقييم الإدارة ما إذا كانت السياسات والإجراءات المذكورة كافية. فهم كيفية تدريب الموظفين المسؤولين عن عمليات وضوابط الأمن السيبراني على الامتثال للسياسات والإجراءات وكيفية تقييمهم للامتثال الداخلي.

E. عملية المؤسسة لتدريب فريق الإدارة المسؤول عن عمليات وضوابط الأمن السيبراني بشكل مناسب للتعرف على الاتجاهات الناشئة وتزويد فرقهم والمؤسسة بالقيادة الإستراتيجية. فهم كيفية تحديد المؤسسة للفرص المتاحة لزيادة قدرات الإدارة لدعم الوعي بالقضايا الناشئة، مثل المشاركة في التدريب والتعليم المهني المستمر.

F. كيفية تعامل المؤسسة مع الأمن السيبراني ضمن دورة تطوير النظم المعلوماتية، بما في ذلك جوانب التحكم التالية:

1. التخطيط: تم تحديد الأمن السيبراني كعنصر رئيسي عند تقييم المخاطر وتحليل نقاط الضعف المحتملة. ينبغي تضمين نطاق وأهداف تنفيذ البرنامج أثناء قيام المؤسسة بتقييم ضوابط الأمن السيبراني أثناء مرحلة التخطيط.
2. جمع المتطلبات: تعد متطلبات الأمن السيبراني عنصرًا عند تحديد المتطلبات الوظيفية، والتي يجب أن تتضمن أيضًا الامتثال لجميع المتطلبات القانونية والتنظيمية المعمول بها .
3. التصميم: يتم تضمين اعتبارات الأمن السيبراني كجزء لا يتجزأ من متطلبات المعالجة التفصيلية. يجب تحديد الضوابط في جميع جوانب التصميم حيث تحدد المؤسسة بشكل رسمي احتياجات تصميم بنية النظام (مثل الأنظمة الأساسية وواجهات المستخدم وقواعد البيانات وغيرها).
4. التطوير: أنشأت المؤسسة بيئة آمنة وحددت رسميًا عملية تطوير تقلل من نقاط الضعف السيبراني (على سبيل المثال، وصول المستخدم المحدود إلى كود التطوير، والفصل المناسب عن بيئة الإنتاج، واستخدام الأدوات المعتمدة، ووجود مسارات تدقيق لتتبع أنشطة التطوير، ومتطلبات الأمن السيبراني المحددة للبرامج التي يطورها المورد، وغيرها).
5. الاختبار: مراجعة وتقييم الأمن السيبراني خلال مرحلة الاختبار (على سبيل المثال، الاختبار الآلي، واختبار الاختراق، وتقييم الثغرات الأمنية). يجب أن تكون المؤسسة قادرة على التنبيه سريعًا ومعالجة أي ثغرات إلكترونية تم تحديدها من خلال الاختبار، والذي يتضمن وصفًا تفصيليًا للثغرة الأمنية وتغييرات التعليمات البرمجية أو ضوابط التخفيف التي تم وضعها استجابةً لذلك.
6. النشر: مع نقل البرامج الجديدة إلى مرحلة الإنتاج، يجب على المؤسسة أن تراقب بعناية تهديدات الأمن السيبراني المحتملة، بما في ذلك ضمان تدريب المستخدمين النهائيين على استخدام البرنامج بطريقة تقلل من مخاطر الأمن السيبراني. يجب على المؤسسة التأكد من تسجيل الأحداث والأخطاء وتحليلها فيما يتعلق بأحداث الأمن السيبراني المحتملة.
7. الصيانة: يجب على المؤسسة التأكد من تطبيق جميع إصدارات البرامج المتعلقة بالأمان في الوقت المناسب ويجب أن يكون لديها اتصال مفتوح مع بائعي البرامج لضمان التحكم بشكل صحيح في المخاطر والتهديدات الناشئة وإبلاغ المستخدمين النهائيين بأي نقاط ضعف معروفة.

G. الضوابط التي أنشأتها المؤسسة لحماية الأجهزة (مثل أجهزة الكمبيوتر المكتبية وأجهزة الكمبيوتر المحمولة والأجهزة المحمولة وغيرها) من مخاطر الأمن السيبراني، والتي تشمل استخدام التشفير أو برامج مكافحة الفيروسات أو متطلبات كلمات المرور المعقدة أو الشبكة الخاصة الافتراضية أو شبكات الثقة المعدومة للمصادقة والتحديث الدوري للبرامج الثابتة، وعملية إدارة الأصول التي تضمن أن الأجهزة الصادرة عن الشركة تتمتع بتكوين أمان مناسب عند الإصدار والحذف المناسب عند إيقاف الأصول.

H. الضوابط التي نشرتها المؤسسة لضمان أن دعم الإنتاج يوفر الحماية من مخاطر الأمن السيبراني، والتي يجب أن تتضمن تصحيح الخوادم بالإصدارات الأمنية في الوقت المناسب للتخفيف من المخاطر الناشئة. القيام بمراجعة ضوابط المراقبة المعمول بها لتحديد ما إذا كان التوافر واستخدام الموارد يعملان بشكل مناسب، مما يسمح بمراجعة وتحليل مشكلات الأمن السيبراني المحتملة التي تهدد الأداء. مراجعة الضوابط المتعلقة بقاعدة البيانات والتي تشمل الحد من وصول المستخدم والمسؤول، وضمان استخدام التشفير، والنسخ الاحتياطي واختبار قواعد البيانات، ووجود ضوابط قوية لأمن الشبكة.

I. الضوابط المتعلقة بالشبكة والتي تنص على التجزئة للحد من مخاطر الأمن السيبراني الناتجة عن الوصول غير المصرح به. القيام بمراجعة كيفية استخدام المؤسسة لجدران الحماية، بما في ذلك مكان وجود جدران الحماية والعملية المستخدمة لمراجعة الوصول إلى الشبكة وتحليله وتقييده، ومنع الوصول غير المصرح به. مراجعة كيفية استخدام المؤسسة لأنظمة كشف/منع التطفل لمنع هجمات الأمن السيبراني واكتشافها والتعافي منها.

J. الضوابط التي أنشأتها المؤسسة لخدمات الاتصالات الشائعة ، مثل استخدام تشفير البريد الإلكتروني، وضمان تطبيق تحديثات أمان متصفح الإنترنت في الوقت المناسب، وإعدادات أمان تطبيقات الاجتماعات بالفيديو/المراسلة (على سبيل المثال، MS Teams ، Zoomوغيرها) إعدادات الأمان المبرمجة لمنع أو ضبط استخدام بعض الملفات التطبيقية (مثل ملفات ال exe) ، واستخدام مصادقة متعددة العوامل لمشاركة الملفات.

K. الضوابط التي وضعتها المؤسسة للتخفيف من مخاطر الأمن السيبراني المتعلقة بتقديم الخدمات، بما في ذلك:

1. التأكد من أن عملية إدارة التغيير تتضمن النظر في مخاطر الأمن السيبراني عند تقييم التغييرات والموافقة عليها والاستجابة للحوادث السيبرانية في الوقت المناسب.
2. يقوم مكتب مساعدة المستخدم بتسجيل جميع أحداث الأمن السيبراني التي ترسلها المؤسسة، ويضمن حلها في الوقت المناسب، ويصعدها إلى العضو المناسب في الإدارة.
3. تم تحديد إدارة الأجهزة المحمولة (مثل البريد الإلكتروني والتطبيقات وغيرها) للتخفيف من مخاطر الأمن السيبراني ويمكن إدارتها عن بعد في حالة تعرض جهاز المستخدم للخطر.

L. ضوابط الأمن المادي لحماية المعلومات عالية المخاطر بما في ذلك مخاطر الأمن السيبراني. تشمل الأمثلة التأكد من أن وصول الطرف الثالث/المورد مناسب وحصر وصول المستخدم الفعلي إلى مراكز البيانات ومراكز عمليات الشبكة ومراكز العمليات الأمنية على الموظفين المخولين.

M. الضوابط التي نفذتها المؤسسة فيما يتعلق بالاستجابة للحوادث والتعافي منها، والتي يجب أن تشمل:
1. خطة موثقة يتم مراجعتها وتحديثها مع تغير عمليات المؤسسة مع مرور الوقت.
2. إجراء الاختبارات الدورية وإبلاغ الإدارة بالنتائج.
3. تحديد ما إذا كان سيتم علاج أية مشاكل تم تحديدها عن طريق الاختبار في الوقت المناسب.

الملحق ب. أداة لتوثيق التوافق مع المعايير الخاصة بمواضيع معينة

الأمن السيبراني – الحوكمة

المتطلبات	المطابقة (نعم / لا / جزئي)	الأدلة التي تم الحصول عليها أو الأساس المنطقي للاستبعاد
A. يتم وضع السياسات والإجراءات المتعلقة بعمليات إدارة مخاطر الأمن السيبراني وتحديثها بشكل دوري، بما في ذلك تعزيز الممارسات القائمة على أطر العمل المعتمدة على نطاق واسع (NIST, COBIT وغيرها) التي تعزز بيئة الرقابة.		
B. الأدوار والمسؤوليات التي تدعم أهداف الأمن السيبراني للمؤسسة محددة بوضوح، ويتم شغل الأدوار بشكل صحيح.		
C. يتم إرسال تحديثات لأهداف واستراتيجيات ومخاطر الأمن السيبراني وضوابط التخفيف إلى مجلس الإدارة بشكل دوري.		
D. يشارك أصحاب المصلحة المعنيون في مناقشة أفضل السبل لإنشاء وتحسين عمليات إدارة مخاطر الأمن السيبراني.		
E. يتم إبلاغ مجلس الإدارة بالموارد المطلوبة (القيادة، والتمويل، والمهارات، والأجهزة، والبرمجيات، والتدريب، وغيرها) اللازمة للتنفيذ الفعال لعمليات إدارة مخاطر الأمن السيبراني.		

الأمن السيبراني – إدارة المخاطر

المتطلبات	المطابقة (نعم / لا / جزئي)	الأدلة التي تم الحصول عليها أو الأساس المنطقي للاستبعاد
A. إنشاء عملية لإدارة المخاطر على مستوى المؤسسة تتضمن تحديد وتحليل وإدارة المخاطر المتعلقة بتكنولوجيا المعلومات والأمن، مع التركيز بشكل خاص على مخاطر الأمن السيبراني وكيف يمكن أن تؤثر تلك المخاطر على قدرة المؤسسة على تحقيق أهدافها.		
B. يتم إجراء عمليات إدارة مخاطر الأمن السيبراني من قبل فريق متعدد الوظائف يتضمن قيادة تكنولوجيا المعلومات، وإدارة المخاطر على مستوى المؤسسة، والإدارة القانونية، والامتثال، وغيرها من الإدارة (على سبيل المثال، العمليات، والمحاسبة/التمويل) وإشراك الأطراف الخارجية (البائعين، الموردين، العملاء وغيرهم) حسب الاقتضاء.		
C. تم وضع السياسات والإجراءات المتعلقة بإدارة مخاطر الأمن السيبراني ويتم تحديثها دوريًا، بما في ذلك تعزيز الممارسات التي تعزز عمليات إدارة مخاطر الأمن السيبراني بناءً على أطر إدارة المخاطر المعتمدة على نطاق واسع، أو التوجيهات الرسمية، أو أفضل الممارسات.		
D. تحديد المساءلة والمسؤولية فيما يتعلق بإدارة مخاطر الأمن السيبراني وتحديد فرد أو فريق يقوم بشكل دوري بمراقبة وإبلاغ كيفية إدارة مخاطر الأمن السيبراني، بما في ذلك متطلبات الموارد للتخفيف من المخاطر وتحديد مخاطر الأمن السيبراني الناشئة التي كانت موجودة سابقًا لم يتم التعرف عليها.		

المتطلبات	المطابقة (نعم / لا / جزئي)	الأدلة التي تم الحصول عليها أو الأساس المنطقي للاستبعاد
E. يتم إنشاء عملية للتصعيد السريع لمخاطر الأمن السيبراني (الناشئة أو التي تم تحديدها مسبقًا) والتي ترتفع إلى مستويات غير مقبولة بناءً على إرشادات إدارة المخاطر المعمول بها في المؤسسة أو للامتثال للمتطلبات القانونية و/أو التنظيمية المعمول بها.		
F. تتضمن إدارة مخاطر الأمن السيبراني التنسيق بين إدارة أمن المعلومات والإدارة القانونية وإدارة الامتثال وغيرها لتحديد جميع الالتزامات القانونية والتعاقدية (القوانين والانظمة) والامتثال لها. يتم إبلاغ حالة الامتثال وعدم الامتثال للمتطلبات المعمول بها إلى المؤسسة بشكل دوري.		
G. توجد عملية لتحديد وإدارة مخاطر الأمن السيبراني المتعلقة بأطراف ثالثة. يُطلب من البائعين والموردين وغيرهم من مقدمي العمليات و/أو الخدمات الخارجية تنفيذ ضوابط فعالة للأمن السيبراني تحمي بشكل مناسب سرية وسلامة وتوافر أنظمة وبيانات المؤسسة التي يمكنهم الوصول إليها.		
H. تم تصميم السياسات والعمليات المتعلقة بتصنيف البيانات والاحتفاظ بها وتدميرها وتشفيرها بشكل مناسب ونشرها بشكل فعال لتوفير نهج منظم يضمن التسجيل الكامل والدقيق للبيانات ويحمي سرية وخصوصية المعلومات الحساسة.		
I. توجد عملية للإبلاغ عن المخاطر التشغيلية للأمن السيبراني لضمان الوعي المناسب من قبل الإدارة والموظفين. ويتم إبلاغ المشاكل والثغرات وأوجه القصور وفشل التحكم إلى مجلس الإدارة والإدارة ويتم مراقبة حالة الإصلاح والإبلاغ عنها عن كثب. يتم تحديد حالات عدم الامتثال لسياسات الأمن السيبراني والتحقيق فيها والإبلاغ عنها ومعالجتها في الوقت المناسب.		

الأمن السيبراني – عمليات الرقابة

المتطلبات	المطابقة (نعم / لا / جزئي)	الأدلة التي تم الحصول عليها أو الأساس المنطقي للاستبعاد
A. إعطاء الأولوية لضوابط الأمن السيبراني والتأكد من تخصيص الميزانية والموارد ذات الصلة (على سبيل المثال، الموظفين والبرامج والأدوات) لتحقيق أقصى قدر من الفوائد المتوقعة.		
B. التأكد من أن ضوابط الأمن السيبراني تعمل بطريقة تعزز تحقيق أهداف الأمن السيبراني التنظيمي وحلها في الوقت المناسب عند حدوث المشاكل.		
C. توفير التدريب الكافي للموظفين المسؤولين عن عمليات الأمن السيبراني.		
D. وضع سياسات وإجراءات كافية لإدارة كافة جوانب عمليات الأمن السيبراني والضوابط المرتبطة بها.		
E. الإدارة لديها الموارد اللازمة للبقاء على اطلاع بقضايا الأمن السيبراني الناشئة من التقنيات الجديدة، وتحديد الفرص لتحسين العمليات، وفهم أفضل السبل لنشر جهود الأمن السيبراني للتأثير على الأهداف والغايات التنظيمية الأوسع.		

المتطلبات	المطابقة (نعم / لا / جزئي)	الأدلة التي تم الحصول عليها أو الأساس المنطقي للاستبعاد
F. دمج الأمن السيبراني بشكل مناسب في دورة حياة تطوير النظام لتطبيقات الأعمال، بما في ذلك البرامج والتطبيقات المكتسبة أو المطورة خصيصًا.		
G. أدراج الأمن السيبراني في إدارة الأجهزة (أجهزة الكمبيوتر المحمولة، وأجهزة الكمبيوتر المكتبية، والأجهزة المحمولة).		
H. تنفيذ ضوابط فعالة فيما يتعلق بدعم أجهزة الإنتاج، مثل التكوين والتصحيح ودعم إدارة وصول المستخدم ومراقبة التوفر والأداء. قامت المؤسسة بتقييم مدى كفاية التصميم والفعالية التشغيلية لهذه الضوابط.		
I. تحسين الضوابط المتعلقة بالشبكة فيما يتعلق بتجزئة الشبكة، واستخدام جدران الحماية ووضعها، والاتصالات المحدودة بالشبكات و/أو الأنظمة الخارجية، واستخدام التقنيات الوقائية والكشفية مثل أنظمة كشف/منع التسلل.		
J. تنفيذ ضوابط فعالة تحيط بخدمات الاتصالات الشائعة مثل البريد الإلكتروني ومتصفحات الإنترنت ومؤتمرات الفيديو والمراسلة وبروتوكولات مشاركة الملفات.		
K. تطبيق ضوابط مناسبة لتقديم الخدمات لضمان تكامل المجالات التالية مع مراقبة الأمن السيبراني: إدارة التغيير، ومكتب الخدمة/المساعدة، وإدارة جهاز المستخدم النهائي.		
L. بتطبيق ضوابط الأمان المادي المناسبة لحماية مراكز المعلومات عالية المخاطر (مثل مراكز البيانات ومراكز عمليات الشبكة ومراكز العمليات الأمنية) من الهجمات.		
M. تطبيق ضوابط الاستجابة للحوادث والاسترداد.		

نبذة عن المعهد الدولي للمدققين الداخليين

المعهد الدولي للمدققين الداخليين (IIA) هو جمعية مهنية دولية تخدم أكثر من 245000 عضو عالمي وقد منحت أكثر من 195000 شهادة مدقق داخلي معتمد (CIA®) في جميع أنحاء العالم. تأسس المعهد الدولي للمدققين الداخليين (IIA) في عام 1941، وهو معروف في جميع أنحاء العالم باعتباره رائدًا في مهنة التدقيق الداخلي في المعايير والشهادات والتعليم والبحث والتوجيه الفني. لمزيد من المعلومات، قم بزيارة www.theiia.org

إخلاء مسؤولية

ينشر معهد المدققين الداخليين هذه الوثيقة لأغراض إعلامية وتعليمية. لا يُقصد من هذه المادة تقديم إجابات نهائية لظروف فردية محددة، وعلى هذا النحو يُقصد استخدامها كدليل فقط. يوصي معهد المدققين الداخليين بطلب مشورة الخبراء المستقلين فيما يتعلق مباشرة بأي موقف محدد. ولا يتحمل معهد المدققين الداخليين أي مسؤولية تجاه أي شخص يعتمد بشكل منفرد على هذه المادة.

حقوق النشر

قام بترجمة المعايير الى اللغة العربية فريق عمل من جمعية المدققين الداخليين في لبنان برئاسة ناجي فياض وعضوية داليا أبو كروم و محمد شهاب.

ابريل 2024

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101