سلطنة عُمان
وزارة التقنية والاتصالات
Sultanate of Oman
Ministry of Technology and Communications

عمان الرقمية
e.oman

إطار إدارة مخاطر تقنية المعلومات

وزارة التقنية والإتصالات

الفهرس

1 المقدمة

تعرف تقنية المعلومات بأنها المحرك الذي يمكّن الحكومة من تقديم خدمات أفضل لمواطنيها، وتمنح قدر أكبر من الإنتاجية للدولة ككل، وتعتمد وحدات الجهاز الإداري للدولة على أنظمة المعلومات القائمة على التقنية بشكل كبير في القيام بمهامها ووظائفها وأعمالها بنجاح، وتتعرض هذه الأنظمة لتهديدات خطيرة يمكن أن تسبب آثار ضارة على العمليات التنظيمية (مثل: المهام، أو الوظائف، أو صورة المؤسسة، أو سمعتها)، أو الأصول التنظيمية، والأفراد، والمؤسسات الأخرى، والدولة من خلال استغلال كل من نقاط الضعف المعروفة وغير المعروفة للإخلال بسرية أو سلامة أو توفر المعلومات التي يتم معالجتها أو تخزينها أو إرسالها بواسطة هذه الأنظمة، وتشمل التهديدات التي تهدد المعلومات: وأنظمتها الهجمات الموجهة، والاختلالات البيئية، والأخطاء البشرية / الآلية والتي تؤدي إلى إحداث ضرر كبير على المصالح الأمنية والوطنية والاقتصادية للسلطنة، لذلك من الضروري أن يدرك القادة والمدراء في جميع المستويات مسؤولياتهم وأنهم مساءلين عن إدارة المخاطر المتصلة بأمن المعلومات –أي المخاطر المرتبطة بتشغيل واستخدام نظم المعلومات الداعمة لمهام وأعمال مؤسساتهم.

تشمل المخاطر التنظيمية العديد من الأنواع (مثل مخاطر إدارة البرامج، والاستثمار، ووضع الموازنة، والمسؤولية القانونية، والسلامة، والتخزين، والمخاطر المرتبطة بسلسلة التوريد، والمخاطر الأمنية). تعتبر المخاطر الأمنية المتعلقة بتشغيل واستخدام نظم المعلومات مجرد جزء من العديد من المخاطر التنظيمية التي يتطلب من كبار القادة / المدراء التنفيذيين معالجتها ضمن مسؤولياتهم المستمرة في إدارة المخاطر. تتطلب الإدارة الفعالة للمخاطر أن تعمل المؤسسات في بيئات معقدة للغاية ومترابطة باستخدام أحدث أنظمة المعلومات والأنظمة القديمة – وهي أنظمة تعتمد عليها المؤسسات لإنجاز مهامها ووظائف مهمة متعلقة بالأعمال. يجب على القادة أن يدركوا أن القرارات الصريحة والواعية المتعلقة بالمخاطر ضرورية لتحقيق التوازن بين الفوائد المكتسبة من تشغيل واستخدام نظم المعلومات ومخاطر أن تكون نفس الأنظمة وسائل يمكن من خلالها شن هجمات موجهة أو حدوث ضرر ناتج عن اضطرابات بيئية أو أخطاء بشرية من شأنها أن تسبب فشل في تأدية المهام أو العمل. تعد إدارة مخاطر أمن المعلومات، مثل إدارة المخاطر بشكل عام، ليست علمًا دقيقًا، فهي تجمع بين أفضل الأحكام الجماعية للأفراد والجماعات في المؤسسات المسؤولة عن التخطيط الاستراتيجي والرقابة والإدارة والعمليات اليومية — من خلال توفير كل من تدابير الاستجابة اللازمة والكافية لمواجهة المخاطر لحماية مهام وأعمال تلك المؤسسات حماية كافية .

يعد دور أمن المعلومات في إدارة المخاطر الناتجة عن تشغيل أنظمة المعلومات واستخدامها أمرًا مهمًا أيضًا لنجاح المؤسسات في تحقيق أهدافها وغاياتها الاستراتيجية. تاريخياً، كان لدى كبار القادة / المدراء التنفيذيين رؤية ضيقة جدًا لأمن المعلومات فإما يعتبرونها قضايا تقنية أو أمور

بيروقراطية مستقلة عن المخاطر التنظيمية وعمليات الإدارة التقليدية. نتج عن هذا المنظور المحدود للغاية عدم كفاية المعرفة بكيفية تأثير مخاطر أمن المعلومات، مثل المخاطر التنظيمية الأخرى، على احتمالية أداء المؤسسات بمهامها وأعمالها بنجاح. تضع هذه الوثيقة أمن المعلومات في السياق التنظيمي الأوسع لتحقيق نجاح المهمة/ العمل. يتمثل الأهداف فيما يلي:

التأكد من إدراك كبار القادة / التنفيذيين لأهمية إدارة مخاطر أمن المعلومات وإنشاء هياكل حوكمة مناسبة لإدارة هذه المخاطر.

• التأكد من أن تنفيذ عملية إدارة المخاطر في المؤسسة تتم على نحو فعال عبر المستويات الثلاثة للمؤسسة، المهام / الأعمال ، ونظم المعلومات.

• تعزيز المناخ التنظيمي الذي يتم فيه مراعاة مخاطر أمن المعلومات في سياق تصميم المهام/ الأعمال ، وتحديد إطار التصميم المؤسسي الشامل، دورة حياة عمليات تطوير النظام.

• مساعدة الأفراد الذين يتولون مسؤوليات تنفيذ نظم المعلومات أو إدارتها على تحقيق فهم أفضل لكيفية ترجمة مخاطر أمن المعلومات المرتبطة بأنظمتهم إلى مخاطر عامة على مستوى المؤسسة، الأمر الذي قد يؤثر، في نهاية المطاف، على نجاح المهمة / العمل.

1.1 الغرض

يكمن الغرض من هذه الوثيقة في تقديم التوجيه للمؤسسات الحكومية بشأن إجراء تقييم للمخاطر. يعد تقييم المخاطر جزءاً من العملية الشاملة لإدارة المخاطر — من خلال تزويد كبار القادة / التنفيذيين بالمعلومات اللازمة لتحديد مسارات العمل المناسبة استجابةً للمخاطر المحددة. تقدم هذه الوثيقة إرشادات تنفيذ لكل خطوة من خطوات عملية تقييم المخاطر (بما في ذلك ، الاستعداد للتقييم، وإجراء التقييم، والإبلاغ بنتائج التقييم، وتحديث التقييم)، وكيفية تقييم المخاطر وغيرها من عمليات إدارة المخاطر التنظيمية التي تؤدي إلى التكامل بعضها البعض.

1.2 الجمهور المستهدف

تستهدف هذه الوثيقة مجموعة مختلفة من المتخصصين في إدارة المخاطر بما في ذلك:

- الأفراد المضطلعون بمسؤوليات الإشراف على إدارة المخاطر (مثل رؤساء المؤسسات، والرؤساء التنفيذيين، والرؤساء التنفيذيين للعمليات، والمسؤولين عن المخاطر [كوظيفة) ؛
- الأفراد المضطلعون بمسؤوليات أداء مهام / أعمال المؤسسة (مثل، أصحاب المهام/ الأعمال، ومالكي/ والمشرفين على المعلومات، والقائمين على التفويض) ؛

- الأفراد المضطلعون بمسؤوليات شراء منتجات أو خدمات أو أنظمة تقنية المعلومات (على سبيل المثال، مسؤولو شراء خدمات وأجهزة تقنية المعلومات، مسؤولو المشتريات، موظفو العقود) ؛
- الأفراد المضطلعون بمسؤوليات تصميم وتطوير / تنفيذ نظام / أمن المعلومات (مثل مدراء البرامج ومصممي الأطر ومهندسي أمن المعلومات ومهندسي نظم المعلومات / ومهندسي الأمن والقائمين على تكامل نظم المعلومات)؛
- الأفراد المسؤولين عن الإشراف على أمن المعلومات، والإدارة، والعمليات التشغيلية (مثل كبار مسؤولي تقنية المعلومات، وكبار ضباط أمن المعلومات، و مدراء أمن المعلومات، ومالكي نظام المعلومات، ومقدمي الرقابة المشتركة)؛ و
- الأفراد المضطلعون بمسؤوليات أمن المعلومات / تقييم المخاطر ومراقبتها (على سبيل المثال، مقيمو النظم، والقائمين بالاختبارات الخاصة بالاختراق، ومراقبو الضوابط الأمنية، ومقيمو المخاطر، والمراجعون / المدققون المستقلون، والمفتشون العامون، والمراجعون).

2 منهجية تقييم المخاطر

تلتزم الجهات الحكومية باستخدام تقييم المخاطر لتحديد مدى التهديد المحتمل والمخاطر المرتبطة بأصول المعلومات. تساعد مخرجات هذه العملية على تحديد الضوابط المناسبة للحد من المخاطر أو القضاء عليها أثناء عملية التخفيف من المخاطر.

يجب إعادة النظر في عملية تقييم المخاطر سنويًا على الأقل (أو كلما طرأ أي تغيير كبير في المؤسسة) من قِبل مدير / مسؤول أمن المعلومات، ويجب أخذ جميع التهديدات ونقاط الضعف الجديدة التي تم تحديدها في الاعتبار لمعالجتها. يجب أيضًا إعادة النظر في المخاطر المحددة مسبقًا (الموجودة) لمعرفة ما إذا كانت الضوابط المطبقة كافية أو تتطلب مزيد من المعالجة.

2.1 تحديد الأصول

تقترح هذه الوثيقة نموذج مرجعي خاص بالتحليل النوعي للمخاطر لتقييم إطار المخاطروتنفيذه. يجب أن يتألف فريق إدارة المخاطر من أفراد من مجموعات مختلفة من المؤسسة. يجب على ممثلي هذه المجموعات العمل معًا كفريق واحد وتحديد الأصول وتشكيل قائمة أصول المعلومات. تحدد هذه القائمة الأصول المختلفة وكذلك الفئة التي تنتمي إليها تلك الأصول إضافة إلى موقع الأصل.

تكون قائمة جرد الأصول بصور مختلفة ويعرف أولئك الذين يمتلكون هذه المعلومات بمالكي أصول المعلومات، والتي يمكن أن تكون:

- أصول المعلومات /البيانات
- أصول التقنية
- أصول الأشخاص
- أصول الخدمة

يجب تحديد وتوثيق جميع أصول معلومات المؤسسة، بمجرد تحديدها، يتم تصنيف الأصول وفقًا لمعايير التصنيف المحددة مسبقًا (يجب أن تحدد المؤسسة إجراءات تصنيف ومعالجة المعلومات).

يجب أن يكون لكل أصل معلوماتي مالك أصول و/ أو أمين أصول. يتم الاحتفاظ بمالك وأمين كل أصل في مخزون الأصول المعني. من وجهة نظر إدارة المخاطر، سيتم اعتبار مالك الأصول مسؤولاً عن اتخاذ الإجراءات المناسبة واعتماد الضوابط الفعالة لتقليل المخاطر.

2.2 تحديد التهديدات

التهديد هو إمكانية قيام مصدر تهديد معين بتنفيذ هجمات (إما عن طريق الخطأ أو عن قصد). من خلال استغلال ثغرة أمنية معينة. مصدر–التهديد إما أن يكون: ؛ (1) مقصود وأسلوب موجه للاستغلال المتعمد للثغرات الأمنية أو (2) حدث أو طريقة قد تؤدي إلى إحداث ثغرة أمنية عن طريق الخطأ. وتمثل الثغرة نقطة ضعف يمكن إحداثها عن طريق الخطأ أو استغلالها عمداً.

لا يشكل مصدر التهديد خطراً عندما لا تكون هناك ثغرة يمكن استغلالها. عند اكتشاف احتمال وجود تهديد، يجب مراعاة مصادر التهديد والثغرات الأمنية المحتملة والضوابط الحالية.

2.2.1 2.1 تحديد مصادر التهديد

يتمثل الهدف من هذه الخطوة في تحديد مصادر التهديد المحتملة وتجميع كشف بالتهديدات يسرد مصادر التهديد المحتملة التي لها علاقة بأصول المعلومات قيد النظر.

يُعرَّف مصدر التهديدات بأنه أي ظرف أو حدث يؤدي إلى احتمال إلحاق ضرر بأصول المعلومات. يمكن أن تكون مصادر التهديدات الشائعة طبيعية أو بشرية أو بيئية. عند تقييم مصادر التهديدات، من المهم الأخذ بعين الاعتبار جميع مصادر التهديدات المحتملة التي يمكن أن تلحق الضرر بأصول المعلومات، على سبيل المثال، على الرغم من أن كشف التهديدات لنظام تقنية المعلومات الموجود في الصحراء قد لا يشمل "فيضانًا طبيعيًا" بسبب انخفاض احتمالية وقوع مثل هذا الحدث، فإن التهديدات البيئية مثل انفجار الأنابيب يمكن أن تغمر غرفة الكمبيوتر بسرعة وتلحق أضرارًا بأصول وموارد تقنية المعلومات الخاصة بالمؤسسة. يمكن للبشر أن يشكلوا مصدر تهديد من خلال الأفعال المتعمدة، مثل الهجمات المتعمدة التي يقوم بها أشخاص يتعمدون إحداث الضرر أو موظفون ساخطون، أو أعمال غير مقصودة، مثل الإهمال والأخطاء.

قد يكون الهجوم المتعمد إما (1) محاولة خبيثة للوصول غير المصرح به إلى نظام تقنية المعلومات (على سبيل المثال، من خلال تخمين كلمة المرور) من أجل إلحاق الضرر بالنظام أو سلامة البيانات أو توفرها أو سريتها أو (2) اختراق حميد وهادف، وهو عبارة عن محاولة للتحايل على أمن النظام. أحد الأمثلة على هذا النوع الأخير من الهجوم المتعمد هو قيام مبرمج بكتابة برنامج يحتوي على خدعة لتجاوز أمن النظام من أجل "إنجاز مهمة ما".

مصادر التهديدات الشائعة:

- **التهديدات الطبيعية** – الفيضانات، والزلازل، والأعاصير، والانهيارات الأرضية، والانهيارات الثلجية، والعواصف الكهربائية، وغيرها من الأحداث المشابهة.
- **التهديدات البشرية** – الحوادث التي يتسبب في حدوثها البشر، مثل الأعمال غير المقصودة (إدخال البيانات غير المقصودة) أو الإجراءات المتعمدة (أو الهجمات التي تستهدف الشبكات، تحميل البرامج الضارة، الوصول غير المصرح به إلى المعلومات السرية).
- التهديدات البيئية – الانقطاع الطويل للتيار الكهربائي، أو التلوث، أو المواد الكيميائية، أو تسرب السوائل.

2.2.2 2.2 الدافع وعمليات التهديد

يعد البشر مصدر تهديد محتمل لتنفيذ الهجمات الإلكترونية نظرًا للدوافع المختلفة والموارد المتاحة لذلك. يقدم الجدول 3–1 نبذة مختصرة للعديد من التهديدات البشرية الشائعة اليوم، ودوافعها المحتملة، وأساليب أو عمليات التهديد التي قد يلجأ إليها منفذوا الجرائم الإلكترونية.

تعد هذه المعلومات مفيدة للمؤسسات التي تسعى إلى فهم بيئات التهديد البشري وتعمل على تخصيص بيانات متعلقة بالتهديدات البشرية. بالإضافة إلى ذلك، سيساعد معرفة تاريخ الهجمات والتسلل إلى الأنظمة ؛ وإعداد تقارير الانتهاكات الأمنية؛ وتقارير الحوادث والمقابلات مع مسؤولي الأنظمة وموظفي الدعم الفني ومجتمع المستخدمين أثناء جمع المعلومات في تحديد مصادر التهديدات البشرية ذات القدرة على إلحاق الضرر بأنظمة تقنية المعلومات وبياناتها والتي قد تكون مصدر قلق عند وجود ثغرة أمنية.

الجدول الأول– مصادر التهديدات ودوافعها

مصدر التهديد	الدافع	أعمال التهديد
قرصان، مخترق	التحدي الغرور التمرد	• القرصنة • الهندسة الاجتماعية • اقتحام وتسلل النظام • الوصول غير المصرح به للنظام
مجرم حاسوبي	إتلاف المعلومات الكشف غير القانوني عن المعلومات تحقيق مكاسب مالية تغيير غير مصرح به للبيانات	• الجريمة الالكترونية (على سبيل المثال، الملاحقة الإلكترونية) • الأعمال الاحتيالية (على سبيل المثال، إعادة، انتحال شخصية، التنصت) • رشوة المعلومات • الخداع • التسلل إلى النظام
الإرهابي	الابتزاز التدمير الاستغلال الانتقام	• قنابل / إرهاب • حرب المعلومات • مهاجمة النظام (على سبيل المثال، رفض الخدمة الموزع) • اختراق النظام • العبث بالنظام
التجسس الصناعي (الشركات والحكومات الأجنبية والمصالح الحكومية الأخرى)	الميزة التنافسية التجسس الاقتصادي	• الاستغلال الاقتصادي • سرقة المعلومات • التسلل على الخصوصية الشخصية • هندسة اجتماعية • اختراق النظام • الوصول غير المصرح به للنظام (الوصول إلى المعلومات السرية، المتعلقة بالملكية، و / أو المتعلقة بالتقنية)
المطلعون (الموظفون ذوو التدريب السيء أو الساخطين أو الخبيثين أو المهملين أو غير	الفضول الغرور الاستخبارات تحقيق مكاسب مالية	• الاعتداء على موظف • الابتزاز • تصفح معلومات الملكية • إساءة استخدام الكمبيوتر

الشرفاء أو الموظفين الذين تم إنهاء خدماتهم)	الانتقام أخطاء غير مقصودة و الإغفالات (مثل الخطأ في إدخال البيانات، الخطأ في البرمجة)	• الاحتيال والسرقة • رشوة المعلومات • إدخال البيانات المزيفة التالفة • التنصت • شفرة ضارة (مثل الفيروسات والقنبلة المنطقية، حصان طروادة) • بيع المعلومات الشخصية • أخطاء النظام • التسلل إلى النظام • تخريب النظام • الوصول غير المصرح به للنظام

يجب وضع تقدير الدوافع والموارد والقدرات التي قد تلزم لتنفيذ هجوم ناجح بعد تحديد مصادر التهديد المحتملة، من أجل تحديد احتمال ممارسة تهديد ما لأحد نقاط ضعف النظام.

يجب تخصيص كشف بالتهديدات، أو قائمة مصادر التهديد المحتملة، للمؤسسة الفردية وبيئة المعالجة الخاصة بها (على سبيل المثال، عادات الحوسبة للمستخدم النهائي). بشكل عام، يجب أن تكون المعلومات المتعلقة بالتهديدات الطبيعية (مثل الفيضانات والزلازل والعواصف) متاحة بسهولة

الناتج: بيان تهديد يحتوي على قائمة بمصادر التهديد التي يمكن أن تستغل نقاط ضعف النظام

2.3 تحديد نقاط الضعف

نقطة الضعف: عيب أو ضعف في إجراءات أمن النظام أو تصميمه أو تنفيذه أو الضوابط الداخلية التي يمكن ممارستها (يتم تشغيله عن طريق الخطأ أو استغلاله عمداً) ويؤدي إلى خرق أمني أو انتهاك لسياسة أمن النظام.

يجب أن يتضمن تحليل التهديد لأصول المعلومات تحليلًا للثغرات الأمنية المرتبطة ببيئة النظام. يتمثل الهدف من هذه الخطوة في وضع قائمة بثغرات النظام (العيوب أو نقاط الضعف) التي يمكن استغلالها من قبل مصادر التهديد المحتملة.

الجدول الثاني– نقاط الضعف والتهديدات

نقطة الضعف	مصدر التهديد	أعمال التهديد
عدم إزالة معرفات نظام الموظفين التي تم إنهاء خدماتهم من النظام	الموظفين التي تم إنهاء خدماتهم	الاتصال بشبكة الشركة والوصول إلى بيانات الملكية الخاصة بالشركة
يتيح جدار حماية الشركة التلنت الوارد، وتم تمكين معرف الضيف على الخادم **XYZ**	المستخدمون غير المصرح لهم (مثل المتسللين والموظفين الذين تم إنهاء خدمتهم والمجرمين الالكترونيين والإرهابيين)	استخدام التلنت لخادم **XYZ** وتصفح ملفات النظام باستخدام معرف الضيف
حدد المورد عيوبًا في التصميم الأمني للنظام ؛ ومع ذلك، لم يتم تطبيق تصحيحات جديدة على النظام	المستخدمون غير المصرح لهم (مثل المتسللين والموظفين الساخطين والمجرمين الالكترونيين والإرهابيين)	الحصول على وصول غير مصرح به إلى ملفات النظام الحساسة بناءً على نقاط ضعف النظام المعروفة
يستخدم مركز البيانات رشاشات المياه لكبت الحرائق؛ ولا يستخدم القماش المشمع لحماية الأجهزة والمعدات من تلف المياه	الحرائق والأشخاص المهملين	تشغيل رشاشات المياه في مركز البيانات

الناتج: قائمة نقاط الضعف في النظام (الملاحظات) التي يمكن أن تمارسها مصادر التهديد المحتملة

2.4 تحليل الضوابط

تهدف هذه الخطوة إلي تحليل الضوابط التي تم تنفيذها، أو المخطط تنفيذها، من قبل المؤسسة لتقليل أو القضاء على احتمال استغلال التهديد لنقاط ضعف النظام.

استنتاج تقييم شامل للإحتمال يشير إلى احتمال استغلال إحدى نقاط الضعف المحتملة في إطار بيئة التهديد المرتبطة بها، يجب مراعاة تطبيق الضوابط الحالية أو المخطط لها. على سبيل المثال، لا يُرجح استغلال نقطة الضعف (مثل ضعف النظام أو الضعف الإجرائي) أو يعتبر احتمالها منخفض في حالة انخفاض مستوي اهتمام مصدر التهديد أو قدرته أو في حالة وجود ضوابط أمنية فعالة يمكنها القضاء على أو تقليل حجم الضرر.

يناقش القسمان 4.1 و 4.2 أدناه، على التوالي، طرق التحكم وفئات التحكم.

2.4.1 4.1 طرق التحكم

تشمل الضوابط الأمنية استخدام الأساليب الفنية وغير الفنية. تمثل الضوابط الفنية ضمانات مدمجة في أجهزة أو برمجيات الكمبيوتر أو البرامج الثابتة (على سبيل المثال، آليات التحكم في الوصول، وآليات تحديد الهوية والتوثيق، وطرق التشفير، وبرامج اكتشاف التسلل). تتمثل الضوابط غير الفنية في الضوابط الإدارية والتشغيلية، مثل السياسات الأمنية ؛ الإجراءات التشغيلية؛ والأفراد، والأمن المادي والبيئي.

2.4.2 4.2 فئات التحكم

يمكن تصنيف فئات التحكم لكل من أساليب التحكم الفنية وغير الفنية على أنها إما وقائية أو كشفية. يتم شرح هاتين الفئتين الفرعيتين على النحو التالي:

- تمنع **الضوابط الوقائية** محاولات انتهاك السياسة الأمنية وتشمل عناصر التحكم مثل فرض التحكم في الوصول والتشفير والمصادقة.
- تحذر الضوابط الكشفية من الانتهاكات أو محاولات انتهاك السياسة الأمنية وتتضمن ضوابط مثل طرق التدقيق وطرق كشف التسلل والاختبارات.

يعد تطبيق هذه الضوابط أثناء عملية التخفيف من المخاطر هو النتيجة المباشرة لتحديد أوجه القصور في الضوابط الحالية أو المخططة أثناء عملية تقييم المخاطر (علي سبيل المثال، عدم وجود الضوابط أو أن الضوابط غير مطبقة بشكل صحيح).

الناتج: قائمة الضوابط الحالية أو المخططة المستخدمة لنظام تقنية المعلومات للتخفيف من احتمال استغلال نقطة الضعف وتقليل تأثير مثل هذا الفعل الضار

2.5 تقييم المخاطر

يمكن وصف التأثير السلبي لحدث أمني من حيث فقدان أو تراجع أي، أو مزيج من أي من الأهداف الأمنية الثلاثة التالية: التكامل والتوافر والسرية. توفر القائمة التالية وصفًا موجزًا لكل هدف أمني ونتائج (أو تأثير) عدم الوفاء به:

- **عدم التكامل.** يشير تكامل النظام والبيانات إلى متطلبات حماية المعلومات من التعديل غير الصحيح. يُفقد التكامل إذا تم إجراء تغييرات غير مصرح بها على البيانات أو نظام تقنية المعلومات من خلال أعمال مقصودة أو عرضية. إذا لم يتم تصحيح فقدان النظام أو تكامل البيانات، فقد يؤدي الاستخدام المتواصل للنظام المتأثر أو البيانات التالفة إلى عدم الدقة أو الاحتيال أو اتخاذ قرارات خاطئة. أيضًا، قد يكون انتهاك السلامة الخطوة الأولى في أي هجوم ناجح ضد توفر النظام أو السرية. لكل هذه الأسباب، يقلل عدم التكامل من ضمان نظام تقنية المعلومات.

- **عدم التوافر:** في حالة عدم توافر نظام تقنية المعلومات ذو أهمية حرجة لمستخدميه النهائيين، فقد تتأثر مهمة المؤسسة. حيث يؤدي فقدان وظائف النظام والفعالية التشغيلية، على سبيل المثال، إلى ضياع الوقت الإنتاجي، وهو ما يعوق أداء المستخدمين النهائيين لوظائفهم في دعم مهمة المؤسسة.

- **فقدان السرية.** تشير سرية النظام والبيانات إلى حماية المعلومات من الكشف غير المصرح به. يمكن أن يتراوح تأثير الكشف غير المصرح به عن المعلومات السرية من تهديد الأمن الوطني إلى الكشف عن بيانات قانون الخصوصية. قد يؤدي الإفصاح غير المصرح به أو غير المتوقع أو غير المقصود إلى فقدان ثقة الجمهور أو الإحراج أو اتخاذ إجراء قانوني ضد المؤسسة.

يتم تقييم مخاطر أصول المعلومات بسبب انتهاك السرية والتكامل والتوافر أولاً، ثم يتم احتساب المخاطر المدمجة باستخدام الصيغة المحددة في هذا البند أدناه.

مخاطر السرية = تأثير السرية٪ * احتمالية السرية٪

مخاطر التوفر = تأثير التوفر٪ * احتمالية التوفر٪

مخاطر التكامل = تأثير التكامل٪ * احتمال التكامل٪

2.5.1 تحديد الاحتمالية

لاستنتاج معدل احتمال استغلال إحدى نقاط الضعف المحتملة في سياق بيئة التهديد المرتبطة، يجب مراعاة العوامل الحاكمة التالية:

- دافع مصدر التهديد وقدرته
- طبيعة نقطة الضعف
- وجود وفعالية الضوابط الحالية

يمكن وصف احتمال وجود ثغرة أمنية محتملة من قبل مصدر تهديد معين بأنه مرتفع جدًا أو مرتفع أو متوسط أو منخفض أو منخفض جدًا. يوضح الجدول أدناه هذه المستويات الخمسة.

الجدول الثالث– احتمال الوقوع (خرق السرية والتكامل والتوافر)

التصنيف	البيان	احتمال الوقوع
1	نادر	من غير المرجح للغاية، لكنه قد يحدث في ظروف استثنائية. يمكن أن يحدث، ولكن ربما لن يحدث ذلك أبداً.
2	من غير المرجح	غير متوقع، ولكن هناك احتمال بسيط بأنه قد يحدث في وقت ما.
3	ممكن	قد يقع هذا الحدث في وقت ما حيث يوجد سجل لحوادث عرضية في المؤسسات المماثلة.
4	محتمل	هناك احتمال قوي لوقوع هذا الحدث حيث يوجد سجل لحوادث متكررة في المؤسسات المماثلة.
5	شبه مؤكد	من المحتمل جدا. من المتوقع أن يقع هذا الحدث في معظم الحالات، حيث

التصنيف	البيان	احتمال الوقوع
		يوجد سجل لأحداث منتظمة في المؤسسات المماثلة.

2.5.2 تحديد الأثر

يتم تحديد التأثير السلبي لفقدان سرية المعلومات وتكاملها وتوافر أصول المعلومات الناتجة عن استغلال ثغرة أمنية من خلال التهديد، استناداً إلى حساسية أصل المعلومات ومستوى الحماية المطلوبة. أصحاب أصول المعلومات هم المسؤولون عن تحديد مستوى التأثير لأصول المعلومات الخاصة بهم.

يقدم الجدول أدناه وصفًا للتأثير بمقياس من 1 إلى 5 (مع التصنيفات المناسبة)، ويرد وصفه من خمس وجهات نظر مختلفة (التأثير المالي، صحة وسلامة العملاء والموظفين، انقطاع الأعمال، السمعة والصورة، وأهداف الشركة).

الجدول الرابع– تأثير انتهاك السرية والتكامل والتوافر

التصنيف	البيان	الأثر المالي	العملاء والموظفين الصحة والأمان	انقطاع الأعمال	السمعة والصورة	أهداف الشركة
1	غير هام	الحد الأدنى من الخسائر المالية ؛ أقل من 300000 دولار	بدون أو إصابة شخصية طفيفة فقط ؛ يلزم إجراء الإسعافات الأولية اللازمة ولكن لا يوجد هدر للوقت	ضئيل؛ عدم توافر الأنظمة ذات الأهمية الحرجة لمدة تقل عن ساعة واحدة	تأثير ضئيل	يتم ضمن الأعمال اليومية

2	ضئيل	300.000 دولار إلى 2 مليون دولار ؛ لا يغطيها التأمين	جرح طفيف؛ العلاج الطبي وهدر بعض الأيام	غير مريح؛عدم توافر الأنظمة ذات الأهمية الحرجة لعدة ساعات	تغطية إعلامية سلبية محلية فقط	تأثير طفيف
3	متوسط	2 مليون دولار إلى 5 ملايين دولار ؛ لا يغطيها التأمين	الإصابة ويحتمل دخول المستشفي وهدر الكثير من الأيام	استياء العميل عدم توافر الأنظمة ذات الأهمية الحرجة لمدة تقل عن يوم واحد	تغطية إعلامية سلبية بالعاصمة	تأثير كبير
4	رئيسي	من 5 ملايين دولار إلى 10 ملايين دولار ؛ لا يغطيها التأمين	وفاة واحدة و / أو مرض طويل الأجل أو إصابات خطيرة متعددة	عدم توافر الأنظمة ذات الأهمية الحرجة ليوم واحد أو سلسلة من الانقطاعات الطويلة	تغطية إعلامية سلبية واسعة على المستوى الوطني	تأثير رئيسي
5	كارثي	أكثر من 10 مليون دولار ؛ لا يغطيها التأمين	حالة (حالات) الوفاة أو العجز الدائم أو اعتلال الصحة	عدم توافر الأنظمة ذات الأهمية الحرجة لأكثر من يوم (في وقت حرج)	طلب التحقيق الحكومي	تأثير كارثي

ملاحظة: يجب على المؤسسات تحديث نطاق التأثير المالي في الجدول أعلاه مع الأخذ في الاعتبار الرغبة في المخاطرة ودليل الصلاحيات المالية.

وبالتالي، قد تتراوح درجة المخاطر (بالنسبة إلى السرية والتكامل والتوافر) بين 1 (القيمة الدنيا) و 5 (القيمة القصوى).
التأثير على الأعمال = 1 إلى 5
الاحتمالية = 1 إلى 5
من المهم حساب درجة المخاطر حيث أنها تساعد في تحديد أولويات معالجة والتعامل مع المخاطر. إذا قمنا بمعالجة المخاطر على الأصول ذات درجة المخاطر المنخفضة، فقد تكون تكلفة التخفيف من المخاطر على تلك الأصول أعلى بكثير من الخسارة التي قد تسببها للشركة.

الجدول الخامس– مصفوفة تأثير المخاطر

		الأثر				
		1	2	3	4	5
الاحتمالية	1	1	2	3	4	5
	2	2	4	6	8	10
	3	3	6	9	12	15
	4	4	8	12	16	20
	5	5	10	15	20	25

الجدول السادس– تعريفات أثر المخاطر

القيم النوعية	القيم شبه الكمية	البيان
عالي جدا	25–21	تعني أن المخاطر عالية جدًا وأنه من المتوقع أن يكون لحدث التهديد تأثيرات **خطيرة متعددة** أو **كارثية** على العمليات التنظيمية أو الأصول التنظيمية أو الأفراد أو المؤسسات الأخرى أو الدولة.
عالي	20 –16	تعني أن المخاطر عالية وأنه يمكن توقع أن يكون لحدث التهديد تأثير **سلبي شديد أو كارثي** على العمليات التنظيمية أو الأصول التنظيمية أو الأفراد أو المؤسسات الأخرى أو الدولة.
متوسط	15–10	تعني أن المخاطر متوسطة وأنه من المتوقع أن يكون لحدث التهديد تأثير **سلبي خطير** على العمليات التنظيمية أو الأصول التنظيمية أو الأفراد أو المؤسسات الأخرى أو الدولة.
منخفض	9–6	تعني أن المخاطر منخفضة وأنه من المتوقع أن يكون لحدثال تهديد **تأثير سلبي محدود** على العمليات التنظيمية أو الأصول التنظيمية أو الأفراد أو المؤسسات الأخرى أو الدولة.

منخفض جدا	1–5	تعني ـن المخاطر منخفضة جدًا وأنه من المتوقع أن يكون لحدث التهديد **تأثير سلبي ضئيل** على العمليات التنظيمية أو الأصول التنظيمية أو الأفراد أو المؤسسات الأخرى أو الدولة.

2.5.3 معدل المخاطر المشتركة

لا تمثل المخاطر المشتركة (CR) متوسطًا عامًا يعتمد على قيم السرية (C) والتكامل (I) والتوافر (A)،بل هو المتوسط المرجح حيث يتم أخذ جميع الشروط الأخرى من تقييم التأثير في الاعتبار.

عندما يلزم إيجاد قيمة المخاطر المشتركة، عادة ما يختار المرء بين:

1. المتوسط
2. أسوأ حالة

ومع ذلك، في الحالات التي تختلف فيها قيمة واحدة فقط عن الأخرى، فإن المتوسط سيخفي القيمة المنحرفة، وتصبح الحالة الأسوأ عالية للغاية. لذلك اخترنا استخدام كل من الحالات المتوسطة والأسوأ.

استخدم الصيغة التالية لحساب المخاطر المشتركة

المخاطر المشتركة = (المتوسط + أسوأ حالة) / 2

حيث أن:

المتوسط = (مخاطر السرية + مخاطر التكامل + مخاطر التوافر) / 3

أسوأ حالة = أعلى قيمة للمخاطر بين مخاطر السرية ومخاطر التكامل ومخاطر التوافر

2.6 معايير قبول المخاطر

تقبل إدارة [المؤسسة الحكومية] المخاطر بقيمة 9 (تسعة) أو أقل وفقًا لإطار إدارة المخاطر الخاص بـ [المؤسسة الحكومية]. ستعتبر أي قيمة مخاطر أعلي من 9 (تسعة) بمثابة انحراف ويجب أن تقبل إدارة [المؤسسة الحكومية] المخاطر باعتبارها انحرافًا أو تتخذ خطوات إضافية لضمان إبقاء قيمة المخاطرة ضمن الحد.

الجدول السابع– نطاق قبول المخاطر

فئة المخاطر	نطاق المخاطر
منخفضة للغاية	1 إلي 5
منخفضة	6 إلي 9
متوسطة	10–15
مرتفعة	16 إلي 20
مرتفعة للغاية	21 إلي 25

3 معالجة المخاطر

تم الوصول إلى خطة معالجة المخاطر على أساس تحليل المخاطر الذي تم القيام به. سيوفر تحليل المخاطر مؤشرات حول مجالات التحسين. سيتم تحديد وتوثيق خطة التصحيح كجزء من مصفوفة تقييم المخاطر. سيعطي هذا صورة كاملة لدورة الحياة الكاملة لتقييم المخاطر والتخفيف من حدتها. سيتم تغطية هذا في العمود "تخفيف المخاطر" في مصفوفة تقييم المخاطر.

3.1 طرق معالجة المخاطر

3.1.1 تخفيف المخاطر

للحد من المخاطر من خلال تطبيق الضوابط التي تقلل من التأثير السلبي للتهديد على الأصول. لا يضمن تطبيق خادم مكافحة الفيروسات في المؤسسة أن الأصول سوف تكون محمية من هجمات الفيروسات. هذه طريقة لتقليل مخاطر هجمات الفيروسات المعروفة. لذلك من خلال تطبيق مكافحة الفيروسات والحفاظ على تحديث تعريفات الفيروسات، فإننا نحد من خطر هجوم الفيروس. وأيضًا من خلال أخذ نسخة احتياطية بتواتر منتظم، فإننا نحد من تأثير التهديد إذا تحقق ذلك.

3.1.2 نقل المخاطر

لنقل المخاطر باستخدام خيارات أخرى للتعويض عن الخسارة، مثل شراء التأمين. يمكن أيضًا نقل المخاطر عن طريق الاستعانة بمصادر خارجية (إبرام عقد مع الموردين الخارجييننفي صورة عقود صيانة أو أي اتفاق آخر بوجود قطع غيار في موقعنا.

3.1.3 تجنب المخاطر

لتجنب المخاطر عن طريق القضاء على سبب و / أو نتيجة الخطر. إذا كان هناك نظام قديم (نظام التشغيل Windows 98 يشغل بعض التطبيقات القديمة / تطبيقات الملكية)، والذي لا يمكن تصحيحه بسبب الثغرات الحالية، فيمكن إيقاف تشغيله عن الشبكة لتجنب المخاطر.

3.1.4 قبول المخاطر

قد لا يمكن دائماً أو لا يصح من الناحية المالية تقليل المخاطر إلى مستوى مقبول. في هذه الظروف، قد يكون من الضروري قبول الخطر عن قصد وبصورة موضوعية.

علي سبيل المثال: نظراً لبعض الأغراض المختبرية، فقد نحتاج إلى نقل أحد الخوادم إلى المنطقة التي تفصل بين الشبكة الداخلية والشبكة الخارجية (DMZ) لفترة زمنية محددة. نظرًا لأن هذا الاختبار إلزامي، يمكن اعتباره خطرًا مقبولًا لتلك الفترة. ولكن هذا يجب أن يتم الاتفاق عليه من قبل الإدارة وأصحاب الأصول.

أو تطبيق ضوابط لخفض المخاطر إلى مستوى مقبول. نحتاج إلى إعطاء أولوية عالية لمتطلبات العمل، مع مراعاة أيضًا كيفية حماية المعلومات. في بعض الحالات نحتاج إلى قبول بعض المخاطر والتأكد من الوفاء بمتطلبات العمل.

3.1.5 المخاطر المتبقية

عد تنفيذ قرارات معالجة المخاطر، ستكون هناك دائمًا مخاطر ذات قيم أعلى من الحد المقبول – تسمى هذه المخاطر "المخاطر المتبقية". يتم عرض المخاطر المتبقية على الإدارة للقبول وتوافق الإدارة على قبول المخاطر المتبقية. يتم توثيق المخاطر المتبقية المقبولة والمعتمدة من قبل الإدارة.

سيتم إعادة النظر في جميع المخاطر المتبقية في كل مرة يتم فيها مراجعة تقييم المخاطر أو اكتشاف تهديد جديد.

4 الملحق أ– قائمة التهديدات ونقاط الضعف

تتمثل إحدى خطوات التخطيط الأولي في برنامج إدارة المخاطر في إنشاء قائمة شاملة بمصادر التهديدات والمخاطر والأحداث التي قد يكون لها تأثير على قدرة المؤسسة على تحقيق أهدافها علي النحو المحدد في تعريف النطاق و الإطار. قد تمنع هذه الأحداث أو تسهم في تراجع أو تؤخر أو تعزز تحقيق تلك الأهداف.

بشكل عام، يمكن أن تكون المخاطر مرتبطة أو تتميز بما يلي:

• الأصل – على سبيل المثال، عوامل التهديد مثل الموظفين العدائيين، والموظفين غير المدربين تدريباً جيداً، والمنافسين، والحكومات، إلخ.

• نشاط أو حدث أو حادثة معينة (مثل التهديد) – على سبيل المثال، النشر غير المصرح به للبيانات السرية، تطبيق المنافسين لسياسة تسويقية جديدة، أو لوائح حماية بيانات جديدة أو منقحة، وانقطاع الطاقة بشكل واسع

• عواقبها أو نتائجها أو أثرها – على سبيل المثال، عدم توفر الخدمة أو فقدان أو زيادة حصتها / أرباحها السوقية، زيادة التنظيم، زيادة أو نقصان القدرة التنافسية، العقوبات، إلخ.

• سبب محدد لحدوثها – على سبيل المثال، خطأ في تصميم النظام أو تدخل بشري أو تنبؤ أو فشل في التنبؤ بنشاط المنافس

• آليات وضوابط الحماية (إلى جانب افتقارها المحتمل إلى الفعالية) – على سبيل المثال، أنظمة التحكم في الوصول والكشف عنه، والسياسات، والتدريب الأمني، وبحوث السوق، ومراقبة السوق

• زمان ومكان حدوثها – على سبيل المثال، حدوث فيضان في غرفة الكمبيوتر أثناء الظروف البيئية القاسية.

4.1 التهديدات

- انقطاع الكهرباء
- فقدان خدمات الدعم
- تعطل المعدات
- الرموز الخبيثة
- إساءة استخدام نظم المعلومات
- إساءة استخدام أدوات التدقيق
- التلوث
- الهندسة الاجتماعية
- أخطاء البرمجيات
- الإضراب
- الهجمات الإرهابية
- السرقة
- الصواعق
- التغيير غير المقصود للبيانات في نظام المعلومات
- الوصول غير المصرح به إلى نظام المعلومات
- التغييرات غير المصرح بها للسجلات
- التثبيت غير المصرح به للبرنامج
- الوصول المادي غير المصرح به
- الاستخدام غير المصرح به لمواد حقوق النشر
- الاستخدام غير المصرح به للبرنامج
- أخطاء المستخدم
- التخريب
- الوصول إلى الشبكة من قبل أشخاص غير مصرح لهم
- الهجوم بقنبلة
- التهديد بوجود قنبلة
- خرق العلاقات التعاقدية
- خرق التشريعات
- الإخلال بالمعلومات السرية
- إخفاء هوية المستخدم
- الأضرار الناجمة عن الغير
- الأضرار الناتجة عن اختبار الاختراق
- إتلاف السجلات
- الكوارث (الناتجة بفعل الإنسان)
- الكوارث (الطبيعية)
- الإفصاح عن المعلومات
- الكشف عن كلمات المرور
- التنصت
- الاختلاس
- أخطاء في الصيانة
- فشل خطوط الاتصالات
- تزوير السجلات
- الحريق
- الفيضانات
- الاحتيال
- التجسس الصناعي
- توقف أعمال المؤسسة

4.2 نقاط الضعف

- عدم كفاية اختبار البرمجيات
- الافتقار إلي سياسة التحكم في الوصول
- الافتقار إلي سياسة نظافة المكتب ووضوح الشاشة
- الافتقار إلي التحكم في بيانات المدخلات والمخرجات
- الافتقار إلي الوثائق الداخلية
- الافتقار إلي أو سوء تنفيذ أعمال التدقيق الداخلي
- الافتقار إلي سياسة استخدام التشفير
- الافتقار إلي إجراءات إزالة حقوق الوصول عند إنهاء العمل
- الافتقار إلي حماية للمعدات المحمولة
- الافتقار إلي وجود أنظمة/ أجهزة إحتياطية
- الافتقار إلي أنظمة لتحديد الهوية والتوثيق
- الافتقار إلي التحقق من صحة البيانات التي تمت معالجتها
- الموقع عرضة للفيضانات
- سوء اختيار بيانات الاختبار
- التحميل غير المراقب من الإنترنت
- الاستخدام غير المنضبط لأنظمة المعلومات
- عدم دافعية الموظفين
- عدم حماية وصلات الشبكة العامة
- عدم مراجعة حقوق المستخدم بانتظام
- عدم تغيير كلمات السر الافتراضية
- التخلص من وسائط التخزين دون حذف البيانات
- حساسية المعدات للرطوبة والملوثات
- حساسية المعدات لدرجة الحرارة
- عدم كفاية أمن الكوابل
- عدم كفاية إدارة القدرات
- عدم كفاية إدارة التغيير
- عدم كفاية تصنيف المعلومات
- عدم كفاية التحكم في الوصول المادي
- عدم كفاية الصيانة
- عدم كفاية إدارة الشبكة
- عدم كفاية أو عدم انتظام النسخ الاحتياطي
- عدم كفاية إدارة كلمة المرور
- عدم كفاية الحماية المادية
- عدم كفاية حماية مفاتيح التشفير
- عدم كفاية استبدال المعدات القديمة
- • عدم كفاية الوعي الأمني
- • عدم كفاية الفصل بين المهام
- عدم كفاية الفصل بين مرافق التشغيل والاختبار
- عدم كفاية الإشراف على الموظفين
- عدم كفاية الإشراف على الموردين
- عدم كفاية تدريب الموظفين
- عدم اكتمال مواصفات تطوير البرمجيات