مصفوفة المخاطر والرقابة لإدارة تكنولوجيا المعلومات وأمن المعلومات

مقدمة

إدارة تكنولوجيا المعلومات وأمن المعلومات تعد من الأجزاء الحيوية في أي مؤسسة، حيث تؤثر بشكل مباشر على استمرارية العمل وسرية البيانات وسلامة الأنظمة. تتضمن هذه الإدارة الحفاظ على أمن وسلامة الأنظمة، والامتثال للمعايير واللوائح، والتأكد من الجاهزية في مواجهة المخاطر المحتملة.

تعريف المخاطر في إدارة تكنولوجيا المعلومات وأمن المعلومات

المخاطر تشمل مجموعة من التهديدات التي يمكن أن تؤثر على أنظمة المعلومات، مثل الهجمات السيبرانية، والفيروسات، والأعطال التقنية، وعدم الامتثال للمعايير. هذه المخاطر قد تؤدي إلى فقدان البيانات، تعطيل العمليات، أو تحمل تكاليف إضافية للتعافي.

دور الرقابة الداخلية في إدارة المخاطر

الرقابة الداخلية تشمل وضع سياسات وإجراءات لتحسين الأمان، التقييم المستمر للمخاطر، والاستجابة الفعالة للحوادث. تتضمن أيضًا التدريب المستمر للموظفين واستخدام أدوات أمان متقدمة لضمان حماية الأنظمة.

نظرة عامة على COSO ERM وISO 31000

يوفر **COSO ERM** إطارًا لإدارة المخاطر بشكل شامل ومتكامل عبر المؤسسة، بينما يقدم **ISO 31000** إرشادات ومبادئ لإدارة المخاطر، مما يساعد في تحديد وتقييم وإدارة المخاطر بشكل فعال.

فوائد استخدام COSO ERM وISO 31000

تطبيق هذه الأطر يساعد المؤسسات على تعزيز الشفافية، الامتثال للمعايير، وتحسين الاستجابة للمخاطر، مما يسهم في تحسين أداء الأنظمة وتقليل المخاطر المحتملة.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
1	فشل النظام الأساسي	تكنولوجي	الفشل في النظام الأساسي أو البرامج الحيوية المستخدمة في العمليات اليومية بسبب الأعطال الفنية أو أخطاء البرمجة.	• إجراء اختبارات نظامية شاملة بشكل دوري لتحديد أي نقاط ضعف. • تنفيذ خطط استعادة الطوارئ والنسخ الاحتياطية بشكل منتظم. • تقديم تدريبات دورية للفريق التقني على إدارة الطوارئ الفنية.	قسم تكنولوجيا المعلومات	مدير تكنولوجيا المعلومات	تشغيل خطة الطوارئ على الفور لتقليل التعطل.	تحليل الأسباب الجذرية للفشل وتحديث خطط الاستجابة.	تحسين استقرار النظام من خلال إجراءات استباقية للصيانة وتحديث البرمجيات.
2	اختراق الأمان السيبراني	أمني	تعرض الأنظمة لاختراق أمني يؤدي إلى فقدان البيانات أو سرقتها، مما يسبب ضررًا ماليًا وسمعيًا للمؤسسة.	• تطبيق تقنيات الجدار الناري المتقدمة وأنظمة كشف التسلل. • إجراء تقييمات أمنية دورية واختبارات الاختراق. • تعزيز الوعي الأمني بين الموظفين من خلال التدريبات المنتظمة.	قسم الأمن السيبراني	مدير الأمن السيبراني	عزل الأنظمة المتأثرة وإبلاغ الفرق الأمنية للتحقيق في الاختراق.	تحديث بروتوكولات الأمان وتطبيق تصحيحات البرمجيات بسرعة.	تعزيز أنظمة الأمان لتجنب الاختراقات المستقبلية.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
3	فقدان البيانات بسبب أعطال التخزين	تكنولوجي	فقدان البيانات الهامة نتيجة أعطال في أجهزة التخزين أو فشل البرمجيات.	• تنفيذ سياسة نسخ احتياطي يومية للبيانات الهامة. • استخدام أنظمة تخزين عالية الاعتمادية مع ميزات التكرار. • إجراء اختبارات استعادة البيانات بانتظام لضمان الفعالية.	قسم تكنولوجيا المعلومات	مدير تخزين البيانات	استعادة البيانات من النسخ الاحتياطية في أسرع وقت ممكن.	تحليل أسباب الفشل وتطوير استراتيجيات لتحسين استمرارية العمل.	تعزيز تدابير حماية البيانات من خلال خطط الطوارئ والتكرار.
4	نقص في سياسات الوصول والتحكم	أمني	غياب سياسات واضحة للتحكم في الوصول إلى الأنظمة، مما يزيد من احتمالية الوصول غير المصرح به للبيانات الحساسة.	• وضع سياسات وصول صارمة تعتمد على أدوار المستخدمين. • تنفيذ تقنيات التحقق متعدد العوامل لتعزيز الأمان. • إجراء تدقيقات وصول دورية لتحديد أي نقاط ضعف محتملة.	قسم الأمن السيبراني	مدير الأمن السيبراني	مراجعة وصول المستخدمين وإزالة أي وصول غير ضروري أو غير مبرر.	تحديث سياسات الوصول وتدريب الموظفين على أهميتها.	تحسين الأمان من خلال سياسات وصول محكمة ومراقبة دورية.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
5	نقص التحديثات الأمنية	تكنولوجي	عدم تطبيق التحديثات الأمنية بانتظام، مما يجعل الأنظمة عرضة للهجمات السيبرانية.	• إعداد جدول زمني منتظم لتحديث البرمجيات وتطبيق التصحيحات الأمنية. • إجراء فحوصات دورية للأنظمة للكشف عن الثغرات الأمنية. • تقديم تدريبات توعية للموظفين حول أهمية التحديثات الأمنية.	قسم تكنولوجيا المعلومات	مدير تكنولوجيا المعلومات	تطبيق التحديثات الأمنية الفورية في حالة الكشف عن ثغرة.	تحليل أسباب التأخير في التحديث وتحسين العمليات لضمان التحديث المستمر.	تعزيز أمان الأنظمة من خلال تحديثات أمنية منتظمة.
6	نقص التدريب على الأمن السيبراني	أمني	نقص التدريب على الأمن السيبراني، مما يزيد من احتمالية وقوع هجمات سيبرانية ناجحة بسبب ضعف الوعي الأمني.	• تطوير برامج تدريبية شاملة للأمن السيبراني لجميع الموظفين. • إجراء تدريبات توعوية دورية حول التهديدات السيبرانية وكيفية الوقاية منها. • تقديم دعم مستمر من خلال فرق متخصصة في الأمن السيبراني.	قسم الأمن السيبراني	مدير الأمن السيبراني	إطلاق برامج تدريبية فورية لتعزيز الوعي بالأمن السيبراني.	تحليل فعالية البرامج التدريبية وتحديثها بانتظام بناءً على المستجدات.	زيادة الوعي الأمني وتقليل احتمالية الهجمات السيبرانية من خلال تدريب فعال.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
7	نقص النسخ الاحتياطية للبيانات	تكنولوجي	عدم وجود نسخ احتياطية كافية للبيانات، مما يزيد من خطر فقدان البيانات في حالة حدوث أعطال.	• إعداد جدول زمني منتظم للنسخ الاحتياطي للبيانات الهامة. • استخدام تقنيات النسخ الاحتياطي التلقائي لضمان الحفظ الدوري. • إجراء اختبارات دورية للتحقق من سلامة النسخ الاحتياطية.	قسم تكنولوجيا المعلومات	مدير تخزين البيانات	إجراء نسخ احتياطي فوري للبيانات المتأثرة واستعادة النسخ عند الحاجة.	تحليل أسباب نقص النسخ الاحتياطية وتحسين العملية لضمان استمرارية العمل.	زيادة استمرارية العمل وحماية البيانات من خلال نسخ احتياطية منتظمة وآمنة.
8	نقص التحكم في الأجهزة المتصلة بالشبكة	أمني	نقص التحكم في الأجهزة المتصلة بالشبكة، مما يزيد من خطر الاختراقات الأمنية.	• تطوير سياسات صارمة للتحكم في الأجهزة المتصلة بالشبكة. • إجراء تدقيقات دورية للأجهزة المتصلة للتحقق من الامتثال للسياسات. • استخدام تقنيات أمان متقدمة لتقييد الوصول إلى الشبكة.	قسم الأمن السيبراني	مدير الأمن السيبراني	إجراء تحقيق فوري في حالة وجود أجهزة غير معروفة أو غير معتمدة واتخاذ الإجراءات اللازمة.	تحليل سياسات التحكم في الأجهزة وتحديثها لتعزيز الأمان والامتثال.	تحسين أمان الشبكة وتقليل المخاطر من خلال سياسات تحكم محكمة وتدقيقات منتظمة.
9	عدم الامتثال لمعايير حماية البيانات	امتثال	عدم الامتثال لمعايير حماية البيانات المحلية والدولية، مما	• تطوير سياسات حماية البيانات	قسم الشؤون القانونية	المستشار القانوني	إجراء تحقيق فوري لمعالجة أي قضايا غير متوافقة	تحليل الامتثال بانتظام وتحديث السياسات	تحقيق الامتثال الكامل لمعايير حماية البيانات لتجنب

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
			يؤدي إلى عقوبات قانونية.	تلتزم بالمعايير المحلية والدولية. • إجراء تدقيقات دورية للتحقق من الامتثال للمعايير. • تقديم تدريبات منتظمة للموظفين حول متطلبات الامتثال وكيفية تحقيقه.			والتواصل مع الجهات القانونية المختصة.	لتجنب العقوبات القانونية.	المخاطر القانونية.
10	نقص الاستثمار في البنية التحتية لتكنولوجيا المعلومات	استراتيجي	نقص الاستثمار في البنية التحتية لتكنولوجيا المعلومات، مما يؤدي إلى ضعف الأداء وعدم القدرة على مواكبة التطورات التكنولوجية.	• تطوير خطة استثمار شاملة لتحديث البنية التحتية لتكنولوجيا المعلومات. • إجراء تقييمات دورية لأداء البنية التحتية وتحديد المجالات التي تحتاج إلى تحسين. • تقديم تقارير مفصلة للإدارة العليا حول الحاجة إلى الاستثمار في البنية التحتية.	قسم تكنولوجيا المعلومات	مدير تكنولوجيا المعلومات	إجراء تقييم فوري للبنية التحتية وتحديد الأولويات للاستثمار المستقبلي.	تحليل الأداء بانتظام وتحديث الخطة الاستثمارية بناءً على الاحتياجات التقنية والتنظيمية.	تحسين الأداء وزيادة الكفاءة من خلال استثمار مناسب في البنية التحتية لتكنولوجيا المعلومات.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
11	نقص التحكم في التغييرات البرمجية	تكنولوجي	نقص التحكم في التغييرات البرمجية، مما يؤدي إلى إدخال أخطاء برمجية أو ثغرات أمنية.	• تطوير إجراءات صارمة للتحكم في التغييرات البرمجية تشمل جميع مراحل التطوير. • إجراء مراجعات دورية للتغييرات البرمجية من قبل فريق متخصص. • تقديم تدريب للموظفين حول كيفية تنفيذ التغييرات البرمجية بشكل آمن وفعال.	قسم تكنولوجيا المعلومات	مدير التطوير البرمجي	إجراء مراجعة فورية للتغييرات البرمجية المتأثرة وتحليل الأسباب وتطبيق التصحيحات.	تحليل أسباب نقص التحكم وتحديث الإجراءات لضمان التوافق مع المعايير الأمنية.	تحسين أمان البرمجيات وتقليل الأخطاء من خلال إجراءات صارمة ومراجعات منتظمة.
12	نقص في خطط الاستجابة لحوادث الأمن السيبراني	أمني	نقص في خطط الاستجابة لحوادث الأمن السيبراني، مما يؤدي إلى زيادة الوقت اللازم لاستعادة الأنظمة.	• تطوير خطط استجابة شاملة لحوادث الأمن السيبراني تشمل جميع السيناريوهات المحتملة. • إجراء تدريبات محاكاة لحوادث الأمن السيبراني لتحسين الجاهزية. • تقديم دعم مستمر للفرق المعنية من خلال فرق	قسم الأمن السيبراني	مدير الأمن السيبراني	تفعيل خطط الاستجابة فوراً عند وقوع حادث أمني وتحليل الحادث لتحسين الجاهزية.	تحليل فعالية خطط الاستجابة بانتظام وتحديثها بناءً على الدروس المستفادة.	تحسين الجاهزية وتقليل الوقت اللازم لاستعادة الأنظمة من خلال خطط استجابة فعالة وتدريبات مستمرة.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
				متخصصة في الاستجابة للحوادث.					
13	فشل في إدارة الأصول التكنولوجية	عملياتي	فشل في إدارة الأصول التكنولوجية، مما يؤدي إلى زيادة التكاليف وصعوبة تتبع الأجهزة والبرمجيات.	• تطوير نظام شامل لإدارة الأصول التكنولوجية يشمل جميع الأجهزة والبرمجيات. • إجراء مراجعات دورية للأصول للتحقق من سلامتها وتحديثها عند الحاجة. • تقديم تدريب للموظفين حول كيفية إدارة الأصول التكنولوجية بشكل فعال.	قسم تكنولوجيا المعلومات	مدير الأصول التكنولوجية	إجراء جرد فوري للأصول المتأثرة وتحليل الأسباب لتحسين الإدارة.	تحليل نظام إدارة الأصول بانتظام وتحديثه لضمان الكفاءة والدقة في التتبع.	تحسين إدارة الأصول التكنولوجية وتقليل التكاليف من خلال نظام فعال ومراجعات دورية.
14	نقص في الوعي بالتطبيقات غير المعتمدة	أمني	نقص في الوعي بالتطبيقات غير المعتمدة التي قد تسبب ثغرات أمنية أو تؤثر على الأداء.	• تطوير سياسة واضحة لتحديد وحظر التطبيقات غير المعتمدة. • إجراء تدقيقات دورية للتطبيقات المثبتة على الأجهزة للكشف	قسم الأمن السيبراني	مدير الأمن السيبراني	إزالة التطبيقات غير المعتمدة فوراً من الأجهزة المتأثرة وتحليل الأسباب لمنع تكرار الحوادث.	تحليل فعالية السياسة الحالية وتحديثها لتعزيز الوعي والتوافق.	تحسين أمان الأجهزة وتقليل المخاطر من خلال حظر التطبيقات غير المعتمدة وتدقيقات منتظمة.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
				عن التطبيقات غير المعتمدة. • تقديم تدريب للموظفين حول المخاطر المرتبطة بالتطبيقات غير المعتمدة.					
15	نقص في إدارة الحقوق الرقمية	أمني	نقص في إدارة الحقوق الرقمية، مما يؤدي إلى الاستخدام غير القانوني للبرمجيات والموارد الرقمية.	• تطوير نظام شامل لإدارة الحقوق الرقمية يشمل جميع البرمجيات والموارد الرقمية. • إجراء تدقيقات دورية للتحقق من الامتثال لقوانين حقوق الملكية الرقمية. • تقديم تدريب للموظفين حول أهمية الامتثال لقوانين حقوق الملكية الرقمية وكيفية تحقيقه.	قسم تكنولوجيا المعلومات	مدير تكنولوجيا المعلومات	تحليل النظام الحالي لإدارة الحقوق الرقمية وتحديثه لتعزيز الامتثال.	إجراء مراجعات دورية لضمان التزام البرمجيات والموارد الرقمية بقوانين الحقوق الرقمية.	تحقيق الامتثال الكامل لقوانين الحقوق الرقمية من خلال نظام فعال وتدقيقات منتظمة.
16	عدم وجود خطط لاستمرارية الأعمال في	استراتيجي	عدم وجود خطط لاستمرارية الأعمال في حالات	• تطوير خطط شاملة لاستمرارية	قسم تكنولوجيا المعلومات	مدير الطوارئ والاستجابة	تفعيل خطط استمرارية الأعمال فوراً عند وقوع	تحليل فعالية خطط الاستمرارية بانتظام	تحسين الجاهزية وتقليل تأثير الطوارئ على

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
	حالات الطوارئ		الطوارئ، مما يعرض الأعمال للخطر في حالة حدوث كوارث.	الأعمال تشمل جميع السيناريوهات الطارئة. • إجراء تدريبات محاكاة للطوارئ لتحسين الجاهزية. • تقديم دعم مستمر للفرق المعنية من خلال فرق متخصصة في إدارة الأزمات.			طارئ وتحليل الأداء لتحسين الجاهزية.	وتحديثها بناءً على الدروس المستفادة.	الأعمال من خلال خطط استمرارية فعالة وتدريبات مستمرة.
17	نقص التحكم في الوصول عن بعد	أمني	نقص التحكم في الوصول عن بعد، مما يزيد من خطر الاختراقات الأمنية.	• تطوير سياسات صارمة للتحكم في الوصول عن بعد تشمل جميع المتغيرات الأمنية. • إجراء تدقيقات دورية للتحقق من الامتثال لسياسات الوصول عن بعد. • استخدام تقنيات أمان متقدمة مثل التحقق الثنائي لتعزيز أمان الوصول.	قسم الأمن السيبراني	مدير الأمن السيبراني	إجراء تحقيق فوري في حالة وجود وصول غير معتمد عن بعد واتخاذ الإجراءات اللازمة لمنعها.	تحليل سياسات الوصول عن بعد وتحديثها لتعزيز الأمان والامتثال.	تحسين أمان الوصول عن بعد وتقليل المخاطر من خلال سياسات تحكم محكمة وتدقيقات منتظمة.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
18	عدم وجود نظام لمراقبة الأنشطة الشبكية	أمني	عدم وجود نظام لمراقبة الأنشطة الشبكية، مما يزيد من خطر الاختراقات الأمنية والهجمات السيبرانية.	• تطوير نظام شامل لمراقبة الأنشطة الشبكية يشمل جميع المتغيرات الأمنية. • إجراء تدقيقات دورية للأنشطة الشبكية للتحقق من الامتثال للسياسات. • استخدام تقنيات أمان متقدمة لتقييد الوصول إلى الشبكة.	قسم الأمن السيبراني	مدير الأمن السيبراني	إجراء تحقيق فوري في حالة وجود أنشطة غير معروفة أو غير معتمدة واتخاذ الإجراءات اللازمة.	تحليل سياسات مراقبة الأنشطة الشبكية وتحديثها لتعزيز الأمان والامتثال.	تحسين أمان الشبكة وتقليل المخاطر من خلال نظام مراقبة فعال وتدقيقات منتظمة.
19	عدم وجود سياسات واضحة لإدارة الهوية والوصول	أمني	غياب سياسات واضحة لإدارة الهوية والوصول، مما يسمح بإمكانية الوصول غير المصرح به للأنظمة والبيانات.	• وضع سياسات صارمة لإدارة الهوية والوصول تحدد مستويات الوصول بناءً على الأدوار الوظيفية. • تطبيق تقنيات التحقق متعدد العوامل لتعزيز الأمان. • إجراء تدقيقات دورية للتحقق من الالتزام بسياسات إدارة	قسم الأمن السيبراني	مدير الأمن السيبراني	إجراء مراجعة فورية لجميع حسابات الوصول والتحقق من صلاحياتها وتحديثها عند الحاجة.	تحديث سياسات إدارة الهوية والوصول بناءً على نتائج التدقيق لتعزيز الأمان والامتثال.	تحسين أمان الأنظمة وتقليل المخاطر من خلال إدارة فعالة للهوية والوصول.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
				الهوية والوصول.					
20	نقص في التوثيق والإجراءات التشغيلية	عملياتي	عدم توثيق السياسات والإجراءات التشغيلية بشكل كافٍ، مما يؤدي إلى أخطاء في تنفيذ العمليات وعدم اتساق الأداء.	• إنشاء دليل شامل للإجراءات التشغيلية يتضمن جميع السياسات والعمليات. • تحديث التوثيق بشكل دوري لضمان دقة المعلومات. • إجراء تدريبات للموظفين على الإجراءات التشغيلية المتبعة.	قسم العمليات	مدير العمليات	مراجعة الوثائق التشغيلية وتحديثها عند الحاجة.	تحليل العمليات بشكل دوري لضمان التزام الجميع بالإجراءات المتبعة.	تحسين الكفاءة وتقليل الأخطاء من خلال توثيق شامل ومحدث للإجراءات التشغيلية.
21	عدم وجود خطة لإدارة التحديثات البرمجية	تكنولوجي	عدم وجود خطة واضحة لإدارة التحديثات البرمجية يؤدي إلى تأخر التحديثات وتعرض الأنظمة للثغرات الأمنية.	• تطوير خطة شاملة لإدارة التحديثات البرمجية تشمل جميع الأنظمة والبرمجيات. • تحديد مواعيد دورية لإجراء التحديثات واختبارها. • تقديم تقارير دورية للإدارة حول حالة	قسم تكنولوجيا المعلومات	مدير النظام	تطبيق التحديثات الفورية على الأنظمة المتأثرة وتحليل أسباب التأخير.	تحليل فعالية خطة التحديث وتحديثها بناءً على نتائج المراجعات.	تحسين أمان الأنظمة وتقليل وقت التعطل من خلال إدارة فعالة للتحديثات البرمجية.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
				التحديثات البرمجية.					
22	نقص في مراقبة أداء الأنظمة	عملياتي	عدم وجود نظام فعال لمراقبة أداء الأنظمة يؤدي إلى تأخير في اكتشاف المشكلات والأعطال.	• تطوير نظام شامل لمراقبة أداء الأنظمة يتضمن مؤشرات أداء رئيسية. • إجراء مراجعات دورية لتحليل أداء الأنظمة وتحديد المشكلات المحتملة. • تقديم تقارير دورية للإدارة حول أداء الأنظمة.	قسم تكنولوجيا المعلومات	مدير تكنولوجيا المعلومات	إجراء تحقيق فوري في حالة اكتشاف تدهور في الأداء واتخاذ الإجراءات اللازمة.	تحليل أداء الأنظمة بشكل دوري وتحديث نظام المراقبة لضمان الكفاءة.	تحسين استقرار الأنظمة وتقليل وقت التعطل من خلال مراقبة فعالة للأداء.
23	عدم وجود سياسة لتأمين البريد الإلكتروني	أمني	عدم وجود سياسة لتأمين البريد الإلكتروني يؤدي إلى خطر الهجمات السيبرانية مثل التصيد الاحتيالي والبرمجيات الخبيثة.	• تطوير سياسة شاملة لتأمين البريد الإلكتروني تشمل إجراءات تصفية البريد والتصدي لهجمات التصيد الاحتيالي. • تنفيذ تقنيات الأمان المتقدمة مثل DMARC	قسم الأمن السيبراني	مدير الأمن السيبراني	عزل البريد الإلكتروني المشبوه والتحقيق في الحادث.	تحليل الحوادث بانتظام وتحديث سياسة تأمين البريد الإلكتروني لتعزيز الأمان.	تحسين أمان البريد الإلكتروني وتقليل الهجمات السيبرانية من خلال سياسة شاملة وتدريبات توعوية.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
				• تقديم تدريبات توعوية للموظفين حول تهديدات البريد الإلكتروني وكيفية التعرف عليها. وSPF وDKIM.					
24	نقص في إدارة استمرارية الأعمال	استراتيجي	نقص في إدارة استمرارية الأعمال، مما يعرض المؤسسة للخطر في حالة الكوارث الطبيعية أو الهجمات السيبرانية.	• تطوير خطط استمرارية الأعمال تشمل جميع السيناريوهات الطارئة المحتملة. • إجراء تدريبات محاكاة للطوارئ لتحسين الجاهزية. • تقديم دعم مستمر للفرق المعنية من خلال فرق متخصصة في إدارة الأزمات.	قسم تكنولوجيا المعلومات	مدير الطوارئ والاستجابة	تفعيل خطط استمرارية الأعمال فوراً عند وقوع طارئ وتحليل الأداء لتحسين الجاهزية.	تحليل فعالية خطط الاستمرارية بانتظام وتحديثها بناءً على الدروس المستفادة.	تحسين الجاهزية وتقليل تأثير الطوارئ على الأعمال من خلال خطط استمرارية فعالة وتدريبات مستمرة.
25	نقص في إدارة الهوية والوصول	أمني	نقص في إدارة الهوية والوصول، مما يؤدي إلى خطر الوصول غير	• تطوير نظام شامل لإدارة الهوية والوصول يشمل جميع	قسم الأمن السيبراني	مدير الأمن السيبراني	إجراء مراجعة فورية لجميع حسابات الوصول والتحقق من	تحليل سياسات إدارة الهوية والوصول بانتظام وتحديثها	تحسين أمان الأنظمة وتقليل المخاطر من خلال إدارة

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
			المصرح به إلى الأنظمة والبيانات الحساسة.	المستخدمين والأدوار. • تطبيق تقنيات التحقق متعدد العوامل لتعزيز الأمان. • إجراء تدقيقات دورية للتحقق من الامتثال لسياسات إدارة الهوية والوصول.			صلاحياتها وتحديثها عند الحاجة.	لتعزيز الأمان والامتثال.	فعالة للهوية والوصول.
26	نقص في خطط النسخ الاحتياطي والاستعادة	تكنولوجي	نقص في خطط النسخ الاحتياطي والاستعادة، مما يؤدي إلى خطر فقدان البيانات في حالة الأعطال أو الهجمات السيبرانية.	• تطوير خطط نسخ احتياطي واستعادة شاملة تشمل جميع البيانات الهامة. • تنفيذ تقنيات النسخ الاحتياطي التلقائي لضمان الحفظ الدوري. • إجراء اختبارات دورية للتحقق من سلامة النسخ الاحتياطية واستعادتها.	قسم تكنولوجيا المعلومات	مدير تخزين البيانات	إجراء نسخ احتياطي فوري للبيانات المتأثرة واستعادة النسخ عند الحاجة.	تحليل أسباب نقص النسخ الاحتياطية وتحسين العملية لضمان استمرارية العمل.	زيادة استمرارية العمل وحماية البيانات من خلال نسخ احتياطية منتظمة وآمنة.
27	عدم الامتثال لمتطلبات اللوائح والأنظمة	امتثال	عدم الامتثال لمتطلبات اللوائح والأنظمة المحلية والدولية، مما	• تطوير سياسات وإجراءات تلتزم	قسم الشؤون القانونية	المستشار القانوني	إجراء تحقيق فوري لمعالجة أي قضايا غير متوافقة	تحليل الامتثال بانتظام وتحديث السياسات	تحقيق الامتثال الكامل لمتطلبات اللوائح

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
			يؤدي إلى عقوبات قانونية ومالية.	باللوائح والأنظمة المحلية والدولية. • إجراء تدقيقات دورية للتحقق من الامتثال للمتطلبات القانونية. • تقديم تدريبات منتظمة للموظفين حول متطلبات الامتثال وكيفية تحقيقها.			والتواصل مع الجهات القانونية المختصة.	لتجنب العقوبات القانونية.	والأنظمة لتجنب المخاطر القانونية.
28	نقص في تأمين الأجهزة المحمولة	أمني	نقص في تأمين الأجهزة المحمولة مثل الهواتف الذكية والأجهزة اللوحية، مما يعرض البيانات الحساسة لخطر السرقة أو الفقدان.	• تطوير سياسات صارمة لتأمين الأجهزة المحمولة تشمل تشفير البيانات وحماية كلمة المرور. • إجراء تدقيقات دورية للأجهزة المحمولة للتحقق من الامتثال للسياسات. • تقديم تدريبات توعوية للموظفين حول أهمية تأمين الأجهزة المحمولة وكيفية تحقيقه.	قسم الأمن السيبراني	مدير الأمن السيبراني	عزل الأجهزة المفقودة أو المسروقة وتعطيل الوصول إليها فوراً.	تحليل حوادث الأجهزة المحمولة بانتظام وتحديث السياسات لتعزيز الأمان.	تحسين أمان الأجهزة المحمولة وتقليل المخاطر من خلال سياسات تحكم محكمة وتدقيقات منتظمة.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
29	عدم وجود سياسة لتأمين الشبكة اللاسلكية	أمني	عدم وجود سياسة لتأمين الشبكة اللاسلكية، مما يعرض الشبكة لخطر الاختراقات والهجمات السيبرانية.	• تطوير سياسة شاملة لتأمين الشبكة اللاسلكية تشمل إجراءات التشفير والمصادقة. • تنفيذ تقنيات الأمان المتقدمة مثل WPA3 وتصفية MAC. • إجراء تدقيقات دورية للشبكة اللاسلكية للتحقق من الامتثال للسياسات.	قسم الأمن السيبراني	مدير الأمن السيبراني	إجراء تحقيق فوري في حالة وجود نشاط غير معتمد على الشبكة اللاسلكية واتخاذ الإجراءات اللازمة.	تحليل فعالية السياسة الحالية وتحديثها لتعزيز أمان الشبكة اللاسلكية.	تحسين أمان الشبكة اللاسلكية وتقليل المخاطر من خلال سياسة شاملة وتدقيقات منتظمة.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
30	عدم وجود نظام لتحديث الأنظمة التلقائي	تكنولوجي	عدم وجود نظام لتحديث الأنظمة التلقائي يؤدي إلى تأخير التحديثات وتعريض الأنظمة للثغرات الأمنية.	• تطوير نظام شامل لتحديث الأنظمة التلقائي يشمل جميع البرمجيات والتطبيقات. • تحديد مواعيد دورية لإجراء التحديثات التلقائية واختبارها. • تقديم تقارير دورية للإدارة حول حالة التحديثات التلقائية.	قسم تكنولوجيا المعلومات	مدير النظام	تطبيق التحديثات الفورية على الأنظمة المتأثرة وتحليل أسباب التأخير.	تحليل فعالية نظام التحديث التلقائي وتحديثه بناءً على نتائج المراجعات.	تحسين أمان الأنظمة وتقليل وقت التعطل من خلال تحديثات تلقائية منتظمة.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
31	نقص في مراقبة حركة البيانات	أمني	نقص في مراقبة حركة البيانات عبر الشبكة يؤدي إلى عدم الكشف عن الأنشطة غير المشروعة أو المحاولات الاختراقية.	• تطوير نظام شامل لمراقبة حركة البيانات يتضمن أدوات تحليل الشبكة. • إجراء تدقيقات دورية لحركة البيانات للتحقق من الامتثال للسياسات. • استخدام تقنيات الأمان المتقدمة لتحديد ومنع الأنشطة غير المصرح بها.	قسم الأمن السيبراني	مدير الأمن السيبراني	إجراء تحقيق فوري في حالة وجود حركة بيانات غير معتادة واتخاذ الإجراءات اللازمة.	تحليل فعالية نظام مراقبة حركة البيانات وتحديثه لتعزيز الأمان والامتثال.	تحسين أمان الشبكة وتقليل المخاطر من خلال مراقبة فعالة لحركة البيانات وتدقيقات منتظمة.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
32	نقص في إدارة مخاطر سلسلة التوريد	استراتيجي	نقص في إدارة مخاطر سلسلة التوريد يؤدي إلى عدم التوريد في الوقت المناسب أو توريد مكونات غير آمنة.	• تطوير نظام شامل لإدارة مخاطر سلسلة التوريد يشمل جميع الموردين والشركاء. • إجراء تدقيقات دورية للتحقق من الامتثال لمعايير الجودة والأمان. • تقديم تدريبات للشركاء والموردين حول متطلبات الأمان وكيفية تحقيقها.	قسم المشتريات	مدير المشتريات	إجراء مراجعة فورية للعقود والشراكات المتأثرة واتخاذ الإجراءات اللازمة.	تحليل فعالية نظام إدارة مخاطر سلسلة التوريد وتحديثه لضمان الكفاءة.	تحسين استمرارية العمل وتقليل المخاطر من خلال إدارة فعالة لمخاطر سلسلة التوريد.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
33	نقص في التوثيق الرقمي	عملياتي	نقص في التوثيق الرقمي يؤدي إلى فقدان البيانات الهامة أو عدم القدرة على استرجاع المعلومات بشكل فعال.	• تطوير نظام شامل للتوثيق الرقمي يشمل جميع أنواع البيانات الهامة. • إجراء مراجعات دورية للتوثيق الرقمي لضمان دقة المعلومات وسلامتها. • تقديم تدريبات للموظفين حول كيفية استخدام النظام بشكل فعال.	قسم تكنولوجيا المعلومات	مدير تكنولوجيا المعلومات	إجراء مراجعة فورية للتوثيق الرقمي المتأثر وتحليل الأسباب لتحسين الإدارة.	تحليل فعالية نظام التوثيق الرقمي وتحديثه بناءً على نتائج المراجعات.	تحسين الكفاءة وتقليل الأخطاء من خلال توثيق رقمي شامل ومحدث.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
34	نقص في إدارة الأصول الرقمية	تكنولوجي	نقص في إدارة الأصول الرقمية يؤدي إلى فقدان الأصول الرقمية أو استخدامها بشكل غير فعال.	• تطوير نظام شامل لإدارة الأصول الرقمية يشمل جميع الأجهزة والبرمجيات. • إجراء مراجعات دورية للأصول للتحقق من سلامتها وتحديثها عند الحاجة. • تقديم تدريب للموظفين حول كيفية إدارة الأصول الرقمية بشكل فعال.	قسم تكنولوجيا المعلومات	مدير الأصول الرقمية	إجراء جرد فوري للأصول المتأثرة وتحليل الأسباب لتحسين الإدارة.	تحليل نظام إدارة الأصول الرقمية بانتظام وتحديثه لضمان الكفاءة والدقة في التتبع.	تحسين إدارة الأصول الرقمية وتقليل التكاليف من خلال نظام فعال ومراجعات دورية.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
35	عدم وجود نظام لإدارة الطوارئ	استراتيجي	عدم وجود نظام لإدارة الطوارئ يؤدي إلى عدم الجاهزية في حالة وقوع كوارث أو أزمات.	• تطوير نظام شامل لإدارة الطوارئ يشمل جميع السيناريوهات المحتملة. • إجراء تدريبات محاكاة للطوارئ لتحسين الجاهزية. • تقديم دعم مستمر للفرق المعنية من خلال فرق متخصصة في إدارة الأزمات.	قسم الطوارئ والاستجابة	مدير الطوارئ والاستجابة	تفعيل نظام إدارة الطوارئ فوراً عند وقوع أزمة وتحليل الأداء لتحسين الجاهزية.	تحليل فعالية نظام إدارة الطوارئ بانتظام وتحديثه بناءً على الدروس المستفادة.	تحسين الجاهزية وتقليل تأثير الطوارئ على الأعمال من خلال نظام إدارة طوارئ فعال وتدريبات مستمرة.
36	نقص في إدارة المخاطر البيئية	استراتيجي	نقص في إدارة المخاطر البيئية يؤدي إلى عدم الامتثال للوائح البيئية وزيادة المخاطر القانونية والمالية.	• تطوير نظام شامل لإدارة المخاطر البيئية يشمل جميع الأنشطة البيئية. • إجراء تدقيقات دورية للتحقق من الامتثال للوائح البيئية. • تقديم تدريبات للموظفين حول متطلبات الامتثال البيئي وكيفية تحقيقها.	قسم البيئة	مدير البيئة	إجراء تحقيق فوري في حالة وجود انتهاكات بيئية واتخاذ الإجراءات اللازمة.	تحليل فعالية نظام إدارة المخاطر البيئية وتحديثه لضمان الامتثال والكفاءة.	تحسين الامتثال البيئي وتقليل المخاطر من خلال نظام إدارة فعال وتدقيقات منتظمة.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
37	نقص في تأمين التطبيقات السحابية	أمني	نقص في تأمين التطبيقات السحابية يؤدي إلى خطر الوصول غير المصرح به إلى البيانات الحساسة.	• تطوير سياسة شاملة لتأمين التطبيقات السحابية تشمل إجراءات التشفير والمصادقة. • تنفيذ تقنيات الأمان المتقدمة مثل IAM وتصفية البيانات. • إجراء تدقيقات دورية للتطبيقات السحابية للتحقق من الامتثال للسياسات.	قسم الأمن السيبراني	مدير الأمن السيبراني	إجراء تحقيق فوري في حالة وجود نشاط غير معتمد على التطبيقات السحابية واتخاذ الإجراءات اللازمة.	تحليل فعالية السياسة الحالية وتحديثها لتعزيز أمان التطبيقات السحابية.	تحسين أمان التطبيقات السحابية وتقليل المخاطر من خلال سياسة شاملة وتدقيقات منتظمة.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
38	نقص في إدارة العلاقات مع الموردين	عملياتي	نقص في إدارة العلاقات مع الموردين يؤدي إلى عدم القدرة على التوريد في الوقت المناسب وتدهور الجودة.	• تطوير نظام شامل لإدارة العلاقات مع الموردين يشمل جميع الموردين والشركاء. • إجراء تدقيقات دورية للتحقق من الامتثال لمعايير الجودة والأمان. • تقديم تدريبات للشركاء والموردين حول متطلبات الجودة وكيفية تحقيقها.	قسم المشتريات	مدير المشتريات	إجراء مراجعة فورية للعقود والشراكات المتأثرة واتخاذ الإجراءات اللازمة.	تحليل فعالية نظام إدارة العلاقات مع الموردين وتحديثه لضمان الكفاءة.	تحسين استمرارية العمل وتقليل المخاطر من خلال إدارة فعالة للعلاقات مع الموردين.
39	عدم وجود سياسة لتأمين الأجهزة المحمولة الشخصية	أمني	عدم وجود سياسة لتأمين الأجهزة المحمولة الشخصية يؤدي إلى خطر الوصول غير المصرح به إلى البيانات الحساسة.	• تطوير سياسة شاملة لتأمين الأجهزة المحمولة الشخصية تشمل إجراءات التشفير والمصادقة. • تنفيذ تقنيات الأمان المتقدمة مثل MDM وتصفية التطبيقات. • إجراء تدقيقات دورية للأجهزة المحمولة	قسم الأمن السيبراني	مدير الأمن السيبراني	إجراء تحقيق فوري في حالة وجود نشاط غير معتمد على الأجهزة المحمولة الشخصية واتخاذ الإجراءات اللازمة.	تحليل فعالية السياسة الحالية وتحديثها لتعزيز أمان الأجهزة المحمولة الشخصية.	تحسين أمان الأجهزة المحمولة الشخصية وتقليل المخاطر من خلال سياسة شاملة وتدقيقات منتظمة.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
				الشخصية للتحقق من الامتثال للسياسات.					
40	نقص في إدارة الموارد البشرية لتكنولوجيا المعلومات	عملياتي	نقص في إدارة الموارد البشرية لتكنولوجيا المعلومات يؤدي إلى نقص في المهارات والكفاءات اللازمة لإدارة الأنظمة بشكل فعال.	• تطوير نظام شامل لإدارة الموارد البشرية لتكنولوجيا المعلومات يشمل جميع الموظفين والمراكز. • إجراء تدقيقات دورية للتحقق من الامتثال لمعايير الجودة والأمان. • تقديم تدريبات للموظفين حول متطلبات الجودة وكيفية تحقيقها.	قسم الموارد البشرية	مدير الموارد البشرية	إجراء مراجعة فورية للموظفين المتأثرين وتحليل الأسباب لتحسين الإدارة.	تحليل فعالية نظام إدارة الموارد البشرية وتحديثه لضمان الكفاءة والدقة في التتبع.	تحسين إدارة الموارد البشرية وتقليل التكاليف من خلال نظام فعال ومراجعات دورية.
41	نقص في إدارة الوصول إلى البيانات الحساسة	أمني	نقص في إدارة الوصول إلى البيانات الحساسة يمكن أن يؤدي إلى تسرب البيانات والوصول غير المصرح به.	• تطوير سياسة صارمة لإدارة الوصول إلى البيانات الحساسة تحدد مستويات الوصول بناءً على الأدوار الوظيفية. • تطبيق تقنيات التحقق متعدد	قسم الأمن السيبراني	مدير الأمن السيبراني	إجراء تحقيق فوري في حالة وجود وصول غير معتمد إلى البيانات الحساسة واتخاذ الإجراءات اللازمة.	تحليل سياسات الوصول إلى البيانات الحساسة وتحديثها لتعزيز الأمان والامتثال.	تحسين أمان البيانات الحساسة وتقليل المخاطر من خلال إدارة فعالة للوصول وتدقيقات منتظمة.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
				العوامل للوصول إلى البيانات الحساسة. • إجراء تدقيقات دورية للتحقق من الالتزام بسياسات الوصول إلى البيانات.					
42	عدم وجود سياسة للتصدي للهجمات الفيروسية	أمني	عدم وجود سياسة للتصدي للهجمات الفيروسية يمكن أن يؤدي إلى انتشار البرمجيات الخبيثة داخل الأنظمة.	• تطوير سياسة شاملة للتصدي للهجمات الفيروسية تشمل استخدام برامج مكافحة الفيروسات وتحديثها بانتظام. • تنفيذ تقنيات الكشف عن البرمجيات الخبيثة وإزالة التهديدات المحتملة. • إجراء تدريبات توعوية للموظفين حول تهديدات الفيروسات وكيفية تجنبها.	قسم الأمن السيبراني	مدير الأمن السيبراني	إجراء فحص شامل للأنظمة المتأثرة وإزالة البرمجيات الخبيثة.	تحليل الحوادث الفيروسية بانتظام وتحديث سياسة التصدي لتعزيز الأمان.	تحسين أمان الأنظمة وتقليل الهجمات الفيروسية من خلال سياسة شاملة وتدقيقات منتظمة.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
43	عدم وجود نظام لإدارة التحديثات البرمجية التلقائية	تكنولوجي	عدم وجود نظام لإدارة التحديثات البرمجية التلقائية يؤدي إلى تأخير التحديثات وتعريض الأنظمة للثغرات الأمنية.	• تطوير نظام شامل لإدارة التحديثات البرمجية التلقائية يشمل جميع الأنظمة والبرمجيات. • تحديد مواعيد دورية لإجراء التحديثات التلقائية واختبارها. • تقديم تقارير دورية للإدارة حول حالة التحديثات البرمجية التلقائية.	قسم تكنولوجيا المعلومات	مدير النظام	تطبيق التحديثات الفورية على الأنظمة المتأثرة وتحليل أسباب التأخير.	تحليل فعالية نظام التحديث البرمجي التلقائي وتحديثه بناءً على نتائج المراجعات.	تحسين أمان الأنظمة وتقليل وقت التعطل من خلال تحديثات برمجية تلقائية منتظمة.
44	نقص في مراقبة أنشطة الشبكة	أمني	نقص في مراقبة أنشطة الشبكة يمكن أن يؤدي إلى عدم الكشف عن الأنشطة غير المصرح بها أو المحاولات الاختراقية.	• تطوير نظام شامل لمراقبة أنشطة الشبكة يتضمن أدوات تحليل الشبكة ومراقبة حركة البيانات. • إجراء تدقيقات دورية لأنشطة الشبكة للتحقق من الامتثال للسياسات.	قسم الأمن السيبراني	مدير الأمن السيبراني	إجراء تحقيق فوري في حالة وجود أنشطة غير معروفة أو غير معتمدة على الشبكة واتخاذ الإجراءات اللازمة.	تحليل سياسات مراقبة أنشطة الشبكة وتحديثها لتعزيز الأمان والامتثال.	تحسين أمان الشبكة وتقليل المخاطر من خلال نظام مراقبة فعال وتدقيقات منتظمة.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
				• استخدام تقنيات الأمان المتقدمة لتحديد ومنع الأنشطة غير المصرح بها.					
45	عدم وجود سياسات لإدارة المخاطر البيئية لتكنولوجيا المعلومات	استراتيجي	عدم وجود سياسات لإدارة المخاطر البيئية لتكنولوجيا المعلومات يمكن أن يؤدي إلى عدم الامتثال للوائح البيئية وزيادة المخاطر القانونية والمالية.	• تطوير سياسات شاملة لإدارة المخاطر البيئية لتكنولوجيا المعلومات تشمل جميع الأنشطة البيئية. • إجراء تدقيقات دورية للتحقق من الامتثال للوائح البيئية. • تقديم تدريبات للموظفين حول متطلبات الامتثال البيئي وكيفية تحقيقها.	قسم البيئة	مدير البيئة	إجراء تحقيق فوري في حالة وجود انتهاكات بيئية واتخاذ الإجراءات اللازمة.	تحليل فعالية سياسات إدارة المخاطر البيئية لتكنولوجيا المعلومات وتحديثها لضمان الامتثال والكفاءة.	تحسين الامتثال البيئي وتقليل المخاطر من خلال سياسات شاملة وتدقيقات منتظمة.
46	نقص في تأمين الهواتف الذكية المستخدمة للعمل	أمني	نقص في تأمين الهواتف الذكية المستخدمة للعمل يمكن أن يؤدي إلى تسرب البيانات والوصول غير المصرح به.	• تطوير سياسة شاملة لتأمين الهواتف الذكية تشمل إجراءات التشفير والمصادقة. • تنفيذ تقنيات الأمان المتقدمة	قسم الأمن السيبراني	مدير الأمن السيبراني	إجراء تحقيق فوري في حالة وجود نشاط غير معتمد على الهواتف الذكية واتخاذ الإجراءات اللازمة.	تحليل فعالية السياسة الحالية وتحديثها لتعزيز أمان الهواتف الذكية.	تحسين أمان الهواتف الذكية المستخدمة للعمل وتقليل المخاطر من خلال سياسة شاملة وتدقيقات منتظمة.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
				مثل MDM وتصفية التطبيقات. • إجراء تدقيقات دورية للهواتف الذكية المستخدمة للعمل للتحقق من الامتثال للسياسات.					
47	عدم وجود نظام لإدارة الأصول البرمجية	عملياتي	عدم وجود نظام لإدارة الأصول البرمجية يمكن أن يؤدي إلى فقدان التراخيص أو استخدام البرمجيات بشكل غير قانوني.	• تطوير نظام شامل لإدارة الأصول البرمجية يشمل جميع البرمجيات المستخدمة. • إجراء تدقيقات دورية للتحقق من الامتثال للتراخيص والقوانين المتعلقة بالبرمجيات. • تقديم تدريبات للموظفين حول أهمية الامتثال لقوانين البرمجيات وكيفية تحقيقه.	قسم تكنولوجيا المعلومات	مدير الأصول البرمجية	إجراء مراجعة فورية للأصول البرمجية المتأثرة وتحليل الأسباب لتحسين الإدارة.	تحليل نظام إدارة الأصول البرمجية بانتظام وتحديثه لضمان الكفاءة والامتثال.	تحسين إدارة الأصول البرمجية وتقليل التكاليف من خلال نظام فعال ومراجعات دورية.
48	نقص في تأمين التطبيقات	أمني	نقص في تأمين التطبيقات المستخدمة للعمل	• تطوير سياسة شاملة لتأمين	قسم الأمن السيبراني	مدير الأمن السيبراني	إجراء تحقيق فوري في حالة وجود نشاط غير	تحليل فعالية السياسة الحالية وتحديثها	تحسين أمان التطبيقات المستخدمة

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
	المستخدمة للعمل		يمكن أن يؤدي إلى تسرب البيانات والوصول غير المصرح به.	التطبيقات المستخدمة للعمل تشمل إجراءات التشفير والمصادقة. • تنفيذ تقنيات الأمان المتقدمة مثل IAM وتصفية البيانات. • إجراء تدقيقات دورية للتطبيقات المستخدمة للعمل للتحقق من الامتثال للسياسات.			معتمد على التطبيقات المستخدمة للعمل واتخاذ الإجراءات اللازمة.	لتعزيز أمان التطبيقات المستخدمة للعمل.	للعمل وتقليل المخاطر من خلال سياسة شاملة وتدقيقات منتظمة.
49	نقص في إدارة المخاطر الناتجة عن التعاقدات الخارجية	استراتيجي	نقص في إدارة المخاطر الناتجة عن التعاقدات الخارجية يمكن أن يؤدي إلى عدم الامتثال للمتطلبات التنظيمية أو المخاطر المالية.	• تطوير نظام شامل لإدارة المخاطر الناتجة عن التعاقدات الخارجية يشمل جميع المتعاقدين والشركاء. • إجراء تدقيقات دورية للتحقق من الامتثال للمتطلبات التنظيمية والجودة. • تقديم تدريبات للمتعاقدين والشركاء حول	قسم الشؤون القانونية	المستشار القانوني	إجراء مراجعة فورية للتعاقدات المتأثرة واتخاذ الإجراءات اللازمة لتحسين الامتثال.	تحليل فعالية نظام إدارة المخاطر الناتجة عن التعاقدات الخارجية وتحديثه لضمان الامتثال والكفاءة.	تحسين الامتثال وتقليل المخاطر من خلال نظام إدارة فعال للتعاقدات الخارجية وتدقيقات منتظمة.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
				متطلبات الامتثال وكيفية تحقيقها.					
50	عدم وجود سياسات واضحة لإدارة البيانات الكبيرة	تكنولوجي	عدم وجود سياسات واضحة لإدارة البيانات الكبيرة يمكن أن يؤدي إلى سوء إدارة البيانات وزيادة المخاطر التنظيمية.	• تطوير سياسات شاملة لإدارة البيانات الكبيرة تشمل إجراءات الحفظ والتحليل والاستخدام. • إجراء تدقيقات دورية للتحقق من الامتثال لسياسات إدارة البيانات الكبيرة. • تقديم تدريبات للموظفين حول متطلبات إدارة البيانات الكبيرة وكيفية تحقيقها.	قسم تكنولوجيا المعلومات	مدير البيانات الكبيرة	إجراء مراجعة فورية للبيانات الكبيرة المتأثرة وتحليل الأسباب لتحسين الإدارة.	تحليل فعالية سياسات إدارة البيانات الكبيرة بانتظام وتحديثها لضمان الكفاءة والامتثال.	تحسين إدارة البيانات الكبيرة وتقليل المخاطر من خلال سياسات شاملة وتدقيقات منتظمة.
51	نقص في إدارة مخاطر الحوسبة السحابية	أمني	نقص في إدارة مخاطر الحوسبة السحابية يمكن أن يؤدي إلى تسرب البيانات والوصول غير المصرح به.	• تطوير نظام شامل لإدارة مخاطر الحوسبة السحابية يشمل جميع التطبيقات والبيانات. • تنفيذ تقنيات الأمان المتقدمة مثل IAM وتصفية البيانات.	قسم الأمن السيبراني	مدير الأمن السيبراني	إجراء تحقيق فوري في حالة وجود نشاط غير معتمد على الحوسبة السحابية واتخاذ الإجراءات اللازمة.	تحليل فعالية نظام إدارة مخاطر الحوسبة السحابية وتحديثه لتعزيز الأمان والامتثال.	تحسين أمان الحوسبة السحابية وتقليل المخاطر من خلال نظام إدارة فعال وتدقيقات منتظمة.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
				• إجراء تدقيقات دورية للحوسبة السحابية للتحقق من الامتثال للسياسات.					
52	نقص في إدارة مخاطر تقنية المعلومات الناشئة	استراتيجي	نقص في إدارة مخاطر تقنية المعلومات الناشئة يمكن أن يؤدي إلى عدم الاستعداد لتطورات التقنية الجديدة وزيادة المخاطر التشغيلية.	• تطوير نظام شامل لإدارة مخاطر تقنية المعلومات الناشئة يشمل جميع الأنشطة التقنية. • إجراء تحليل دوري لتقنيات المعلومات الناشئة وتقييم المخاطر المرتبطة بها. • تقديم تدريبات للموظفين حول التقنيات الناشئة وكيفية التعامل مع المخاطر المتعلقة بها.	قسم تكنولوجيا المعلومات	مدير تكنولوجيا المعلومات	إجراء تقييم فوري لتقنيات المعلومات الناشئة وتحليل المخاطر المرتبطة بها واتخاذ الإجراءات اللازمة.	تحليل فعالية نظام إدارة مخاطر تقنية المعلومات الناشئة وتحديثه لضمان الكفاءة والاستعداد.	تحسين الاستعداد للتقنيات الناشئة وتقليل المخاطر من خلال نظام إدارة فعال وتدقيقات منتظمة.
53	نقص في تأمين أدوات التعاون الرقمي	أمني	نقص في تأمين أدوات التعاون الرقمي يمكن أن يؤدي إلى تسرب البيانات	• تطوير سياسة شاملة لتأمين أدوات التعاون الرقمي تشمل	قسم الأمن السيبراني	مدير الأمن السيبراني	إجراء تحقيق فوري في حالة وجود نشاط غير معتمد على أدوات التعاون الرقمي واتخاذ	تحليل فعالية السياسة الحالية وتحديثها لتعزيز أمان أدوات التعاون الرقمي.	تحسين أمان أدوات التعاون الرقمي وتقليل المخاطر من خلال سياسة

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
			والوصول غير المصرح به.	إجراءات التشفير والمصادقة. • تنفيذ تقنيات الأمان المتقدمة مثل MDM وتصفية البيانات. • إجراء تدقيقات دورية لأدوات التعاون الرقمي للتحقق من الامتثال للسياسات.			الإجراءات اللازمة.		شاملة وتدقيقات منتظمة.
54	نقص في إدارة المخاطر الناتجة عن الأعمال المشتركة	استراتيجي	نقص في إدارة المخاطر الناتجة عن الأعمال المشتركة يمكن أن يؤدي إلى عدم الامتثال للمتطلبات التنظيمية أو المخاطر المالية.	• تطوير نظام شامل لإدارة المخاطر الناتجة عن الأعمال المشتركة يشمل جميع الشركاء والمتعاقدين. • إجراء تدقيقات دورية للتحقق من الامتثال للمتطلبات التنظيمية والجودة. • تقديم تدريبات للشركاء والمتعاقدين حول متطلبات الامتثال وكيفية تحقيقها.	قسم الشؤون القانونية	المستشار القانوني	إجراء مراجعة فورية للأعمال المشتركة المتأثرة واتخاذ الإجراءات اللازمة لتحسين الامتثال.	تحليل فعالية نظام إدارة المخاطر الناتجة عن الأعمال المشتركة وتحديثه لضمان الامتثال والكفاءة.	تحسين الامتثال وتقليل المخاطر من خلال نظام إدارة فعال للأعمال المشتركة وتدقيقات منتظمة.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
55	نقص في تأمين أجهزة الحوسبة المحمولة	أمني	نقص في تأمين أجهزة الحوسبة المحمولة يمكن أن يؤدي إلى تسرب البيانات والوصول غير المصرح به.	• تطوير سياسة شاملة لتأمين أجهزة الحوسبة المحمولة تشمل إجراءات التشفير والمصادقة. • تنفيذ تقنيات الأمان المتقدمة مثل MDM وتصفية التطبيقات. • إجراء تدقيقات دورية لأجهزة الحوسبة المحمولة للتحقق من الامتثال للسياسات.	قسم الأمن السيبراني	مدير الأمن السيبراني	إجراء تحقيق فوري في حالة وجود نشاط غير معتمد على أجهزة الحوسبة المحمولة واتخاذ الإجراءات اللازمة.	تحليل فعالية السياسة الحالية وتحديثها لتعزيز أمان أجهزة الحوسبة المحمولة.	تحسين أمان أجهزة الحوسبة المحمولة وتقليل المخاطر من خلال سياسة شاملة وتدقيقات منتظمة.
56	نقص في إدارة المخاطر الناجمة عن الاعتماد على طرف ثالث	استراتيجي	نقص في إدارة المخاطر الناجمة عن الاعتماد على طرف ثالث يمكن أن يؤدي إلى عدم الامتثال للمتطلبات التنظيمية أو المخاطر المالية.	• تطوير نظام شامل لإدارة المخاطر الناجمة عن الاعتماد على طرف ثالث يشمل جميع الشركاء والمتعاقدين. • إجراء تدقيقات دورية للتحقق من الامتثال للمتطلبات التنظيمية والجودة.	قسم الشؤون القانونية	المستشار القانوني	إجراء مراجعة فورية للعلاقات المتأثرة واتخاذ الإجراءات اللازمة لتحسين الامتثال.	تحليل فعالية نظام إدارة المخاطر الناجمة عن الاعتماد على طرف ثالث وتحديثه لضمان الامتثال والكفاءة.	تحسين الامتثال وتقليل المخاطر من خلال نظام إدارة فعال للعلاقات مع الأطراف الثالثة وتدقيقات منتظمة.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
				• تقديم تدريبات للشركاء والمتعاقدين حول متطلبات الامتثال وكيفية تحقيقها.					
57	نقص في تأمين الاتصالات الداخلية والخارجية	أمني	نقص في تأمين الاتصالات الداخلية والخارجية يمكن أن يؤدي إلى تسرب البيانات أو اختراق الأنظمة.	• تطوير سياسة شاملة لتأمين الاتصالات تشمل تشفير البيانات واستخدام بروتوكولات أمان قوية. • تنفيذ تقنيات الأمان المتقدمة مثل TLS وVPN للاتصالات الآمنة. • إجراء تدقيقات دورية للاتصالات للتحقق من الامتثال للسياسات.	قسم الأمن السيبراني	مدير الأمن السيبراني	إجراء تحقيق فوري في حالة وجود نشاط غير معتمد على الاتصالات واتخاذ الإجراءات اللازمة.	تحليل فعالية السياسة الحالية وتحديثها لتعزيز أمان الاتصالات.	تحسين أمان الاتصالات الداخلية والخارجية وتقليل المخاطر من خلال سياسة شاملة وتدقيقات منتظمة.
58	نقص في إدارة مخاطر البرمجيات مفتوحة المصدر	تكنولوجي	نقص في إدارة مخاطر البرمجيات مفتوحة المصدر يمكن أن يؤدي إلى وجود	• تطوير سياسة شاملة لإدارة مخاطر البرمجيات مفتوحة المصدر	قسم تكنولوجيا المعلومات	مدير تكنولوجيا المعلومات	إجراء مراجعة فورية للبرمجيات مفتوحة المصدر المتأثرة وتحليل	تحليل نظام إدارة مخاطر البرمجيات مفتوحة المصدر بانتظام وتحديثه	تحسين أمان البرمجيات مفتوحة المصدر وتقليل المخاطر من خلال سياسة

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
			ثغرات أمنية أو انتهاكات حقوق الملكية الفكرية.	تشمل تقييم الأمان والامتثال. • إجراء تدقيقات دورية للتحقق من الامتثال لسياسات البرمجيات مفتوحة المصدر. • تقديم تدريبات للموظفين حول مخاطر البرمجيات مفتوحة المصدر وكيفية التعامل معها.			الأسباب لتحسين الإدارة.	لضمان الكفاءة والامتثال.	شاملة وتدقيقات منتظمة.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
59	نقص في إدارة مخاطر البرامج القديمة	تكنولوجي	نقص في إدارة مخاطر البرامج القديمة يمكن أن يؤدي إلى وجود ثغرات أمنية أو أداء ضعيف للأنظمة.	• تطوير سياسة شاملة لإدارة مخاطر البرامج القديمة تشمل تحديث الأنظمة وإزالة البرامج غير المدعومة. • إجراء تدقيقات دورية للتحقق من الامتثال لسياسات البرامج القديمة. • تقديم تدريبات للموظفين حول مخاطر البرامج القديمة وكيفية التعامل معها.	قسم تكنولوجيا المعلومات	مدير تكنولوجيا المعلومات	إجراء مراجعة فورية للبرامج القديمة المتأثرة وتحليل الأسباب لتحسين الإدارة.	تحليل نظام إدارة مخاطر البرامج القديمة بانتظام وتحديثه لضمان الكفاءة والامتثال.	تحسين أمان الأنظمة وتقليل المخاطر من خلال إدارة فعالة للبرامج القديمة وتحديثات منتظمة.
60	نقص في تأمين الأجهزة الطبية المتصلة بالشبكة	أمني	نقص في تأمين الأجهزة الطبية المتصلة بالشبكة يمكن أن يؤدي إلى تسرب البيانات الطبية أو تعطل الأجهزة.	• تطوير سياسة شاملة لتأمين الأجهزة الطبية المتصلة بالشبكة تشمل إجراءات التشفير والمصادقة. • تنفيذ تقنيات الأمان المتقدمة مثل MDM وتصفية البيانات. • إجراء تدقيقات دورية للأجهزة الطبية المتصلة	قسم الأمن السيبراني	مدير الأمن السيبراني	إجراء تحقيق فوري في حالة وجود نشاط غير معتمد على الأجهزة الطبية المتصلة بالشبكة واتخاذ الإجراءات اللازمة.	تحليل فعالية السياسة الحالية وتحديثها لتعزيز أمان الأجهزة الطبية.	تحسين أمان الأجهزة الطبية المتصلة بالشبكة وتقليل المخاطر من خلال سياسة شاملة وتدقيقات منتظمة.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
				بالشبكة للتحقق من الامتثال للسياسات.					
61	نقص في إدارة المخاطر الناتجة عن الاستعانة بمصادر خارجية	استراتيجي	نقص في إدارة المخاطر الناتجة عن الاستعانة بمصادر خارجية يمكن أن يؤدي إلى عدم الامتثال للمتطلبات التنظيمية أو المخاطر المالية.	• تطوير نظام شامل لإدارة المخاطر الناتجة عن الاستعانة بمصادر خارجية يشمل جميع الشركاء والمتعاقدين. • إجراء تدقيقات دورية للتحقق من الامتثال للمتطلبات التنظيمية والجودة. • تقديم تدريبات للشركاء والمتعاقدين حول متطلبات الامتثال وكيفية تحقيقها.	قسم الشؤون القانونية	المستشار القانوني	إجراء مراجعة فورية للعلاقات المتأثرة واتخاذ الإجراءات اللازمة لتحسين الامتثال.	تحليل فعالية نظام إدارة المخاطر الناتجة عن الاستعانة بمصادر خارجية وتحديثه لضمان الامتثال والكفاءة.	تحسين الامتثال وتقليل المخاطر من خلال نظام إدارة فعال للعلاقات مع المصادر الخارجية وتدقيقات منتظمة.
62	نقص في تأمين قواعد البيانات	أمني	نقص في تأمين قواعد البيانات يمكن أن يؤدي إلى تسرب البيانات والوصول غير المصرح به.	• تطوير سياسة شاملة لتأمين قواعد البيانات تشمل إجراءات التشفير والمصادقة.	قسم الأمن السيبراني	مدير الأمن السيبراني	إجراء تحقيق فوري في حالة وجود نشاط غير معتمد على قواعد البيانات واتخاذ الإجراءات اللازمة.	تحليل فعالية السياسة الحالية وتحديثها لتعزيز أمان قواعد البيانات.	تحسين أمان قواعد البيانات وتقليل المخاطر من خلال سياسة شاملة وتدقيقات منتظمة.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
				• تنفيذ تقنيات الأمان المتقدمة مثل IAM وتصفية البيانات. • إجراء تدقيقات دورية لقواعد البيانات للتحقق من الامتثال للسياسات.					
63	نقص في إدارة مخاطر تقنية الذكاء الاصطناعي	تكنولوجي	نقص في إدارة مخاطر تقنية الذكاء الاصطناعي يمكن أن يؤدي إلى سوء استخدام التقنية وزيادة المخاطر التشغيلية.	• تطوير نظام شامل لإدارة مخاطر تقنية الذكاء الاصطناعي يشمل جميع الأنشطة التقنية. • إجراء تحليل دوري لتقنيات الذكاء الاصطناعي وتقييم المخاطر المرتبطة بها. • تقديم تدريبات للموظفين حول التقنيات الناشئة وكيفية التعامل مع المخاطر المتعلقة بها.	قسم تكنولوجيا المعلومات	مدير تكنولوجيا المعلومات	إجراء تقييم فوري لتقنيات الذكاء الاصطناعي وتحليل المخاطر المرتبطة بها واتخاذ الإجراءات اللازمة.	تحليل فعالية نظام إدارة مخاطر تقنية الذكاء الاصطناعي وتحديثه لضمان الكفاءة والاستعداد.	تحسين الاستعداد لتقنيات الذكاء الاصطناعي وتقليل المخاطر من خلال نظام إدارة فعال وتدقيقات منتظمة.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
64	نقص في تأمين أجهزة إنترنت الأشياء	أمني	نقص في تأمين أجهزة إنترنت الأشياء يمكن أن يؤدي إلى تسرب البيانات أو اختراق الأنظمة.	• تطوير سياسة شاملة لتأمين أجهزة إنترنت الأشياء تشمل إجراءات التشفير والمصادقة. • تنفيذ تقنيات الأمان المتقدمة مثل IAM وتصفية البيانات. • إجراء تدقيقات دورية لأجهزة إنترنت الأشياء للتحقق من الامتثال للسياسات.	قسم الأمن السيبراني	مدير الأمن السيبراني	إجراء تحقيق فوري في حالة وجود نشاط غير معتمد على أجهزة إنترنت الأشياء واتخاذ الإجراءات اللازمة.	تحليل فعالية السياسة الحالية وتحديثها لتعزيز أمان أجهزة إنترنت الأشياء.	تحسين أمان أجهزة إنترنت الأشياء وتقليل المخاطر من خلال سياسة شاملة وتدقيقات منتظمة.
65	نقص في إدارة مخاطر البيانات الكبيرة	تكنولوجي	نقص في إدارة مخاطر البيانات الكبيرة يمكن أن يؤدي إلى سوء إدارة البيانات وزيادة المخاطر التنظيمية.	• تطوير سياسات شاملة لإدارة البيانات الكبيرة تشمل إجراءات الحفظ والتحليل والاستخدام. • إجراء تدقيقات دورية للتحقق من الامتثال لسياسات إدارة البيانات الكبيرة. • تقديم تدريبات للموظفين حول متطلبات إدارة	قسم تكنولوجيا المعلومات	مدير البيانات الكبيرة	إجراء مراجعة فورية للبيانات الكبيرة المتأثرة وتحليل الأسباب لتحسين الإدارة.	تحليل فعالية سياسات إدارة البيانات الكبيرة بانتظام وتحديثها لضمان الكفاءة والامتثال.	تحسين إدارة البيانات الكبيرة وتقليل المخاطر من خلال سياسات شاملة وتدقيقات منتظمة.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
				البيانات الكبيرة وكيفية تحقيقها.					
66	نقص في تأمين الأنظمة التشغيلية الصناعية	أمني	نقص في تأمين الأنظمة التشغيلية الصناعية يمكن أن يؤدي إلى تسرب البيانات أو تعطل الأنظمة الحيوية.	• تطوير سياسة شاملة لتأمين الأنظمة التشغيلية الصناعية تشمل إجراءات التشفير والمصادقة. • تنفيذ تقنيات الأمان المتقدمة مثل MDM وتصفية البيانات. • إجراء تدقيقات دورية للأنظمة التشغيلية الصناعية للتحقق من الامتثال للسياسات.	قسم الأمن السيبراني	مدير الأمن السيبراني	إجراء تحقيق فوري في حالة وجود نشاط غير معتمد على الأنظمة التشغيلية الصناعية واتخاذ الإجراءات اللازمة.	تحليل فعالية السياسة الحالية وتحديثها لتعزيز أمان الأنظمة التشغيلية الصناعية.	تحسين أمان الأنظمة التشغيلية الصناعية وتقليل المخاطر من خلال سياسة شاملة وتدقيقات منتظمة.
67	نقص في إدارة مخاطر البرمجيات الخبيثة	أمني	نقص في إدارة مخاطر البرمجيات الخبيثة يمكن أن يؤدي إلى انتشار البرمجيات الضارة داخل الأنظمة.	• تطوير سياسة شاملة لإدارة مخاطر البرمجيات الخبيثة تشمل استخدام برامج مكافحة الفيروسات وتحديثها بانتظام. • تنفيذ تقنيات الكشف عن	قسم الأمن السيبراني	مدير الأمن السيبراني	إجراء فحص شامل للأنظمة المتأثرة وإزالة البرمجيات الخبيثة.	تحليل الحوادث الفيروسية بانتظام وتحديث سياسة التصدي لتعزيز الأمان.	تحسين أمان الأنظمة وتقليل الهجمات الفيروسية من خلال سياسة شاملة وتدقيقات منتظمة.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
				البرمجيات الخبيثة وإزالة التهديدات المحتملة. • إجراء تدريبات توعوية للموظفين حول تهديدات البرمجيات الخبيثة وكيفية تجنبها.					
68	نقص في تأمين أجهزة البنية التحتية الحيوية	أمني	نقص في تأمين أجهزة البنية التحتية الحيوية يمكن أن يؤدي إلى تسرب البيانات أو تعطل الأنظمة الحيوية.	• تطوير سياسة شاملة لتأمين أجهزة البنية التحتية الحيوية تشمل إجراءات التشفير والمصادقة. • تنفيذ تقنيات الأمان المتقدمة مثل MDM وتصفية البيانات. • إجراء تدقيقات دورية لأجهزة البنية التحتية الحيوية للتحقق من الامتثال للسياسات.	قسم الأمن السيبراني	مدير الأمن السيبراني	إجراء تحقيق فوري في حالة وجود نشاط غير معتمد على أجهزة البنية التحتية الحيوية واتخاذ الإجراءات اللازمة.	تحليل فعالية السياسة الحالية وتحديثها لتعزيز أمان أجهزة البنية التحتية الحيوية.	تحسين أمان أجهزة البنية التحتية الحيوية وتقليل المخاطر من خلال سياسة شاملة وتدقيقات منتظمة.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
69	نقص في إدارة مخاطر البيانات البيومترية	أمني	نقص في إدارة مخاطر البيانات البيومترية يمكن أن يؤدي إلى تسرب البيانات الحساسة واستخدامها بشكل غير قانوني.	• تطوير نظام شامل لإدارة مخاطر البيانات البيومترية يشمل جميع الأنشطة المتعلقة بالبيانات الحساسة. • تنفيذ تقنيات الأمان المتقدمة مثل التشفير والمصادقة المتعددة العوامل. • إجراء تدقيقات دورية للتحقق من الامتثال لسياسات إدارة البيانات البيومترية.	قسم الأمن السيبراني	مدير الأمن السيبراني	إجراء تحقيق فوري في حالة وجود نشاط غير معتمد على البيانات البيومترية واتخاذ الإجراءات اللازمة.	تحليل فعالية نظام إدارة مخاطر البيانات البيومترية وتحديثه لضمان الأمان والامتثال.	تحسين أمان البيانات البيومترية وتقليل المخاطر من خلال إدارة فعالة وتدقيقات منتظمة.
70	نقص في تأمين الشبكات الافتراضية الخاصة (VPN)	أمني	نقص في تأمين الشبكات الافتراضية الخاصة يمكن أن يؤدي إلى تسرب البيانات أو اختراق الأنظمة.	• تطوير سياسة شاملة لتأمين الشبكات الافتراضية الخاصة تشمل إجراءات التشفير والمصادقة. • تنفيذ تقنيات الأمان المتقدمة مثل TLS وIPSec للاتصالات الآمنة.	قسم الأمن السيبراني	مدير الأمن السيبراني	إجراء تحقيق فوري في حالة وجود نشاط غير معتمد على الشبكات الافتراضية الخاصة واتخاذ الإجراءات اللازمة.	تحليل فعالية السياسة الحالية وتحديثها لتعزيز أمان الشبكات الافتراضية الخاصة.	تحسين أمان الشبكات الافتراضية الخاصة وتقليل المخاطر من خلال سياسة شاملة وتدقيقات منتظمة.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
				• إجراء تدقيقات دورية للشبكات الافتراضية الخاصة للتحقق من الامتثال للسياسات.					
71	نقص في إدارة مخاطر البرمجيات الضارة	أمني	نقص في إدارة مخاطر البرمجيات الضارة يمكن أن يؤدي إلى انتشار البرمجيات الضارة داخل الأنظمة.	• تطوير سياسة شاملة لإدارة مخاطر البرمجيات الضارة تشمل استخدام برامج مكافحة الفيروسات وتحديثها بانتظام. • تنفيذ تقنيات الكشف عن البرمجيات الضارة وإزالة التهديدات المحتملة. • إجراء تدريبات توعوية للموظفين حول تهديدات البرمجيات الضارة وكيفية تجنبها.	قسم الأمن السيبراني	مدير الأمن السيبراني	إجراء فحص شامل للأنظمة المتأثرة وإزالة البرمجيات الضارة.	تحليل الحوادث البرمجية الضارة بانتظام وتحديث سياسة التصدي لتعزيز الأمان.	تحسين أمان الأنظمة وتقليل الهجمات البرمجية الضارة من خلال سياسة شاملة وتدقيقات منتظمة.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
72	نقص في تأمين الأجهزة الطبية المتصلة بالإنترنت	أمني	نقص في تأمين الأجهزة الطبية المتصلة بالإنترنت يمكن أن يؤدي إلى تسرب البيانات الطبية أو تعطل الأجهزة.	• تطوير سياسة شاملة لتأمين الأجهزة الطبية المتصلة بالإنترنت تشمل إجراءات التشفير والمصادقة. • تنفيذ تقنيات الأمان المتقدمة مثل MDM وتصفية البيانات. • إجراء تدقيقات دورية للأجهزة الطبية المتصلة بالإنترنت للتحقق من الامتثال للسياسات.	قسم الأمن السيبراني	مدير الأمن السيبراني	إجراء تحقيق فوري في حالة وجود نشاط غير معتمد على الأجهزة الطبية المتصلة بالإنترنت واتخاذ الإجراءات اللازمة.	تحليل فعالية السياسة الحالية وتحديثها لتعزيز أمان الأجهزة الطبية المتصلة بالإنترنت.	تحسين أمان الأجهزة الطبية المتصلة بالإنترنت وتقليل المخاطر من خلال سياسة شاملة وتدقيقات منتظمة.
73	نقص في إدارة مخاطر البريد الإلكتروني	أمني	نقص في إدارة مخاطر البريد الإلكتروني يمكن أن يؤدي إلى تسرب البيانات أو الهجمات السيبرانية.	• تطوير سياسة شاملة لإدارة مخاطر البريد الإلكتروني تشمل إجراءات تصفية البريد الإلكتروني والتصدي لهجمات التصيد الاحتيالي. • تنفيذ تقنيات الأمان المتقدمة مثل DMARC وSPF وDKIM.	قسم الأمن السيبراني	مدير الأمن السيبراني	عزل البريد الإلكتروني المشبوه والتحقيق في الحادث.	تحليل الحوادث البريدية بانتظام وتحديث سياسة إدارة البريد الإلكتروني لتعزيز الأمان.	تحسين أمان البريد الإلكتروني وتقليل الهجمات السيبرانية من خلال سياسة شاملة وتدقيقات منتظمة.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
				• إجراء تدريبات توعوية للموظفين حول تهديدات البريد الإلكتروني وكيفية التعرف عليها.					
74	نقص في تأمين التطبيقات الصحية	أمني	نقص في تأمين التطبيقات الصحية يمكن أن يؤدي إلى تسرب البيانات الطبية أو الوصول غير المصرح به.	• تطوير سياسة شاملة لتأمين التطبيقات الصحية تشمل إجراءات التشفير والمصادقة. • تنفيذ تقنيات الأمان المتقدمة مثل IAM وتصفية البيانات. • إجراء تدقيقات دورية للتطبيقات الصحية للتحقق من الامتثال للسياسات.	قسم الأمن السيبراني	مدير الأمن السيبراني	إجراء تحقيق فوري في حالة وجود نشاط غير معتمد على التطبيقات الصحية واتخاذ الإجراءات اللازمة.	تحليل فعالية السياسة الحالية وتحديثها لتعزيز أمان التطبيقات الصحية.	تحسين أمان التطبيقات الصحية وتقليل المخاطر من خلال سياسة شاملة وتدقيقات منتظمة.
75	نقص في إدارة مخاطر التطبيقات المالية	تكنولوجي	نقص في إدارة مخاطر التطبيقات المالية يمكن أن يؤدي إلى فقدان البيانات أو اختراق الأنظمة المالية.	• تطوير نظام شامل لإدارة مخاطر التطبيقات المالية يشمل جميع التطبيقات والبيانات المالية.	قسم الأمن السيبراني	مدير الأمن السيبراني	إجراء تحقيق فوري في حالة وجود نشاط غير معتمد على التطبيقات المالية واتخاذ الإجراءات اللازمة.	تحليل فعالية نظام إدارة مخاطر التطبيقات المالية وتحديثه لتعزيز الأمان والامتثال.	تحسين أمان التطبيقات المالية وتقليل المخاطر من خلال نظام إدارة فعال وتدقيقات منتظمة.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
				• تنفيذ تقنيات الأمان المتقدمة مثل IAM وتصفية البيانات. • إجراء تدقيقات دورية للتطبيقات المالية للتحقق من الامتثال للسياسات.					
76	نقص في تأمين الأجهزة الشخصية المستخدمة في العمل	أمني	نقص في تأمين الأجهزة الشخصية المستخدمة في العمل يمكن أن يؤدي إلى تسرب البيانات والوصول غير المصرح به.	• تطوير سياسة شاملة لتأمين الأجهزة الشخصية المستخدمة في العمل تشمل إجراءات التشفير والمصادقة. • تنفيذ تقنيات الأمان المتقدمة مثل MDM وتصفية التطبيقات. • إجراء تدقيقات دورية للأجهزة الشخصية المستخدمة في العمل للتحقق من الامتثال للسياسات.	قسم الأمن السيبراني	مدير الأمن السيبراني	إجراء تحقيق فوري في حالة وجود نشاط غير معتمد على الأجهزة الشخصية المستخدمة في العمل واتخاذ الإجراءات اللازمة.	تحليل فعالية السياسة الحالية وتحديثها لتعزيز أمان الأجهزة الشخصية.	تحسين أمان الأجهزة الشخصية المستخدمة في العمل وتقليل المخاطر من خلال سياسة شاملة وتدقيقات منتظمة.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
77	نقص في إدارة مخاطر الأجهزة الذكية	أمني	نقص في إدارة مخاطر الأجهزة الذكية يمكن أن يؤدي إلى تسرب البيانات أو اختراق الأنظمة.	• تطوير سياسة شاملة لإدارة مخاطر الأجهزة الذكية تشمل إجراءات التشفير والمصادقة. • تنفيذ تقنيات الأمان المتقدمة مثل IAM وتصفية البيانات. • إجراء تدقيقات دورية للأجهزة الذكية للتحقق من الامتثال للسياسات.	قسم الأمن السيبراني	مدير الأمن السيبراني	إجراء تحقيق فوري في حالة وجود نشاط غير معتمد على الأجهزة الذكية واتخاذ الإجراءات اللازمة.	تحليل فعالية السياسة الحالية وتحديثها لتعزيز أمان الأجهزة الذكية.	تحسين أمان الأجهزة الذكية وتقليل المخاطر من خلال سياسة شاملة وتدقيقات منتظمة.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
78	نقص في تأمين الأجهزة الطبية المتنقلة	أمني	نقص في تأمين الأجهزة الطبية المتنقلة يمكن أن يؤدي إلى تسرب البيانات الطبية أو تعطل الأجهزة.	• تطوير سياسة شاملة لتأمين الأجهزة الطبية المتنقلة تشمل إجراءات التشفير والمصادقة. • تنفيذ تقنيات الأمان المتقدمة مثل MDM وتصفية البيانات. • إجراء تدقيقات دورية للأجهزة الطبية المتنقلة للتحقق من الامتثال للسياسات.	قسم الأمن السيبراني	مدير الأمن السيبراني	إجراء تحقيق فوري في حالة وجود نشاط غير معتمد على الأجهزة الطبية المتنقلة واتخاذ الإجراءات اللازمة.	تحليل فعالية السياسة الحالية وتحديثها لتعزيز أمان الأجهزة الطبية المتنقلة.	تحسين أمان الأجهزة الطبية المتنقلة وتقليل المخاطر من خلال سياسة شاملة وتدقيقات منتظمة.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
79	نقص في إدارة مخاطر العمل عن بُعد	استراتيجي	نقص في إدارة مخاطر العمل عن بُعد يمكن أن يؤدي إلى تسرب البيانات أو اختراق الأنظمة.	• تطوير نظام شامل لإدارة مخاطر العمل عن بُعد يشمل جميع التطبيقات والبيانات. • تنفيذ تقنيات الأمان المتقدمة مثل VPN وتصفية البيانات. • إجراء تدقيقات دورية للتحقق من الامتثال للسياسات الأمنية للعمل عن بُعد.	قسم الأمن السيبراني	مدير الأمن السيبراني	إجراء تحقيق فوري في حالة وجود نشاط غير معتمد أثناء العمل عن بُعد واتخاذ الإجراءات اللازمة.	تحليل فعالية نظام إدارة مخاطر العمل عن بُعد وتحديثه لتعزيز الأمان والامتثال.	تحسين أمان العمل عن بُعد وتقليل المخاطر من خلال نظام إدارة فعال وتدقيقات منتظمة.
80	نقص في تأمين الأجهزة المحمولة المستخدمة في العمليات الحساسة	أمني	نقص في تأمين الأجهزة المحمولة المستخدمة في العمليات الحساسة يمكن أن يؤدي إلى تسرب البيانات أو تعطل العمليات.	• تطوير سياسة شاملة لتأمين الأجهزة المحمولة المستخدمة في العمليات الحساسة تشمل إجراءات التشفير والمصادقة. • تنفيذ تقنيات الأمان المتقدمة مثل MDM وتصفية البيانات. • إجراء تدقيقات دورية للأجهزة المحمولة	قسم الأمن السيبراني	مدير الأمن السيبراني	إجراء تحقيق فوري في حالة وجود نشاط غير معتمد على الأجهزة المحمولة المستخدمة في العمليات الحساسة واتخاذ الإجراءات اللازمة.	تحليل فعالية السياسة الحالية وتحديثها لتعزيز أمان الأجهزة المحمولة المستخدمة في العمليات الحساسة.	تحسين أمان الأجهزة المحمولة المستخدمة في العمليات الحساسة وتقليل المخاطر من خلال سياسة شاملة وتدقيقات منتظمة.

الرقم التسلسلي	الخطر المحتمل	التصنيف	وصف الخطر	إجراءات الرقابة	موقع الخطر	الشخص المسؤول	الإجراءات الفورية عند حدوث الخطر	الإجراءات المتخذة لمعالجة الخطر	التخفيف النهائي
				المستخدمة في العمليات الحساسة للتحقق من الامتثال للسياسات.					

تصميم: مصطفى صباح