المعايير الخاصة بموضوع الأمن السيبراني

Topical Requirement

دليل المستخدم

The Institute of Internal Auditors

المحتويات

نظرة عامة على المعايير الخاصة بمواضيع معينة

تعد المعايير الخاصة بمواضيع معينة عنصرًا أساسيًا في الإطار الدولي للممارسات المهنية (International Professional Practices Framework®)، إلى جانب المعايير العالمية للتدقيق الداخلي والإرشادات العالمية (Global Internal Audit Standards™) يشترط المعهد الدولي للمدققين الداخليين، باعتباره واضع المعايير لمهنة التدقيق الداخلي، استخدام هذه المعايير الخاصة الإلزامية كمكمل للمعايير العالمية للتدقيق الداخلي، والتي تعمل بمثابة المرجع للممارسات المطلوبة الموضحة والمشار إليها في المعايير الخاصة للمواضيع المعينة.. تظهر الإشارات إلى المعايير في جميع أنحاء هذا الدليل كمصدر لمعلومات أكثر تفصيلا.

تضفي المعايير الخاصة بمواضيع معينة الطابع الرسمي على كيفية معالجة المدققين الداخليين لمجالات المخاطر السائدة لتعزيز الجودة والاتساق داخل المهنة. تضع المعايير الخاصة بمواضيع معينة الخط الأساسي وتوفر المعايير ذات الصلة لأداء خدمات التأكيد المتعلقة بالموضوع المعين (معايير التقييم المعيارية 13.4). يعتبر التوافق مع المعايير الخاصة بمواضيع معينة إلزامي لخدمات التأكيد وموصى به أثناء الخدمات الاستشارية. لا يقصد بالمعايير الخاصة بمواضيع معينة تغطية جميع الجوانب المحتملة التي يجب مراعاتها عند تنفيذ التزامات التأكيد. ولكن الغرض منها هو توفير الحد الأدنى من المتطلبات لتمكين تقييم متسق وموثوق للموضوع.

ترتبط المعايير الخاصة بوضوح بنموذج الخطوط الثلاثة للمعهد الدولي للتدقيق الداخلي وبالمعايير العالمية للتدقيق الداخلي. تعد عمليات الحوكمة وإدارة المخاطر والرقابة هي المكونات الرئيسية للمعايير الخاصة بمواضيع معينة التي تتوافق مع المعيار 9.1 فهم الحوكمة وإدارة المخاطر وعمليات الرقابة. بالإشارة إلى نموذج الخطوط الثلاثة، ترتبط الحوكمة بمجلس الإدارة/الهيئة الإدارية، وترتبط إدارة المخاطر بالخط الثاني، وترتبط عمليات الضوابط أو الرقابة بالخط الأول. وفي حين أن الإدارة ممثلة في الخطين الأول والثاني، فإن وظيفة التدقيق الداخلي تظهر في الخط الثالث بوصفها جهة مستقلة وموضوعية تقدم تقاريرها إلى مجلس الإدارة (المبدأ 8 الاشراف من قبل المجلس).

قابلية التطبيق والمخاطر والحكم المهني

يجب اتباع المعايير الخاصة بمواضيع معينة عندما تقوم وظائف التدقيق الداخلي بإجراء مهام التأكيد على المواضيع التي يوجد لها معايير خاصة أو عندما يتم تحديد جوانب المعايير الخاصة بمواضيع معينة ضمن التزامات التأكيد الأخرى.

كما هو موضح في المعايير العالمية للتدقيق الداخلي، يعد تقييم المخاطر جزءا مهما من مرحلة التخطيط. يتطلب تحديد التزامات التأكيد التي يجب تضمينها في خطة التدقيق الداخلي تقييم استراتيجيات المؤسسة وأهدافها ومخاطرها سنويا على الأقل (المعيار 9.4 خطة التدقيق الداخلي). عند التخطيط لارتباطات التأكيد الفردية ، يجب على المدققين الداخليين تقييم المخاطر ذات الصلة بالمهمة (المعيار 13.2 تقييم مخاطر المهمة).

عندما يتم تحديد الموضوع المعين أثناء عملية تخطيط التدقيق الداخلي القائم على المخاطر ويتم تضمينه في خطة التدقيق، يجب استخدام المعايير الخاصة لتقييم الموضوع ضمن المهمة المعمول بها. بالإضافة إلى ذلك ، عندما يقوم المدققون الداخليون بإجراء مهمة (سواء كانت مدرجة أو غير مدرجة في الخطة) وتظهر عناصر من موضوع معين، يجب تقييم المتطلبات الخاصة بالموضوع المعين لقابليتها للتطبيق كجزء من المهمة. أخيرا، إذا تم طلب مهمة لم تكن في الأصل في الخطة وتتضمن الموضوع ، فيجب تقييم المتطلبات الخاصة به لقابليتها للتطبيق.

يلعب الحكم المهني دورا رئيسيا في تطبيق المعايير الخاصة بموضوع معين. تقود تقييمات المخاطر قرارات رؤساء المديرين التنفيذيين للتدقيق بشأن الالتزامات التي يجب تضمينها في خطة التدقيق الداخلي (المعيار 9.4 خطة التدقيق الداخلي). بالإضافة إلى ذلك ، يستخدم المدققون الداخليون الحكم المهني لتحديد الجوانب التي سيتم تغطيتها في كل مهمة (المعايير 13.3 أهداف المهمة ونطاقها ، 13.4 معايير التقييم ، و 13.6 برنامج العمل). الملحق أ "أمثلة التطبيق العملي" يصف كيف يحدد المدققون الداخليون ما إذا كان الموضوع تنطبق عليه المعايير الخاصة.

يجب الاحتفاظ بالدليل على أن كل متطلب في المعايير الخاصة قد تم تقييمه من أجل قابلية التطبيق ، بما في ذلك الأساس المنطقي الذي يفسر استبعاد أي متطلبات. يجب توثيق التوافق مع المعايير الخاصة باستخدام الحكم المهني للمدقق كما هو موضح في توثيق المهمة 14.6.

في حين أن المعايير الخاصة بموضوع الأمن السيبراني توفر خط أساس لعمليات الرقابة التي يجب مراعاتها ، فقد تحتاج المؤسسات التي تقيم المخاطر السيبرانية على أنها عالية جدا إلى تقييم جوانب إضافية.

إذا قرر الرئيس التنفيذي للتدقيق أن وظيفة التدقيق الداخلي لا تملك المعرفة المطلوبة لأداء ارتباطات التدقيق حول معايير موضوع معين الموضوعية، فيمكن الاستعانة بمصادر خارجية (المعايير 3.1 الكفاءة، 7.2 المؤهلات التنفيذية لرئيس التدقيق، 10.2 إدارة الموارد البشرية). وحتى في هذه الحالة، فإن الاستعانة بمصادر خارجية لا تعفي وظيفة التدقيق الداخلي من مسؤوليتها عن الامتثال للمعايير الخاصة بالموضوع. يحتفظ الرئيس التنفيذي للتدقيق بالمسؤولية النهائية عن ضمان المطابقة. بالإضافة إلى ذلك، إذا قرر الرئيس التنفيذي للتدقيق أن موارد التدقيق الداخلي غير كافية، فيجب عليه إبلاغ المجلس بأثر عدم كفاية الموارد وكيفية معالجة أي نقص في الموارد (الموارد 8.2).

الأداء والتوثيق وإعداد التقارير

عند تطبيق المعايير الخاصة بمواضيع معينة، يجب على المدققين الداخليين أيضا الامتثال للمعايير العالمية للتدقيق الداخلي، وإجراء عملهم بما يتماشى مع المجال الخامس: أداء خدمات التدقيق الداخلي. تصف المعايير الواردة في المجال الخامس تخطيط المهام (المبدأ 13 تخطيط المهام بشكل فعال) ، وإجراء المهام (المبدأ 14 إجراء عمل المهمة) ، وإبلاغ نتائج المهمة (المبدأ 15 الإبلاغ عن نتائج المهمة ومراقبة خطط العمل).

يمكن توثيق تغطية متطلبات المعايير الخاصة إما في خطة التدقيق الداخلي أو أوراق عمل المهمة بناء على الحكم المهني للمدققين. قد تغطي مهمة واحدة أو أكثر من عمليات التدقيق الداخلي المتطلبات. بالإضافة إلى ذلك ، قد لا تكون جميع المتطلبات قابلة للتطبيق. يجب الاحتفاظ بالدليل على أن الشروط قد تم تقييمها من أجل قابلية التطبيق ، بما في ذلك الأساس المنطقي الذي يشرح أي استثناءات.

يمكن استخدام الأداة الاختيارية في الملحق ج كمرجع ولتوثيق العمل الذي يؤديه المدققون الداخليون.

ضمان الجودة

تتطلب المعايير من الرئيس التنفيذي للتدقيق تطوير وتنفيذ والحفاظ على برنامج ضمان الجودة وتحسينه يغطي جميع جوانب وظيفة التدقيق الداخلي (المعيار 8.3 الجودة). يجب إبلاغ النتائج إلى مجلس الإدارة والإدارة العليا. يجب أن تقدم البلاغات تقريرا عن توافق وظيفة التدقيق الداخلي مع المعايير وتحقيق أهداف الأداء.

سيتم تقييم التوافق مع المعايير الخاصة بمواضيع معينة في تقييمات الجودة. للتحضير لتدقيق الجودة ، يمكن للمراجعين الداخليين استخدام الأداة المقدمة في الملحق جيم.

الأمن السيبراني

الأمن السيبراني هو موضوع واسع يتعلق بمعظم الجوانب التكنولوجية لأي مؤسسة. بالإضافة إلى تكنولوجيا المعلومات، يعد الأمن السيبراني عادة جزءا من العمليات التجارية، مما يستلزم قيام المدققين الداخليين بتقييم المخاطر المتعلقة بالإنترنت عند التخطيط وتحديد النطاق وتنفيذ ارتباطات الضمان.

يعرف المعهد الوطني للمعايير والتكنولوجيا (NIST)، وهو جزء من وزارة التجارة الأمريكية، الأمن السيبراني ببساطة بأنه "القدرة على حماية أو الدفاع عن استخدام الفضاء السيبراني من الهجمات الإلكترونية". تركز المعايير الخاصة بموضوع الأمن السيبراني على المحيط الخارجي الذي تؤمنه المؤسسات للتخفيف من المخاطر من المستخدمين غير المصرح لهم والتهديدات السيبرانية الضارة. الأمن السيبراني هو مجموعة فرعية من أمن المعلومات الشامل، والذي يعرفه NIST بأنه "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".

تشمل متطلبات المعايير الخاصة بمواضيع معينة للأمن السيبراني ما يلي:

- الحوكمة - أهداف واستراتيجيات الأمن السيبراني الأساسية المحددة بوضوح والتي تدعم الأهداف والسياسات والإجراءات التنظيمية.

- إدارة المخاطر - عمليات تحديد التهديدات السيبرانية وتحليلها وإدارتها ومراقبتها ، بما في ذلك عملية تصعيد المخاطر السيبرانية على الفور.
- الضوابط - عمليات الرقابة التي أنشأتها الإدارة وتقييمها بشكل دوري للتخفيف من المخاطر السيبرانية.

الاعتبارات

قد يستخدم المدققون الداخليون الاعتبارات التالية للمساعدة في تقييمهم للمتطلبات الواردة في المعايير الخاصة بموضوع الأمن السيبراني. وهذه الاعتبارات، التي تشير إلى المتطلبات، توضيحية، ولكنها ليست إلزامية. يجب على المدققين الداخليين الاعتماد على الحكم المهني عند تحديد ما يجب تضمينه في تقييماتهم.

اعتبارات الحوكمة

لتقييم كيفية تطبيق عمليات الحوكمة على أهداف الأمن السيبراني، قد يراجع المدققون الداخليون:

أ. الخطة والأهداف الاستراتيجية للأمن السيبراني الرسمية والموثقة ، بما في ذلك الأدلة على أن مجلس الإدارة يقوم بتدقيق تحديثات الأمن السيبراني بشكل دوري (بشكل عام ربع سنوي) لتحديثات الأمن السيبراني التي يقدمها رئيس وظيفة أمن المعلومات ، مثل كبير مسؤولي أمن المعلومات (CISO). قد تشمل الأدلة الإبلاغ عن:
   - مراقبة تحقيق الأهداف الاستراتيجية.
   - احتياجات الميزانية لدعم أهداف وغايات الأمن السيبراني.
   - التركيز على المخاطر والضوابط الداخلية ، بما في ذلك تقدم المعالجة.
   - مؤشرات الأداء الرئيسية (KPIs) لقياس النجاح.
   - الموارد البشرية اللازمة لتوظيف وتدريب وتطوير موظفي الأمن السيبراني.

ب. السياسات والإجراءات والوثائق الأخرى ذات الصلة المستخدمة لإدارة عمليات الأمن السيبراني، بما في ذلك:
   - السياسات التي تتم مراجعتها وتحديثها سنويا على الأقل. قد تتطلب المخاطر السيبرانية الناشئة حدوث المراجعات والتحديثات بشكل متكرر.
   - عملية لتحديد ما إذا كانت السياسات والإجراءات كافية لدعم عمليات الأمن السيبراني.
   - أطر عمل معتمدة على نطاق واسع (NIST و COBIT وغيرها) لتعزيز عمليات الأمن السيبراني والضوابط الداخلية.

ت. الأدوار والمسؤوليات التي تدعم تحقيق أهداف الأمن السيبراني، بما في ذلك الهيكل الذي يضمن أن وظيفة الأمن السيبراني تقدم تقاريرها إلى مستوى في المؤسسة لديه رؤية كافية لتحقيق الدعم التنظيمي.
   - عملية لتقييم المعرفة والمهارات والقدرات بشكل دوري للموظفين الذين يشغلون أدوار الأمن السيبراني.

ث. دليل على المهمة مع أصحاب المصلحة المعنيين (على سبيل المثال، الإدارة العليا، والعمليات، وإدارة المخاطر، والموارد البشرية، والقانونية، والامتثال، والبائعين الاستراتيجيين، وغيرها)، بما في ذلك التواصل حول المخاطر السيبرانية الحالية والناشئة ونقاط الضعف المحتملة المعروفة. قد يتضمن دليل الاتصال محاضر الاجتماع أو التقارير أو رسائل البريد الإلكتروني.

اعتبارات إدارة المخاطر

لتقييم كيفية تطبيق عمليات إدارة المخاطر على أهداف الأمن السيبراني، قد يراجع المدققون الداخليون:

أ. كيف تقوم المؤسسة بتقييم مخاطر الأمن السيبراني وإدارتها، بما في ذلك كيفية التهديدات ونقاط الضعف:
   - تم تحديدها والإبلاغ عنها في البداية.
   - تم تحليلها لتقييم المخاطر التي تهدد تحقيق الأهداف التنظيمية.

- مخفف من حدة العقوبة، بما في ذلك خطط العمل لتقليل المخاطر إلى مستوى مقبول.
- مراقبة، بما في ذلك خطة للإبلاغ المستمر حتى يتم حل التهديدات بالكامل.

ب. كيف تحصل المؤسسة على مدخلات دورية فيما يتعلق بإدارة مخاطر الأمن السيبراني من المجالات الوظيفية ، مثل تكنولوجيا المعلومات ، وإدارة مخاطر المؤسسة ، والموارد البشرية ، والقانونية ، والامتثال ، والعمليات ، والمحاسبة ، والتمويل. يمكن استخدام فريق الأمن السيبراني متعدد الوظائف أو اللجنة التوجيهية لتكنولوجيا المعلومات للحصول على المعلومات.

ت. كيف قامت المؤسسة بتعيين المساءلة والمسؤولية عن إدارة مخاطر الأمن السيبراني إلى فرد أو فريق.

- يجب على الشخص (الأشخاص) المسؤول الإبلاغ عن التحديثات المستمرة لمخاطر الأمن السيبراني في جميع أنحاء المؤسسة بشكل دوري (ربع سنوي أو شهري أو حسب الحاجة) وقد يتضمن أيضا متطلبات الموارد لاستراتيجيات التخفيف من المخاطر.

ث. عمليات التصعيد لمخاطر الأمن السيبراني، بما في ذلك كيفية تقييم مستوى التهديد أو المخاطر وتعيينه وتحديد أولوياته. قد تشمل التدقيق تحديد:

- مستويات المخاطر المحددة للمؤسسة - مثل المرتفعة والمتوسطة والمنخفضة - مع تفسيرات مفصلة لكل مستوى من مستويات المخاطر وإجراءات التصعيد لكل فئة من فئات المخاطر.
- قائمة بمخاطر الأمن السيبراني المحددة حاليا وحالة التخفيف من حدة كل حدث من أحداث المخاطر.
- المتطلبات القانونية والتنظيمية ومتطلبات الامتثال المعمول بها.
- كل من الآثار المالية وغير المالية (على سبيل المثال ، السمعة) على المخاطر.

ج. عملية توصيل مخاطر الأمن السيبراني للإدارة والموظفين ، والتي تشمل:

- تدريب دوري (سنويا على الأقل) على الأمن السيبراني للموظفين، مثل حملات التصيد الاحتيالي غير المعلنة والمحاكاة لاختبار الوعي التنظيمي وتتبعه.
- تحديثات حول معالجة مشكلات الأمن السيبراني الحالية، مع تواريخ الانتهاء المتوقعة.
- مراقبة عدم الامتثال الذي يتضمن تحديثات لمجلس الإدارة والإدارة العليا.
- إعادة تقييم التهديدات عندما تتغير رغبة المؤسسة في المخاطرة وتحمل المخاطر.

ح. العمليات التي نفذتها المؤسسة فيما يتعلق بالاستجابة للحوادث والتعافي منها ، والتي تشمل:

- خطة موثقة تتم مراجعتها وتحديثها مع تغير عمليات المؤسسة بمرور الوقت. يجب أن تتضمن الخطة:
  - كيف يتم اكتشاف الحوادث والإبلاغ عنها.
  - كيف يتم احتواء الحوادث لمنع المزيد من الضرر.
  - كيف ستتعافى المؤسسة وتستجيب لاستئناف العمليات.
  - كيف سيتم تحليل الحادث لتحديد الدروس المستفادة وكيفية منع حدوث أحداث مستقبلية مماثلة.
- الاختبار الدوري (سنويا على الأقل) (تمرين الطاولة) والإبلاغ عن النتائج إلى الإدارة العليا وأصحاب المصلحة المعنيين. قد تنتج خطط العمل عن الاختبار.

اعتبارات عملية التحكم

لتقييم كيفية تطبيق عمليات الرقابة على أهداف الأمن السيبراني ، قد يراجع المدققون الداخليون:

أ. نهج الإدارة لبناء بيئة رقابة داخلية فعالة للأمن السيبراني ، بما في ذلك:

- تقييم وتنفيذ الضوابط الداخلية المطلوبة للتخفيف من المخاطر المرتفعة وحماية البيانات الحساسة أو الحرجة أو الشخصية أو السرية ، المستنيرة بعملية تقييم المخاطر التنظيمية.
- تحديد متطلبات الموارد للحفاظ على ضوابط الأمن السيبراني الرئيسية.
- النظر في عناصر التحكم المستندة إلى البائع كجزء من بيئة التحكم، والتي تتضمن تدقيق تقارير عناصر التحكم في تنظيم الخدمة (SOC) من الموردين قبل بدء علاقة العمل وطوال مدة العلاقة.
- اختبار دوري لضوابط الأمن السيبراني تعمل بطريقة تخفف من المخاطر وتدعم تحقيق أهداف الأمن السيبراني.
- عملية معالجة أوجه القصور في الرقابة الداخلية أو معالجة النتائج من التقييمات التي تجريها وظيفة التدقيق الداخلي أو مزودي الضمان الآخرين (على سبيل المثال ، اختبار الاختراق).

ب. عملية إدارة المواهب في المؤسسة لتوظيف وتدريب المتخصصين في الأمن السيبراني، بما في ذلك كيفية تحديد المؤسسة للفرص لزيادة قدرات المتخصصين في الأمن السيبراني لدعم المعرفة التقنية وتحسين الوعي التنظيمي بالقضايا الناشئة.

- تشمل الأمثلة المشاركة في التدريب ، والمشاركة في مجموعات تبادل المعرفة ، والتعليم المهني المستمر الذي يتضمن الحصول على الشهادات المتعلقة بالإنترنت.

ت. عملية الإدارة لتحديد تهديدات ونقاط الضعف الناشئة في مجال الأمن السيبراني وتحديد أولوياتها ومراقبتها والإبلاغ عنها على أساس مستمر يركز على العمليات اليومية. قد تشمل التدقيق إنشاء عمليات لتقييم التهديدات ونقاط الضعف المتعلقة بالتقنيات الجديدة أو الناشئة مثل استخدام الذكاء الاصطناعي.

ث. تم وضع عمليات الإدارة والضوابط لإدارة أصول تكنولوجيا المعلومات وحمايتها طوال دورة الحياة بما في ذلك اختيار الأجهزة والبرامج وخدمات البائعين واستخدامها وصيانتها وإيقاف تشغيلها. تتضمن الأجهزة الخوادم ومعدات الشبكات (مثل أجهزة التوجيه أو جدران الحماية) وأجهزة الكمبيوتر المكتبية وأجهزة الكمبيوتر المحمولة والهواتف المحمولة والأجهزة اللوحية والأجهزة الطرفية. يتضمن البرنامج أنظمة التشغيل (مثل Windows) وبرامج تخطيط موارد المؤسسات والتطبيقات وبرامج مكافحة الفيروسات وغيرها. قد تشمل اعتبارات الأجهزة والبرامج ما يلي:

- استخدام المؤسسة للتشفير وبرامج مكافحة الفيروسات وإدارة الأجهزة المحمولة ومتطلبات كلمات المرور المعقدة والشبكة الافتراضية الخاصة (VPN) / شبكة انعدام الثقة (ZTN) للمصادقة والتحديث الدوري للبرامج الثابتة.
- عملية إدارة الأصول التي تضمن أن الأجهزة الصادرة عن الشركة لديها تكوين أمان مناسب عند الإصدار والتخلص الصحيح عند إيقاف الأصول.
- عناصر التحكم المتعلقة بقاعدة البيانات التي تتضمن تقييد وصول المستخدم والمسؤول ، وضمان استخدام التشفير ، والنسخ الاحتياطي واختبار قواعد البيانات ، ووجود ضوابط أمان قوية للشبكة.
- كيف يتم النظر في تهديدات الأمن السيبراني أو نقاط الضعف في دورة حياة تطوير النظام (SDLC).
- يتضمن النهج المستخدم من قبل التطوير والأمن والعمليات (DevSecOps) لضمان أن عملية تطوير البرامج الأمن السيبراني لتحديد نقاط الضعف بشكل استباقي.

ج. العمليات المستخدمة لتعزيز الأمن السيبراني، بما في ذلك:

- تكوين إعدادات الأمان لتقليل مخاطر الأمن السيبراني.
- تم تكوين إدارة الأجهزة المحمولة (بما في ذلك استخدام البريد الإلكتروني والتطبيقات) للتخفيف من مخاطر الأمن السيبراني وإدارتها عن بعد في حالة تعرض جهاز المستخدم للخطر.
- استخدام التشفير للبيانات "الثابتة"، مثل المعلومات المخزنة على القرص الصلب، أو البيانات "أثناء النقل"، مثل تشفير رسائل البريد الإلكتروني.
- تصحيح الخوادم أو البرامج (مثل نظام التشغيل) بأحدث إصدارات الأمان.
- إدارة وصول المستخدم مثل استخدام المصادقة متعددة العوامل (MFA) ومعرفات المستخدمين الفريدة بكلمات مرور معقدة تنتهي صلاحيتها بشكل دوري.
- ضوابط المراقبة المعمول بها لتحديد ما إذا كان التوافر واستخدام الموارد يعمل بشكل كاف ، مما يسمح بمراجعة وتحليل مشكلات الأمن السيبراني المحتملة التي تهدد الأداء.

- دمج الأمن السيبراني في SDLC لتحديد نقاط الضعف في الأمن السيبراني ومعالجتها قبل نقل البرامج إلى الإنتاج.

ح. عناصر التحكم المتعلقة بالشبكة التي تؤمن محيط المؤسسة، بما في ذلك كيفية استخدام المؤسسة:

- تجزئة الشبكة.
- جدران الحماية.
- عناصر التحكم في وصول المستخدم.
- القيود المفروضة على كل من الاتصالات الخارجية والداخلية.
- عناصر التحكم المحيطة بإنترنت الأشياء (IoT) للشبكات المترابطة.
- أنظمة الكشف عن التسلل / الوقاية منه لمنع هجمات الأمن السيبراني واكتشافها والتعافي منها.

خ. عناصر الضبط المحيطة بأمان اتصالات نقطة النهاية المطبقة على الخدمات مثل البريد الإلكتروني ومتصفحات الإنترنت ومؤتمرات الفيديو والمراسلة (Zoom و MS Teams وغيرها) والوسائط الاجتماعية والسحابة وبروتوكولات مشاركة الملفات. قد تتضمن عناصر التحكم تقييد استخدام امتدادات ملفات معينة (مثل ملفات .exe) والمصادقة متعددة العوامل لمشاركة الملفات.

الملحق أ. أمثلة التطبيق العملي

تصف الأمثلة التالية السيناريوهات التي يمكن فيها تطبيق المعايير الخاصة بموضوع الأمن السيبراني:

مثال 1: يتم تحديد الأمن السيبراني لمهمة التدقيق الداخلي المضمنة في خطة التدقيق الداخلي.

عندما تكمل وظيفة التدقيق الداخلي عملية التخطيط القائمة على المخاطر وتتضمن مهمة واحدة أو أكثر حول الأمن السيبراني في خطة التدقيق الداخلي، يتم تفويض المعايير الخاصة بمواضيع معينة عند إجراء مثل هذه الالتزامات. يمكن تحقيق المطابقة من خلال تضمين المتطلبات عبر التزام واحد أو أكثر في خطة التدقيق الداخلي.

يعد الأمن السيبراني موضوعا واسعا، وقد يكون تطبيق كل متطلبات المعايير الخاصة غير مطلوب في كل مهمة. عندما يطبق المدققون الداخليون الحكم المهني ويقررون أن واحدا أو أكثر من متطلبات المعايير الخاصة بموضوع الأمن السيبراني غير قابل للتطبيق وبالتالي يجب استبعاده من المهمة، يجب على المدققين الداخليين توثيق الأساس المنطقي لاستبعاد هذه المتطلبات والاحتفاظ به. على سبيل المثال، قد يكون الأساس المنطقي لاستبعاد بعض المتطلبات هو أن وظيفة التدقيق الداخلي تؤدي العديد من ارتباطات الأمن السيبراني على أساس التناوب أو حددت أن أهمية المخاطر في المهمة منخفضة.

مثال 2: يتم تحديد مخاطر الأمن السيبراني أثناء مهمة التدقيق التي لا تركز على الأمن السيبراني.

قد يحدد المدققون الداخليون أخطار الأمن السيبراني أثناء تقييم عملية لا تتعلق مباشرة بالأمن السيبراني. على سبيل المثال، قد يقوم المدققون الداخليون بتقييم عملية الحسابات الدائنة في مهمة لا تركز على الأمن السيبراني ولا يحددون مخاطر الأمن السيبراني ضمن النطاق عند التخطيط للمهمة. ومع ذلك، بعد إجراء الإرشادات الأولية ، يقرر المدققون الداخليون أن هذه المخاطر يجب أن تكون في النطاق. على سبيل المثال، يحددون مخاطر الأمن السيبراني المتعلقة بتقديم طلب أمر شراء أولي على شبكة الإنترنت (تقييم مخاطر المهمة القياسي 13.2).

بمجرد تحديد المخاطر ذات الصلة، يجب على المدققين الداخليين مراجعة المعايير الخاصة بموضوع الأمن السيبراني وتحديد المتطلبات القابلة للتطبيق. في هذا المثال، قد يستبعدون عملية حوكمة الأمن السيبراني أو عملية إدارة مخاطر الأمن السيبراني. يجب عليهم توثيق الأساس المنطقي لاستبعاد المتطلبات الأخرى للمعايير الخاصة بالأمن السيبراني والاحتفاظ بالوثائق.

مثال 3: طلب مهمة الأمن السيبراني التي لم يتم تضمينها في الأصل في خطة التدقيق الداخلي.

قد يطلب أصحاب المصلحة مثل مجلس الإدارة أو الإدارة أو الجهة التنظيمية من المدققين الداخليين إجراء تقييمات للأمن السيبراني خارج خطة التدقيق الأصلية. على سبيل المثال، عندما تكون المؤسسات هدفا لهجوم إلكتروني، قد يطلب مجلس الإدارة من التدقيق الداخلي تقييم ضوابط الأمن السيبراني. في هذه الحالة تكون المعايير الخاصة بمواضيع معينة قابلة للتطبيق ، ويجب تقييم المتطلبات ، وتوثيق أي استثناءات.

الملحق ب - الربط بالأطر

قد يكون للمؤسسة جهودها الخاصة في مجال الأمن السيبراني، باستخدام أطر إدارة المخاطر والحوكمة مثل COBIT أو NIST. قد يكون المدققون الداخليون قد طوروا بالفعل برامج تدقيق وإجراءات اختبار بناء على هذه الأطر. يجب على المدققين الداخليين التوفيق بين اختبارات عمليات الضبط المقصودة ومتطلبات المعايير الخاصة بالأمن السيبراني لضمان التغطية الكافية. يرسم الرسم البياني أدناه المعايير الخاصة بموضوع الأمن السيبراني إلى ثلاثة أطر عمل شائعة الاستخدام: NIST Cybersecurity Framework 2.0 و COBIT 2019 و NIST 800-53. وقد تم رسم هذه الأطر لأنها متاحة بسهولة دون أي تكلفة.

متطلبات الحوكمة	مراجع الإطار		
	NIST CSF 2.0	NIST 800-53	COBIT 2019
أ. يتم وضع استراتيجية وأهداف رسمية للأمن السيبراني وتحديثها 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.	GV.RM-01; GV.RM-02; GV.RM-03; GV.RM-04; GV.OC-02; GV.RR-03; GV.RR-04; GV.PO-01; GV.PO-02; GV.OV-01; GV.OV-03	PM-1, PM-4; AT-2; AT-3; PM-9; PM-28	EDM01; EDM03; EDM04; APO06; APO01; APO10; APO12
ب. وضع السياسات والإجراءات المتعلقة بالأمن السيبراني وتحديثها دوريا وتعزيز بيئة الرقابة.	GV.PO-01; GV.PO-02; GV.OV-01; GV.OV-02; GV.OV-03; GV.SC-01; GV.SC-03; GV.RR-03	AC-1, PM-9; AC-1; AT-1; CA-1; CM-1; IA-1; IR-1; MP-1; PE-1	EDM01; EDM02; EDM03; APO01; APO11
ج. يتم تحديد الأدوار والمسؤوليات التي تدعم أهداف الأمن السيبراني، وتوجد عملية لتقييم المعرفة والمهارات والقدرات بشكل دوري لأولئك الذين يشغلون هذه الأدوار.	GV.RR-02; GV.RR-04; GV.SC-02; GV.OC-02	PM-13; AT-2; AT-3	EDM02; APO01; APO07
د. يتم إشراك أصحاب المصلحة المعنيين لمناقشة نقاط الضعف الحالية والتهديدات الناشئة في بيئة الأمن السيبراني والعمل بشأنها. يشمل أصحاب المصلحة الإدارة العليا والعمليات وإدارة المخاطر والموارد البشرية والقانونية والامتثال والبائعين وغيرها.	GV.OC-02; GV.RM-01; GV.RM-05; GV.RM-07; GV.OV-03; GV.SC-03	AC-1; CM-1	EDM05; EDM01.01; EDM03; MEA01.02; APO01; APO08; APO11; APO13; MEA02
متطلبات إدارة المخاطر	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**

متطلبات عملية الرقابة	NIST CSF 2.0	NIST 800-53	COBIT 2019
أ. تشمل عمليات تقييم المخاطر وإدارة المخاطر في المؤسسة تحديد تهديدات الأمن السيبراني وتحليلها والتخفيف من حدتها ومراقبتها وتأثيرها على تحقيق الأهداف الاستراتيجية.	GV.RM-01; GV.RM-03; GV.OC-01	AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
ب. يتم إجراء إدارة مخاطر الأمن السيبراني في جميع أنحاء المؤسسة ، والتي قد تشمل المجالات التالية: تكنولوجيا المعلومات ، وإدارة مخاطر المؤسسة ، والموارد البشرية ، والقانونية ، والامتثال ، والعمليات ، وسلسلة التوريد ، والمحاسبة ، والتمويل ، وغيرها.	GV.RM-01; GV.RM-05; GV.RR-01; GV.RR-02; GV.OC-03; GV.SC-07	PM-29; AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
ج. يتم تحديد المساءلة والمسؤولية عن إدارة مخاطر الأمن السيبراني ويتم 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.	GV.RR-01; GV.RR-02; GV.RR-03; GV.0V-01; GV.OV-02; GV.OV-03	PM-9; PM-29	EDM03; APO01; APO10; APO12
د. يتم إنشاء عملية لتصعيد أي مخاطر للأمن السيبراني بسرعة (ناشئة أو محددة مسبقا) ترتفع إلى مستوى غير مقبول بناء على إرشادات إدارة المخاطر المعمول بها في المؤسسة أو للامتثال للمتطلبات القانونية والتنظيمية المعمول بها. يجب مراعاة كل من الآثار المالية وغير المالية لمخاطر الأمن السيبراني.	GV.RM; ID.RA; RS.MA-04	CA-7; RA-3; RA-7	EDM03; APO01, APO10; APO12
ه. يتم إنشاء عملية لإيصال الوعي بمخاطر الأمن السيبراني إلى الإدارة والموظفين، وللمراجعة الدورية من قبل الإدارة للمشكلات، أو الفجوات أو أوجه القصور أو إخفاقات التحكم مع الإبلاغ والمعالجة.	PR.AT; GV.RR.01; GV.RR-04; GV.PO	AT-2	APO01; APO02; EDM03; MEA03
و. 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.	RS; RC	IR-4; IR-5; IR-6; IR-7; IR-8; IR-10; SA-15	DSS02; DSS03; DSS04; DSS05.07

أ. يتم إنشاء عملية تضمن وجود كل من الضوابط الداخلية والضوابط القائمة على المورد لحماية سرية وسلامة وتوافر أنظمة وبيانات المؤسسة. يتم تقييم الضوابط بشكل دوري لتحديد أنها تعمل بطريقة تعزز تحقيق أهداف الأمن السيبراني التنظيمي وحل المشكلات في الوقت المناسب.	ID.IM-01; ID.IM-02; ID.IM-03; PR; DE; RS; RC; ID.RA06; GV.RM-05; GV.SC; ID.IM-02; RS.MA-01; DE.CM-06	AC-3; AC-4; AC-10; AC-13; AC-17; PM-30; RA-3; SA-9; SR-2	MEA02; MEA04; EDM03; APO09; APO10; DSS01
ب. يتم إنشاء عملية إدارة المواهب ومراجعتها بشكل دوري لعمليات الأمن السيبراني والتي تتضمن فرصا تدريبية لتطوير الكفاءات الفنية والحفاظ عليها.	PR.AT-01; PR.AT-02; GV.RR-03	AT-2; AT-3; IR-2; PM-14	APOO7; DSS04
ج. يتم إنشاء عملية لمراقبة تهديدات ونقاط الضعف الناشئة في مجال الأمن السيبراني والإبلاغ عنها باستمرار وتحديد الفرص لتحسين عمليات الأمن السيبراني وتحديد أولوياتها وتنفيذها.	ID.RA-02; ID.RA-03, ID.RA-04	CA-7; PM-31; RA-5	DSS03.05
د. يتم تضمين الأمن السيبراني في إدارة دورة التطوير (الاختيار والاستخدام والصيانة وإيقاف التشغيل) لجميع أصول تكنولوجيا المعلومات، بما في ذلك الأجهزة والبرامج وخدمات البائعين.	ID.AM; PR.PS-03; PR.IR; DE.CM-09; ID.AM-08; ID.RA-09; PR.PS-06	AU-9; CM-7; SC-49; SC-51; CM-2; SA-3; SA-10; SA-15; SA-17; SA-20; AU-6; IR-7	DSS05.03; BAI03; BAI09; BAI03; BAI11; DSS05.01; DSS02; DSS03; DSS06.06
ه - يتم إنشاء عمليات لتعزيز الأمن السيبراني بما في ذلك التكوين وإدارة جهاز المستخدم النهائي والتشفير والتصحيح وإدارة نفاذ المستعمل ومراقبة التوافر والأداء. يتم تضمين اعتبارات الأمن السيبراني في تطوير البرامج (DevSecOps).	PR.PS-01; PR.PS-06; PR.DS-01; PR.DS-02; PR.PS-05; DE.CM-03	CM-6; SI-2; AC-3; CA-7; SA-4; AC-16; AC-18	BAI10; DSS05; DSS06.03; DSS01.03; MEA01
و - يتم وضع ضوابط متعلقة بالشبكة، مثل ضوابط الوصول إلى الشبكة والتجزئة؛ واستخدام جدران الحماية ووضعها ومحدودة التوصيلات من وإلى الشبكات الخارجية؛ والشبكة الافتراضية الخاصة (VPN)/النفاذ إلى شبكة انعدام الثقة (ZTNA)، وإدراج ضوابط شبكة إنترنت الأشياء (IoT)، وأنظمة الكشف عن التسلل/الوقاية (IDS وIPS).	PR.IR; DE.CM-01	AC-6; AC-17; AC-18; AC-20; SC-7; SC-10; CA-8	DSS05.02

BAI10	AC-2; AC-16; AU-10; CA-3; SI-8; SI-20; SC-8	PR.DS-01; PR.DS-02; PR.DS-10; PR.IR	ز. يتم إنشاء عناصر تحكم أمان اتصالات نقطة النهاية فيما يتعلق بخدمات مثل البريد الإلكتروني ومتصفحات الإنترنت ومؤتمرات الفيديو والمراسلة والوسائط الاجتماعية والسحابة وبروتوكولات مشاركة الملفات.

الملحق جيم - أداة التوثيق الاختيارية

ويتوقع من المدققين الداخليين أن يمارسوا الحكم المهني في تحديد مدى انطباق المتطلبات بناء على تقييم المخاطر وأن يوثقوا بشكل مناسب استثناءات بعض المتطلبات. يمكن توثيق المعايير الخاصة بمواضيع معينة في خطة التدقيق الداخلي أو في أوراق عمل المهمة بناء على الحكم المهني للمدقق. قد تغطي مهمة واحدة أو أكثر من عمليات التدقيق الداخلي المتطلبات. بالإضافة إلى ذلك، قد لا تكون جميع المتطلبات قابلة للتطبيق. يوفر النموذج القابل للطباعة أدناه خيارا واحدا لتوثيق التوافق مع المعايير الخاصة بموضوع الأمن السيبراني، ولكن استخدامه ليس إلزاميا.

الأمن السيبراني - الحوكمة

مرجع الوثائق	التغطية المنفذة أو حيثيات الاستبعاد	احتياج
		أ. يتم وضع استراتيجية وأهداف رسمية للأمن السيبراني وتحديثها دوريا. 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. يتم وضع السياسات والإجراءات المتعلقة بالأمن السيبراني وتحديثها بشكل دوري وتعزيز بيئة الرقابة.
		ج. يتم تحديد الأدوار والمسؤوليات التي تدعم أهداف الأمن السيبراني، وتوجد عملية لتقييم المعرفة والمهارات والقدرات بشكل دوري لأولئك الذين يشغلون الأدوار.
		د. يتم إشراك أصحاب المصلحة المعنيين لمناقشة نقاط الضعف الحالية والتهديدات الناشئة في بيئة الأمن السيبراني والعمل بشأنها. يشمل أصحاب المصلحة الإدارة العليا والعمليات وإدارة المخاطر والموارد البشرية والقانونية والامتثال والبائعين وغيرها.

الأمن السيبراني - إدارة المخاطر

مرجع الوثائق	التغطية المنفذة أو حيثيات الاستبعاد	احتياج
		أ. تشمل عمليات تقييم المخاطر وإدارة المخاطر في المؤسسة تحديد تهديدات الأمن السيبراني وتحليلها والتخفيف من حدتها ومراقبتها وتأثيرها على تحقيق الأهداف الاستراتيجية.

مرجع الوثائق	التغطية المنفذة أو حيثيات الاستبعاد	احتياج
		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.
		جيم - 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.
		د. 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.
		ه. 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.
		و. نفذت المؤسسة عملية الاستجابة لحوادث الأمن السيبراني والتعافي منها، بما في ذلك الكشف والاحتواء والتعافي وتحليل ما بعد الحادث. يتم اختبار عملية الاستجابة للحوادث والتعافي بشكل دوري.

مرجع الوثائق	التغطية المنفذة أو حيثيات الاستبعاد	احتياج
		أ. يتم إنشاء عملية لضمان وجود كل من الضوابط الداخلية والضوابط القائمة على البائع 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. تم إنشاء عملية إدارة المواهب التي تشمل التدريب لتطوير الكفاءات الفنية المتعلقة بعمليات الأمن السيبراني والحفاظ عليها. تتم مراجعة العملية بشكل دوري.
		ج. يتم إنشاء عملية لمراقبة تهديدات ونقاط الضعف الناشئة في مجال الأمن السيبراني والإبلاغ عنها باستمرار وتحديد الفرص لتحسين عمليات الأمن السيبراني وتحديد أولوياتها وتنفيذها.
		د. يتم تضمين الأمن السيبراني في إدارة دورة الحياة (الاختيار والاستخدام والصيانة وإيقاف التشغيل) لجميع أصول تكنولوجيا المعلومات، بما في ذلك الأجهزة والبرامج وخدمات البائعين.
		ه. يتم إنشاء عمليات لتعزيز الأمن السيبراني، بما في ذلك التكوين وإدارة جهاز المستخدم النهائي والتشفير والترقيع وإدارة نفاذ المستعملين ومراقبة التوافر والأداء. يتم تضمين اعتبارات الأمن السيبراني في تطوير البرامج (DevSecOps).
		و. يتم إنشاء ضوابط متعلقة بالشبكة، مثل ضوابط الوصول إلى الشبكة والتجزئة ؛ استخدام جدران الحماية ووضعها ؛ اتصالات محدودة من وإلى الشبكات الخارجية ؛ الشبكة الافتراضية الخاصة (VPN) / الوصول إلى شبكة الثقة (ZTNA) ، ضوابط شبكة إنترنت الأشياء (IoT) ، وأنظمة الكشف عن التسلل / منعه (IDS و IPS).

مرجع الوثائق	التغطية المنفذة أو حيثيات الاستبعاد	احتياج
		ز. يتم إنشاء عناصر تحكم أمان اتصالات نقطة النهاية لخدمات مثل البريد الإلكتروني ومتصفحات الإنترنت ومؤتمرات الفيديو والمراسلة والوسائط الاجتماعية والسحابة وبروتوكولات مشاركة الملفات.

نبذة عن معهد المدققين الداخليين

لمعهد الدولي للمدققين 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 المعهدالدولي للمدققين الداخليين في عام 1941 ، وهو معترف به في جميع أنحاء العالم كرائد في مهنة التدقيق الداخلي و المعايير والشهادات والتعليم والبحث والتوجيه الفني. لمزيد من المعلومات www.theiia.org.

اخلاء المسؤوليه

ينشر معهد المدققين الداخليين هذه الوثيقة لأغراض إعلامية وتعليمية. لا يقصد من هذه المادة تقديم إجابات نهائية لظروف فردية محددة، وبالتالي فهي مخصصة فقط لاستخدامها كدليل. ويوصي المعهد الدولي للمدققين الداخليين بالتماس مشورة الخبراء المستقلين فيما يتعلق مباشرة بأي حالة محددة. ولا يتحمل المعهد الدولي للمدققين الداخليين أي مسؤولية عن أي شخص يعتمد وحده على هذه المواد.

حقوق النشر

فبراير 2025

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