هذا المربع مخصّص لأغراض توجيهية. احذف جميع المربعات التوجيهية بعد تعبئة النموذج. يجب تحرير البنود الملوّنة باللون الأزرق بصورة مناسبة. ويجب إزالة التظليل الملون بعد إجراء التعديلات.

أدخل شعار الجهة بالضغط على الصورة الموضحة.

نموذج إجراء إدارة مخاطر الأمن السيبراني

اختر التصنيف

التاريخ: اضغط هنا لإضافة تاريخ

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

استبدل <اسم الجهة> باسم الجهة في مجمل صفحات الوثيقة. وللقيام بذلك، اتبع الخطوات التالية:

- اضغط على مفتاحي "Ctrl" و"H" في الوقت نفسه.
- أضف "<اسم الجهة>" في مربع البحث عن النص.
- أدخل الاسم الكامل لجهتك في مربع "استبدال" النص.
- اضغط على "المزيد" وتأكّد من اختيار "Match case".
- اضغط على "استبدل الكل".
- أغلق مربع الحوار.

إخلاء المسؤولية

طُور هذا النموذج عن طريق الهيئة الوطنية للأمن السيبراني كمثال توضيحي يمكن استخدامه كدليل ومرجع للجهات. يجب أن يتم تعديل هذا النموذج ومواءمته مع أعمال <اسم الجهة> والمتطلبات التشريعية والتنظيمية ذات العلاقة. كما يجب أن يُعتمد هذا النموذج من قبل رئيس الجهة أو من يقوم/تقوم بتفويضه. وتخلي الهيئة مسؤوليتها من استخدام هذا النموذج كما هو، وتؤكد على أن هذا النموذج ما هو إلا مثال توضيحي.

اختر التصنيف

الإصدار <١,٠>

اعتماد الوثيقة

الدور	المسمى الوظيفي	الاسم	التاريخ	التوقيع
اختر الدور	<أدخل المسمى الوظيفي>	<أدخل الاسم الكامل للموظف>	اضغط هنا لإضافة تاريخ	<أدخل التوقيع>

نسخ الوثيقة

النسخة	التاريخ	عُدِّلَ بواسطة	أسباب التعديل
<أدخل رقم النسخة>	اضغط هنا لإضافة تاريخ	<أدخل الاسم الكامل للموظف>	<أدخل وصف التعديل>

جدول المراجعة

معدل المراجعة	التاريخ لأخر مراجعة	تاريخ المراجعة القادمة
مره واحدة كل سنة	اضغط هنا لإضافة تاريخ	اضغط هنا لإضافة تاريخ

قائمة المحتويات

الغرض

يهدف هذا الإجراء إلى تحديد المتطلبات التفصيلية المتعلقة بعملية إدارة مخاطر الأمن السيبراني في <اسم الجهة>. وتتوافق هذه المتطلبات مع أفضل الممارسات في هذا المجال و تتوافق مع سياسة إدارة المخاطر في <اسم الجهة>.

كما تمت مواءمة هذه المتطلبات مع متطلبات الأمن السيبراني الصادرة عن الهيئة الوطنية للأمن السيبراني وتشمل، على سبيل المثال لا الحصر: الضوابط الأساسية للأمن السيبراني (ECC – ١: ٢٠١٨)، وضوابط الأمن السيبراني للأنظمة الحساسة (CSCC – ١: ٢٠١٩) وغيرها من المتطلبات التشريعية والتنظيمية ذات العلاقة.

نطاق الإجراء

يغطي هذا الإجراء عملية إدارة مخاطر الأمن السيبراني لدى <اسم الجهة> وينطبق على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

لمحة عامة عن عملية إدارة مخاطر الأمن السيبراني

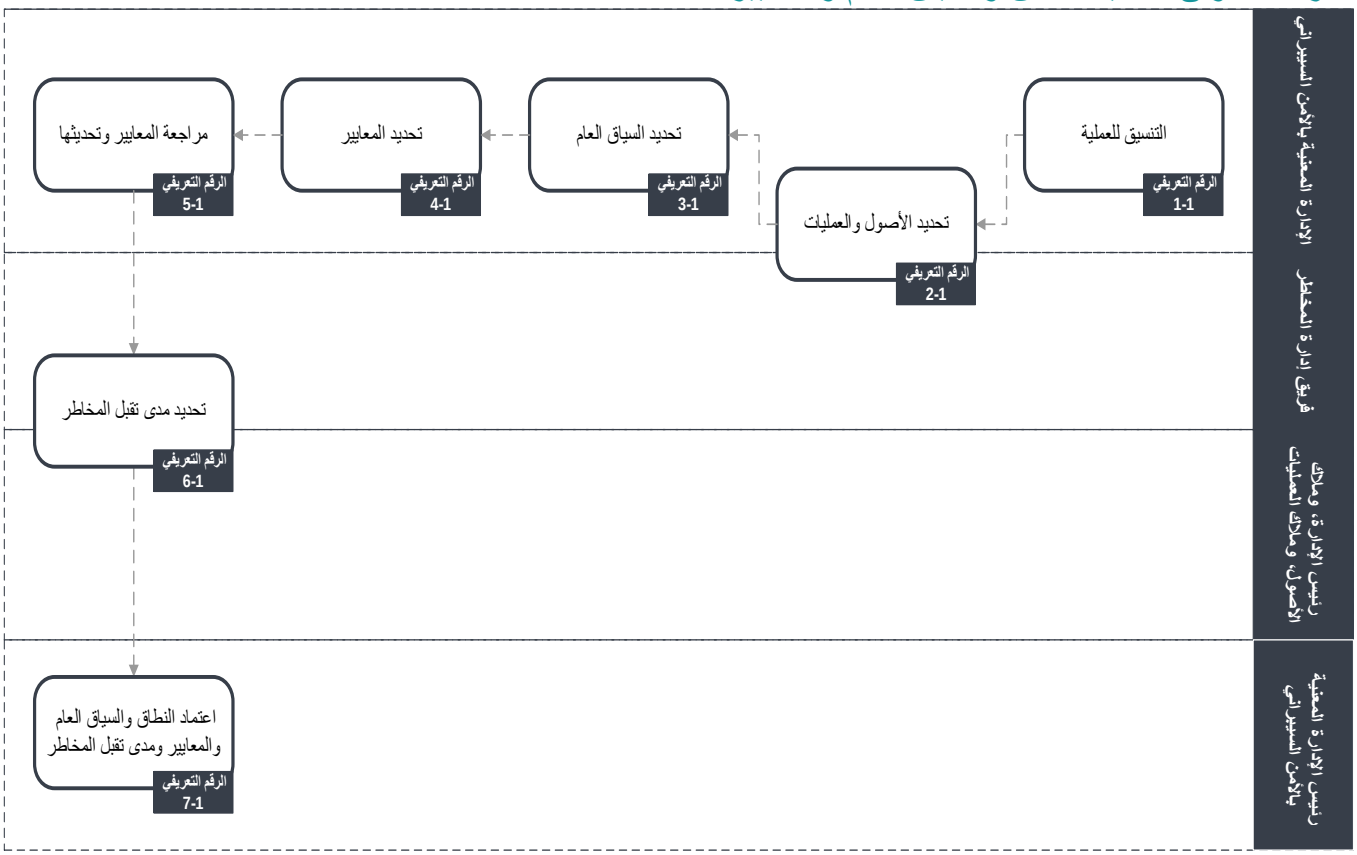
يجب أن تعتمد عملية إدارة مخاطر الأمن السيبراني على الخطوات التالية:

١. تحديد النطاق والسياق العام والمعايير
٢. عملية تقييم مخاطر الأمن السيبراني
   ٢,١ تحديد المخاطر
   ٢,٢ تحليل المخاطر
   ٢,٣ تقييم المخاطر
٣. معالجة مخاطر الأمن السيبراني
٤. التسجيل وإعداد التقارير
٥. التواصل والمتابعة

الشكل ١ - لمحة عامة عن مراحل الإجراء

تفاصيل عملية إدارة مخاطر الأمن السيبراني

المرحلة الأولى: تحديد النطاق والسياق العام والمعايير



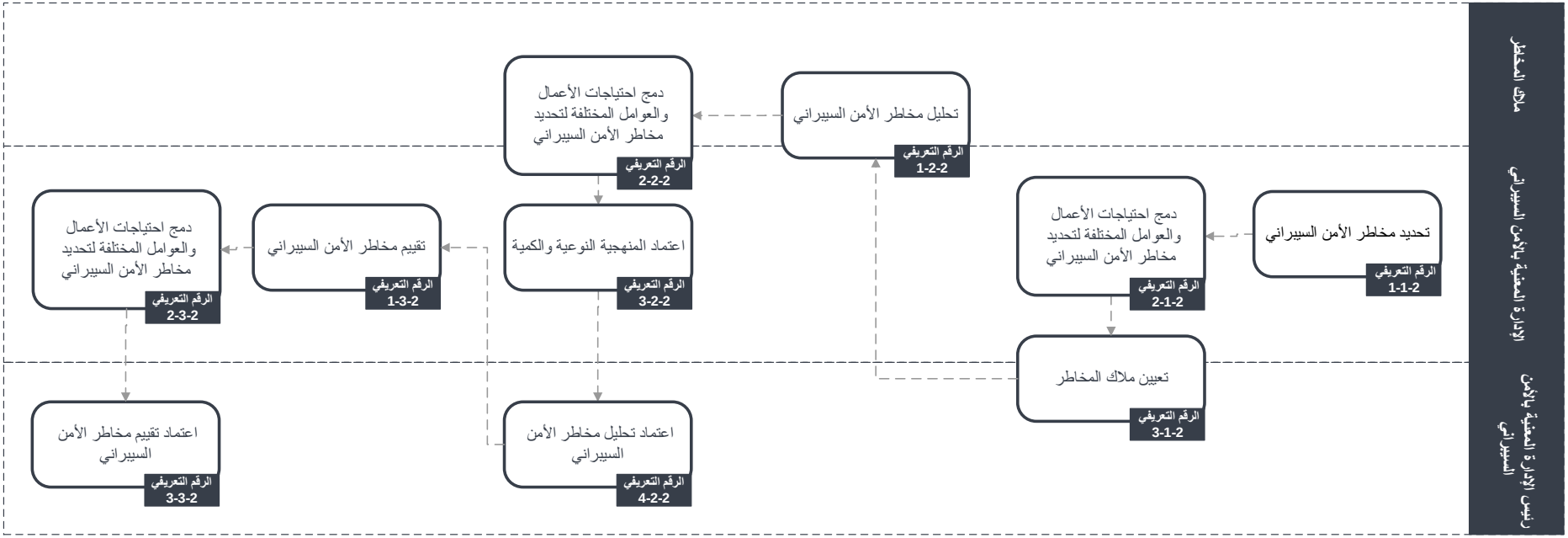
الشكل ٢ - مخطط سير العمل في مرحلة تحديد النطاق والسياق العام والمعايير

الرقم	الخطوة	الوصف	المالك / المسؤول	المُدخلات	المُخرجات	الأطراف المعنية
١-١	التنسيق للعملية	التنسيق لعملية إدارة مخاطر الأمن السيبراني بالكامل في <اسم الجهة>.	الإدارة المعنية بالأمن السيبراني	الوثائق الحالية المتعلقة بإدارة مخاطر الأمن السيبراني	خطوات العملية المنسقة	الإدارة المعنية بالأمن السيبراني
١-٢	تحديد الأصول والعمليات	يجب تحديد الأصول والعمليات ذات الصلة بـ <اسم الجهة> وطريقة استخدامها من جانب <اسم الجهة>.	الإدارة المعنية بالأمن السيبراني، ورئيس الإدارة، وملاك الأصول، وملاك العمليات	الأصول والعمليات في <اسم الجهة>	الأصول والعمليات ذات الصلة المحددة لدى <اسم الجهة>	الإدارة المعنية بالأمن السيبراني، ورئيس الإدارة، وملاك الأصول، وملاك العمليات
١-٣	تحديد السياق العام	يجب تحديد السياق العام الداخلي والخارجي لعملية إدارة مخاطر الأمن السيبراني الذي تسعى فيه <اسم الجهة> إلى تحديد وتحقيق أهدافها. ويجب أن يستند السياق العام لعملية إدارة مخاطر الأمن السيبراني إلى فهم البيئة الخارجية والداخلية التي تعمل فيها <اسم الجهة> وأن يعكس البيئة المحددة للنشاط الذي سيتم تطبيق العملية عليه. ويجب مراعاة العوامل التالية على وجه التحديد: ١. مواءمة تقييم مخاطر الأمن السيبراني مع العلاقات والأهداف والسياسات الداخلية. ٢. نموذج الأنظمة والتقنيات (البنية التحتية والأصول). ٣. العوامل الاجتماعية والثقافية والسياسية والتشريعية والتنظيمية والمالية والتقنية والاقتصادية، سواءً كانت	الإدارة المعنية بالأمن السيبراني	أهداف وغايات <اسم الجهة> والأصول الموجودة والعوامل الخارجية	السياق العام المحدد لإدارة مخاطر الأمن السيبراني في <اسم الجهة>	الإدارة المعنية بالأمن السيبراني

الرقم	الخطوة	الوصف	المالك / المسؤول	المُدخلات	المُخرجات	الأطراف المعنية
		على الصعيد الدولي أو الوطني أو الإقليمي أو المحلي، التي قد تؤثر على تقييم مخاطر الأمن السيبراني. ٤. علاقات وتصورات وقيم واحتياجات وتوقعات الجهات المعنية الخارجية. العلاقات التعاقدية والالتزامات والترتيبات مع الموردين الخارجيين.				
٤-١	تحديد المعايير	يجب تحديد معايير تقييم مدى أهمية مخاطر الأمن السيبراني ودعم عمليات اتخاذ القرار. ويجب أن تكون معايير تقييم مخاطر الأمن السيبراني متوافقة مع إطار إدارة مخاطر الأمن السيبراني لدى <اسم الجهة> وأن يتم تخصيصها بما يتناسب مع الغرض المحدد ونطاق النشاط الخاضع للدراسة. كما يجب أن تعكس معايير تقييم مخاطر الأمن السيبراني قيم وأهداف وموارد <اسم الجهة> وأن تكون متسقة مع السياسات والبيانات المتعلقة بإدارة مخاطر الأمن السيبراني. ويجب تحديد المعايير مع مراعاة التزامات <اسم الجهة> وآراء الجهات المعنية. ولتحديد المعايير، يجب مراعاة ما يلي: ١. طبيعة ونوع الشكوك التي قد تؤثر على النتائج والأهداف (الملموسة وغير الملموسة) ٢. كيفية تحديد وقياس العواقب (الإيجابية والسلبية) والاحتمالية ٣. العوامل المرتبطة بالوقت	الإدارة المعنية بالأمن السيبراني	السياق العام المحدد لإدارة مخاطر الأمن السيبراني	المعايير المحددة لتقييم إدارة مخاطر الأمن السيبراني	الإدارة المعنية بالأمن السيبراني

الرقم	الخطوة	الوصف	المالك / المسؤول	المُدخلات	المُخرجات	الأطراف المعنية
		٤. الاتساق في استخدام المقاييس ٥. كيفية تحديد مستوى مخاطر الأمن السيبراني ٦. كيفية مراعاة مجموعات وتسلسلات العديد من مخاطر الأمن السيبراني قدرات <اسم الجهة>.				
١-٥	مراجعة المعايير وتحديثها	رغم أنه يجب تحديد معايير تقييم المخاطر في بداية عملية تقييم مخاطر الأمن السيبراني، إلا أنها ديناميكية ويجب مراجعتها وتعديلها باستمرار، إذا لزم الأمر.	الإدارة المعنية بالأمن السيبراني	المعايير المحددة لتقييم إدارة مخاطر الأمن السيبراني	المعايير المراجعة والمحدّثة	الإدارة المعنية بالأمن السيبراني
١-٦	تحديد مدى تقبل المخاطر	يجب تحديد مدى تقبل مخاطر الأمن السيبراني. كما يجب تحديد معايير تقبل مخاطر الأمن السيبراني وتوثيقها وفقًا لمستوى تلك المخاطر وتكلفة معالجتها مقارنةً بتأثيرها.	الإدارة المعنية بالأمن السيبراني، وفريق إدارة المخاطر	النطاق والسياق العام والمعايير المحددة	تحديد مدى تقبل مخاطر الأمن السيبراني	الإدارة المعنية بالأمن السيبراني، وفريق إدارة المخاطر
١-٧	اعتماد النطاق والسياق العام والمعايير ومدى تقبل المخاطر	يجب اعتماد النطاق والسياق العام والمعايير ومدى تقبل مخاطر الأمن السيبراني المحددة.	رئيس الإدارة المعنية بالأمن السيبراني	النطاق والسياق العام والمعايير ومدى تقبل المخاطر المحددة	اعتماد النطاق والسياق العام والمعايير ومدى تقبل المخاطر	رئيس الإدارة المعنية بالأمن السيبراني

المرحلة الثانية: عملية تقييم مخاطر الأمن السيبراني



الشكل ٣ - مخطط سير العمل في مرحلة تقييم مخاطر الأمن السيبراني

المرحلة ٢-١: تحديد مخاطر الأمن السيبراني

الرقم	الخطوة	الوصف	المالك / المسؤول	المُدخلات	المُخرجات	الأطراف المعنية
٢-١-١	تحديد مخاطر الأمن	يجب تحديد مخاطر الأمن السيبراني على أعمال أو أصول أو موظفي <اسم الجهة>. والغرض من تحديد مخاطر الأمن السيبراني	الإدارة المعنية بالأمن	المعلومات عن أعمال وأصول وموظفي <اسم	مخاطر الأمن السيبراني	الإدارة المعنية بالأمن

اختر التصنيف

الإصدار <١,٠>

الرقم	الخطوة	الوصف	المالك / المسؤول	المُدخلات	المُخرجات	الأطراف المعنية
	السيبراني	هو تحديد المخاطر التي قد تساعد الجهة أو تمنعها من تحقيق أهدافها وإدراك تلك المخاطر ووصفها. ويجب تحديد جميع الأحداث والظروف التي قد تضر بسرية وسلامة وتوافر المعلومات والأصول التقنية. ويشمل ذلك، على وجه الخصوص، تحديد الأصول المعلوماتية والتقنية والتهديدات التي من المحتمل أن تتعرّض لها والثغرات ذات الصلة والضوابط المطبقة، ثمّ تحديد الآثار الناجمة عن فقدان سريّة هذه الأصول وسلامتها وتوافرها. يجب تحديد مخاطر الأمن السيبراني، سواءً كانت مصادرها تحت سيطرة ملاك المخاطر أم لا، ولكنها في مجال اهتماماتهم. ويجب مراعاة أنه قد يكون هناك أكثر من نوع واحد من النتائج، مما قد يؤدي إلى مجموعة متنوعة من التداعيات الملموسة وغير الملموسة.	السيبراني	الجهة>	المحددة	السيبراني
٢-١-٢	دمج احتياجات الأعمال والعوامل المختلفة لتحديد مخاطر الأمن السيبراني	تجب مراعاة العوامل التالية خلال عملية تحديد مخاطر الأمن السيبراني: ١. مصادر مخاطر الأمن السيبراني الملموسة وغير الملموسة. ٢. الأسباب والأحداث. ٣. التهديدات والفرص. ٤. الثغرات والقدرات.	الإدارة المعنية بالأمن السيبراني	مخاطر الأمن السيبراني واحتياجات الأعمال المحددة	القائمة المعدلة لمخاطر الأمن السيبراني	الإدارة المعنية بالأمن السيبراني

الرقم	الخطوة	الوصف	المالك / المسؤول	المُدخلات	المُخرجات	الأطراف المعنية
		٥. التغيرات في السياق العام الخارجي والداخلي. ٦. مؤشرات مخاطر الأمن السيبراني الناشئة. ٧. طبيعة وقيمة الأصول والموارد. ٨. العواقب وتأثيرها على الأهداف. ٩. القيود المتعلقة بالمعرفة وموثوقية المعلومات. ١٠. العوامل المرتبطة بالوقت. ١١. تحيزات وافتراضات ومعتقدات المشاركين.				
٢-١-٣	تعيين ملاك المخاطر	يجب تعيين ملاك المخاطر، وتعيين رؤساء الإدارات أو ملاك الأصول والعمليات الذين سيشاركون في عملية إدارة مخاطر الأمن السيبراني.	رئيس الإدارة المعنية بالأمن السيبراني، والإدارة المعنية بالأمن السيبراني	قائمة مخاطر الأمن السيبراني	تعيين الملاك لكل خطر من مخاطر الأمن السيبراني المحددة	رئيس الإدارة المعنية بالأمن السيبراني، وملاك المخاطر، والإدارة المعنية بالأمن السيبراني

المرحلة ٢-٢: تحليل مخاطر الأمن السيبراني

الرقم	الخطوة	الوصف	المالك / المسؤول	المُدخلات	المُخرجات	الأطراف المعنية
٢-٢-١	تحليل مخاطر الأمن	يجب تحليل مخاطر الأمن السيبراني الكامنة المحددة بالتنسيق مع جميع الجهات المعنية. كما يجب تقييم احتمالية وقوع التهديدات	الإدارة المعنية بالأمن السيبراني، وملاك	قائمة مخاطر الأمن	المستوى التقديري لكل خطر من مخاطر الأمن	الإدارة المعنية بالأمن السيبراني، وملاك

الرقم	الخطوة	الوصف	المالك / المسؤول	المُدخلات	المُخرجات	الأطراف المعنية
	السيبراني	وحجمها / تأثيرها وتداعياتها، مع تقدير المستوى العام لمخاطر الأمن السيبراني بناءً على ذلك.	المخاطر	السيبراني	السيبراني	المخاطر
٢-٢-٢	دمج احتياجات الأعمال والعوامل المختلفة لتحديد مخاطر الأمن السيبراني	عند تحليل المخاطر، ينبغي إجراء دراسة تفصيلية للشكوك ومصادر مخاطر الأمن السيبراني والتداعيات واحتمالية الحدوث والأحداث والسيناريوهات والضوابط ومستوى الفعالية. يجب مراعاة الاختلاف في الآراء والتحيزات والتصورات بشأن مخاطر الأمن السيبراني والأحكام وجودة المعلومات المستخدمة والافتراضات والاستثناءات المطبقة وأي قيود تتعلق بالتقنيات وكيفية تنفيذها، لأنها قد تؤثر على تحليل مخاطر الأمن السيبراني. ويجب توثيق هذه العوامل وتعميمها على صانعي القرار.	الإدارة المعنية بالأمن السيبراني، وملاك المخاطر	قائمة مخاطر الأمن السيبراني، والمستوى التقديري لكل خطر من مخاطر الأمن السيبراني	القائمة المعدلة لمخاطر الأمن السيبراني	الإدارة المعنية بالأمن السيبراني، وملاك المخاطر
٣-٢-٢	اعتماد المنهجية النوعية والكمية	يمكن اعتماد منهجية نوعية أو كمية، أو كليهما، لتحليل مخاطر الأمن السيبراني الكامنة بناءً على المنهجية المستخدمة في الإدارة المعنية بإدارة المخاطر. ويجب اعتماد المنهجية الكمّية لتحليل كل خطر من مخاطر الأمن السيبراني من أجل حساب التصنيف العام للمخاطر وتقييم مستوى أهميتها ومقارنتها بمدى تقبل المخاطر. كما يجب استخدام المنهجية النوعية لتقييم كل خطر من المخاطر المعقدة، مع ضرورة مراعاة العديد من العوامل. ويمكن استخدام المنهجية النوعية كأساس جيد لاستخدام المنهجية الكمية.	الإدارة المعنية بالأمن السيبراني	قائمة مخاطر الأمن السيبراني	التصنيف العام المحتسب للمخاطر، ومستوى الأهمية المقيَّم مقارنةً بمدى تقبل المخاطر	الإدارة المعنية بالأمن السيبراني
٤-٢-٢	اعتماد تحليل مخاطر	يجب اعتماد نتائج تحليل مخاطر الأمن السيبراني.	رئيس الإدارة المعنية	قائمة مخاطر الأمن السيبراني، والتصنيف	النتائج المعتمدة لتحليل	رئيس الإدارة المعنية

اختر التصنيف

الإصدار <١,٠>

الرقم	الخطوة	الوصف	المالك / المسؤول	المُدخلات	المُخرجات	الأطراف المعنية
	الأمن السيبراني		بالأمن السيبراني	العام المحتسب للمخاطر، ومستوى الأهمية المقيَّم مقارنةً بمدى تقبل المخاطر	مخاطر الأمن السيبراني	بالأمن السيبراني

المرحلة ٢-٣: تقييم مخاطر الأمن السيبراني

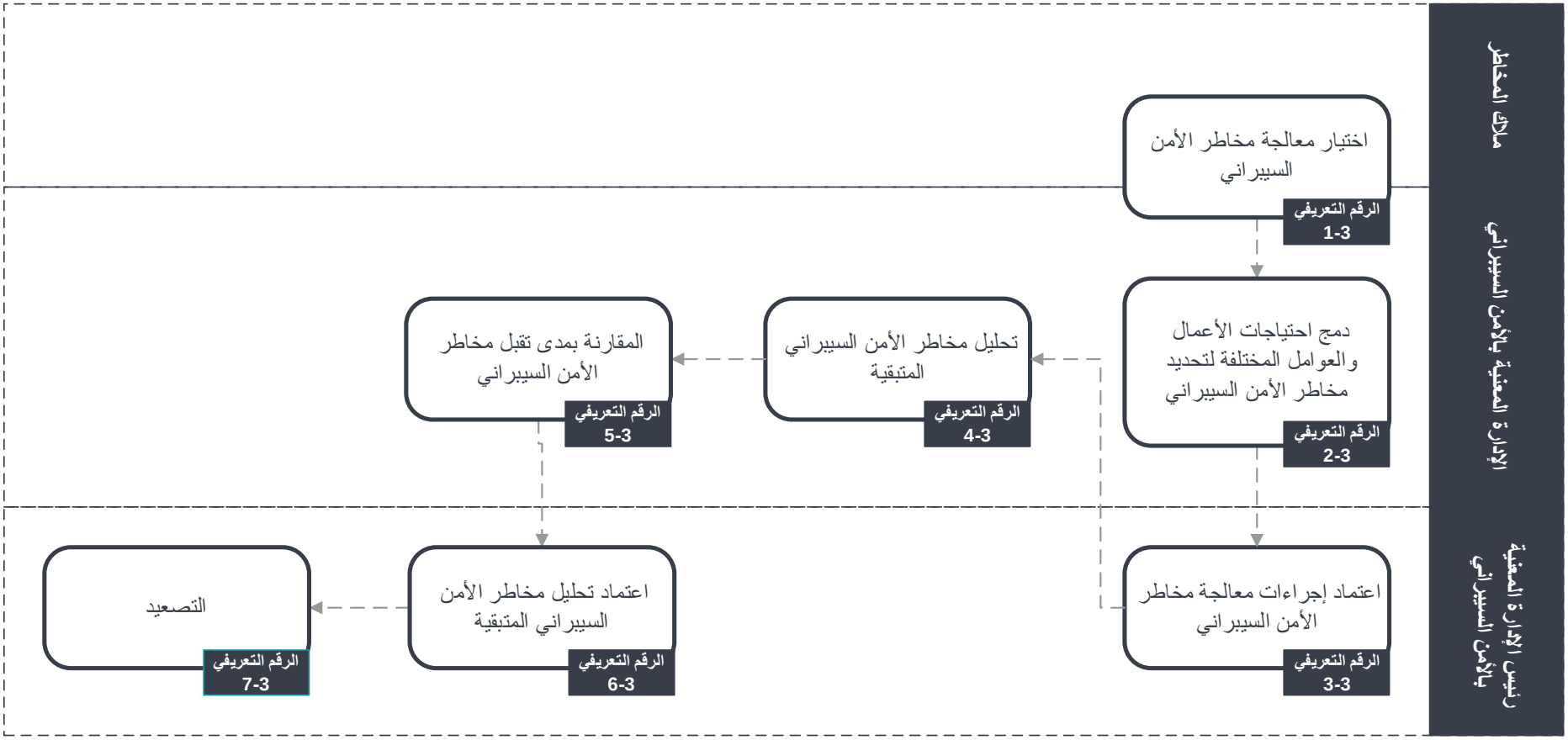
الرقم	الخطوة	الوصف	المالك / المسؤول	المُدخلات	المُخرجات	الأطراف المعنية
٢-٣-١	تقييم مخاطر الأمن السيبراني	يجب تقييم مخاطر الأمن السيبراني وفقًا لمعايير التقييم المحددة لدى <اسم الجهة> من أجل تحديد الخطوات التالية وتقييم مدى أولوية إجراءات معالجة تلك المخاطر. ويمكن اتخاذ القرارات التالية: ١. مراعاة خيارات معالجة مخاطر الأمن السيبراني. ٢. إجراء المزيد من التحليلات لتكوين فهم أفضل لمخاطر الأمن السيبراني. ٣. إعادة النظر في الأهداف.	الإدارة المعنية بالأمن السيبراني	قائمة مخاطر الأمن السيبراني	تقييم مخاطر الأمن السيبراني وفقًا للمعايير المحددة	الإدارة المعنية بالأمن السيبراني
٢-٣-٢	دمج احتياجات الأعمال والعوامل المختلفة لتحديد	يجب أن يُراعى في القرارات السياق العام والتداعيات الفعلية والمتوقعة على الجهات المعنية الخارجية والداخلية.	الإدارة المعنية بالأمن السيبراني	تقييم مخاطر الأمن السيبراني وفقًا للمعايير	القائمة المعدلة لمخاطر الأمن السيبراني	الإدارة المعنية بالأمن السيبراني

اختر التصنيف

الإصدار <١,٠>

الرقم	الخطوة	الوصف	المالك / المسؤول	المُدخلات	المُخرجات	الأطراف المعنية
	مخاطر الأمن السيبراني			المحددة، واحتياجات الأعمال		
٣-٣-٢	اعتماد تقييم مخاطر الأمن السيبراني	يجب اعتماد تقييم مخاطر الأمن السيبراني الذي تم إجراؤه.	رئيس الإدارة المعنية بالأمن السيبراني	قائمة مخاطر الأمن السيبراني، وتقييم مخاطر الأمن السيبراني وفقًا للمعايير المحددة	النتائج المعتمدة لتقييم مخاطر الأمن السيبراني	رئيس الإدارة المعنية بالأمن السيبراني

المرحلة الثالثة: معالجة مخاطر الأمن السيبراني



الشكل ٤ - مخطط سير العمل في مرحلة معالجة مخاطر الأمن السيبراني

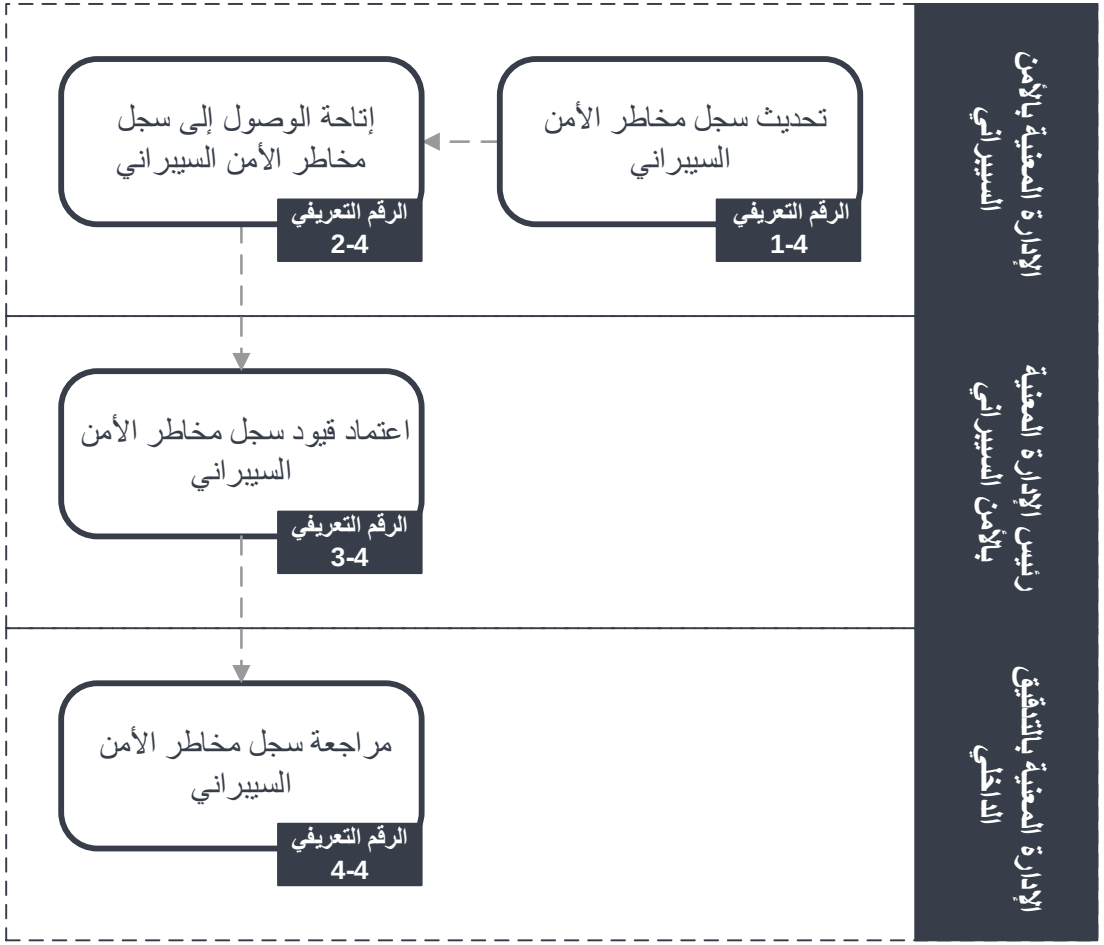
الرقم	الخطوة	الوصف	المالك / المسؤول	المُدخلات	المُخرجات	الأطراف المعنية
٣-١	اختيار معالجة مخاطر الأمن السيبراني	يجب تحديد خيارات معالجة مخاطر الأمن السيبراني من بين ما يلي: ١. التخفيف من مخاطر الأمن السيبراني: يتم التخفيف من مخاطر الأمن السيبراني من خلال تطبيق الضوابط الأمنية المطلوبة للحد من احتماليتها أو حجمها / تأثيرها، أو كليهما، والوصول بتقييم تلك المخاطر إلى مستوى يمكن قبوله. ٢. تجنّب مخاطر الأمن السيبراني: تجنّب الظروف والأحوال التي تنتج عنها تلك المخاطر. ٣. تحويل مخاطر الأمن السيبراني: نقل تلك المخاطر إلى طرف آخر يتمتع بقدرات أفضل للتعامل معها أو التأمين على الأصول المعلوماتية والتقنية ضد تلك المخاطر. ٤. تقبّل مخاطر الأمن السيبراني: يكون مستوى تلك المخاطر مقبولاً، لكن يجب مراقبتها باستمرار تحسبًا لأي تغيير.	الإدارة المعنية بالأمن السيبراني، وملاك المخاطر	قائمة مخاطر الأمن السيبراني	خيارات معالجة مخاطر الأمن السيبراني المحددة	الإدارة المعنية بالأمن السيبراني، وملاك المخاطر، ومنفّذ الضوابط
٣-٢	دمج احتياجات الأعمال والعوامل المختلفة لتحديد مخاطر الأمن السيبراني	يجب تحديد خيارات معالجة مخاطر الأمن السيبراني وتوثيقها بناءً على نتائج التقييم الذي تم إجراؤه سابقًا لتلك المخاطر وتحليل تكلفة التنفيذ والفوائد المتوقعة.	الإدارة المعنية بالأمن السيبراني	خيارات معالجة مخاطر الأمن السيبراني المحددة، واحتياجات الأعمال	خيارات معالجة مخاطر الأمن السيبراني المعدلة	الإدارة المعنية بالأمن السيبراني

الرقم	الخطوة	الوصف	المالك / المسؤول	المُدخلات	المُخرجات	الأطراف المعنية
٣-٣	اعتماد إجراءات معالجة مخاطر الأمن السيبراني	يجب اعتماد إجراءات معالجة مخاطر الأمن السيبراني المحددة.	رئيس الإدارة المعنية بالأمن السيبراني	خيارات معالجة مخاطر الأمن السيبراني المعدلة	إجراءات معالجة مخاطر الأمن السيبراني المعتمدة	رئيس الإدارة المعنية بالأمن السيبراني، وملاك المخاطر
٤-٣	تحليل مخاطر الأمن السيبراني المتبقية	يجب تحليل مخاطر الأمن السيبراني المتبقية، مع تقدير مدى احتمالية وقوع تلك المخاطر وحجمها / تأثيرها على وجه التحديد.	الإدارة المعنية بالأمن السيبراني	إجراءات معالجة مخاطر الأمن السيبراني المعتمدة	تحليل مخاطر الأمن السيبراني المتبقية	الإدارة المعنية بالأمن السيبراني
٥-٣	المقارنة بمدى تقبل مخاطر الأمن السيبراني	يجب مقارنة تقييم مخاطر الأمن السيبراني المتبقية بمدى تقبّل مخاطر الأمن السيبراني. وفي حالة تجاوز المخاطر المتبقية لمدى تقبّل المخاطر، يجب تطبيق ضوابط أخرى للحد من مخاطر الأمن السيبراني إلى مستوى مقبول.	الإدارة المعنية بالأمن السيبراني	تحليل مخاطر الأمن السيبراني المتبقية	نتائج مقارنة مخاطر الأمن السيبراني المتبقية بمدى تقبّل المخاطر	الإدارة المعنية بالأمن السيبراني
٦-٣	اعتماد تحليل مخاطر الأمن السيبراني المتبقية	يجب اعتماد تحليل مخاطر الأمن السيبراني المتبقية ونتائج مقارنتها بمدى تقبّل مخاطر الأمن السيبراني.	رئيس الإدارة المعنية بالأمن السيبراني	نتائج مقارنة مخاطر الأمن السيبراني المتبقية بمدى تقبّل المخاطر	النتائج المعتمدة لمقارنة مخاطر الأمن السيبراني المتبقية بمدى تقبّل المخاطر	رئيس الإدارة المعنية بالأمن السيبراني
٧-٣	التصعيد	في حالة عدم إمكانية الحد من مخاطر الأمن السيبراني المتبقية إلى مستوى تقبّل مخاطر الأمن السيبراني أو إذا كانت تكلفتها تتجاوز الأرباح، يتم تصعيد المسألة إلى رئيس <اسم الجهة> لاتخاذ الإجراءات أو القرارات اللازمة.	رئيس الإدارة المعنية بالأمن السيبراني	مخاطر الأمن السيبراني المتبقية تتجاوز مدى تقبّل المخاطر أو تكلفتها تتجاوز الأرباح	التصعيد إلى رئيس <اسم الجهة>	رئيس الإدارة المعنية بالأمن السيبراني، ورئيس <اسم الجهة>

اختر التصنيف

الإصدار <١,٠>

المرحلة الرابعة: التسجيل وإعداد التقارير



الشكل ٥ - مخطط سير العمل في مرحلة التسجيل والإبلاغ

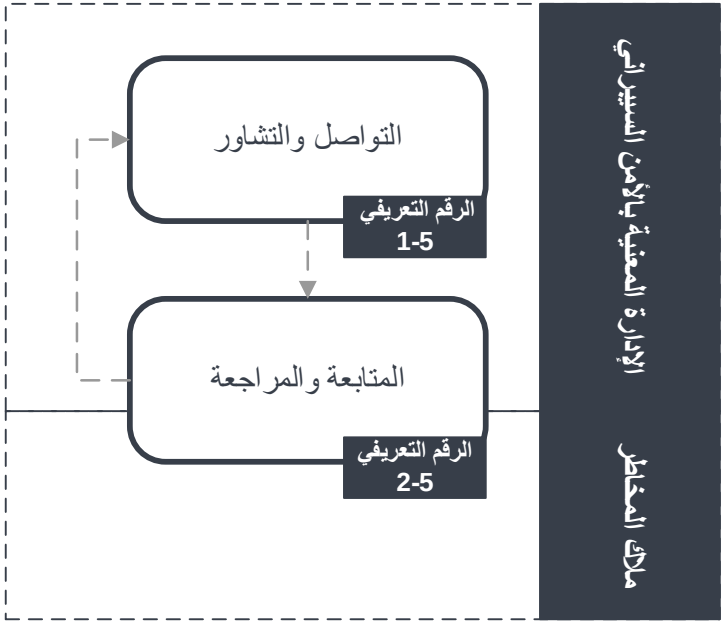
اختر التصنيف

الإصدار <١,٠>

الرقم	الخطوة	الوصف	المالك / المسؤول	المُدخلات	المُخرجات	الأطراف المعنية
٤-١	تحديث سجل مخاطر الأمن السيبراني	يجب إعداد سجل لمخاطر الأمن السيبراني وتحديثه لتوثيق نتائج عملية إدارة مخاطر الأمن السيبراني. ويجب أن يشمل السجل، على الأقل، المعلومات التالية: ١. الرمز التعريفي لمخاطر الأمن السيبراني ٢. نطاق مخاطر الأمن السيبراني (المنطقة المتأثرة بمخاطر الأمن السيبراني) ٣. مالك مخاطر الأمن السيبراني ٤. وصف مخاطر الأمن السيبراني، بما في ذلك سببها وتأثيرها ٥. تحليل مخاطر الأمن السيبراني الذي يسلط الضوء على عواقبها والإطار الزمني لها ٦. تقييم وتصنيف مخاطر الأمن السيبراني الذي يشمل احتمالية وقوع المخاطر وحجمها /تأثيرها والتصنيف العام لها حال وقوعها ٧. خطة معالجة مخاطر الأمن السيبراني التي تشمل إجراءات معالجتها والمسؤول عنها والجدول الزمني لها ٨. وصف مخاطر الأمن السيبراني المتبقية وتحليلها ٩. وصف الخطوات السابقة.	الإدارة المعنية بالأمن السيبراني	قائمة مخاطر الأمن السيبراني، وملاك المخاطر، وخيارات معالجة مخاطر الأمن السيبراني، ومخاطر الأمن السيبراني المتبقية المحللة	سجل مخاطر الأمن السيبراني	الإدارة المعنية بالأمن السيبراني

الرقم	الخطوة	الوصف	المالك / المسؤول	المُدخلات	المُخرجات	الأطراف المعنية
٤-٢	إتاحة الوصول إلى سجل مخاطر الأمن السيبراني	يجب إتاحة الوصول إلى سجل مخاطر الأمن السيبراني إلى جميع الجهات المعنية على أساس مبدأ "الحاجة إلى المعرفة".	الإدارة المعنية بالأمن السيبراني	سجل مخاطر الأمن السيبراني	منح صلاحية الوصول إلى سجل مخاطر الأمن السيبراني إلى الجهات المعنية	الإدارة المعنية بالأمن السيبراني
٤-٣ ٤	اعتماد قيود سجل مخاطر الأمن السيبراني	يجب اعتماد جميع القيود المضافة حديثًا إلى سجل مخاطر الأمن السيبراني والصلاحيات الممنوحة للوصول إليه.	رئيس الإدارة المعنية بالأمن السيبراني	سجل مخاطر الأمن السيبراني	اعتماد سجل مخاطر الأمن السيبراني وصلاحيات الوصول الممنوحة	رئيس الإدارة المعنية بالأمن السيبراني
٤-٤ ٤	مراجعة سجل مخاطر الأمن السيبراني	يجب مراجعة سجل مخاطر الأمن السيبراني سنويًا على الأقل، خاصةً في إطار تنفيذ إجراءات معالجة مخاطر الأمن السيبراني.	الإدارة المعنية بالتدقيق الداخلي	سجل مخاطر الأمن السيبراني	سجل مخاطر الأمن السيبراني المراجَع	الإدارة المعنية بالتدقيق الداخلي

المرحلة الخامسة: التواصل والمتابعة



الشكل ٦ - مخطط سير العمل في الاتصال والمراقبة

الرقم	الخطوة	الوصف	المالك / المسؤول	المُدخلات	المُخرجات	الأطراف المعنية
١-٥	التواصل والتشاور	يجب التواصل والتشاور بشأن جميع الخطوات والإجراءات المتخذة خلال عملية إدارة مخاطر الأمن السيبراني مع جميع الجهات المعنية الداخلية والخارجية. والغرض من هذا هو توفير فهم أفضل	الإدارة المعنية بالأمن السيبراني	جميع خطوات العملية	التواصل والتشاور بوضوح مع الجهات المعنية بشأن الإجراءات	الإدارة المعنية بالأمن السيبراني

الرقم	الخطوة	الوصف	المالك / المسؤول	المُدخلات	المُخرجات	الأطراف المعنية
		ومبررات لجميع الإجراءات المتخذة فيما يتعلق بعملية إدارة مخاطر الأمن السيبراني.			المتخذة	
٢-٥	المتابعة والمراجعة	يجب متابعة جميع مخاطر الأمن السيبراني المحددة وتدابير معالجتها المطبقة ومراجعتها باستمرار. ويجب أن تتم المتابعة والمراجعة في جميع مراحل العملية.	الإدارة المعنية بالأمن السيبراني، وملاك المخاطر	سجل مخاطر الأمن السيبراني	متابعة ومراجعة سجل مخاطر الأمن السيبراني	الإدارة المعنية بالأمن السيبراني، وملاك المخاطر

الأدوار والمسؤوليات

١- **مالك الإجراء:** <رئيس الإدارة المعنية بالأمن السيبراني>.

٢- **مراجعة الإجراء وتحديثه:** <الإدارة المعنية بالأمن السيبراني>.

٣- **تنفيذ الإجراء وتطبيقه:** <الإدارة المعنية بتقنية المعلومات> و<الإدارة المعنية بالأمن السيبراني>.

٤- **قياس الالتزام بالإجراء:** <الإدارة المعنية بالأمن السيبراني>.

التحديث والمراجعة

يجب على <الإدارة المعنية بالأمن السيبراني> مراجعة الإجراء سنويًا على الأقل أو في حال حدوث تغييرات في السياسات أو الإجراءات التنظيمية في <اسم الجهة> أو المتطلبات التشريعية والتنظيمية ذات العلاقة.

الالتزام بالإجراء

١- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> التأكد من التزام <اسم الجهة> بهذا الإجراء دوريًا.

٢- يغطي هذا الإجراء جميع محطات العمل والخوادم في <اسم الجهة> و يجب على كافة العاملين في <اسم الجهة> الالتزام بهذا الإجراء.

٣- قد يعرض أي انتهاك لهذا الإجراء صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في <اسم الجهة>.