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

أدخل شعار الجهة بالضغط على الصورة الموضحة.

نموذج الهيكل التنظيمي للأمن السيبراني

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

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

اختر التصنيف

التاريخ: اضغط هنا لإضافة نص

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

اعتماد الوثيقة

الدور	الاسم	التاريخ	التوقيع
اختر الدور	<أدخل الاسم الكامل للشخص>	اضغط هنا لإضافة نص	<أدخل التوقيع>

نسخ الوثيقة

النسخة	التاريخ	عُدّل بواسطة	أسباب التعديل
<أدخل رقم النسخة>	اضغط هنا لإضافة نص	<أدخل الاسم الكامل للشخص>	<أدخل وصف التعديل>

قائمة المحتويات

الأهداف

تم إنشاء <الإدارة المعنية بالأمن السيبراني> والمستقلة عن <الإدارة المعنية بتقنية المعلومات> وفقاً للأمر السامي الكريم رقم ٣٧١٤٠ بتاريخ ١٤٣٨/٨/١٤هـ ووفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ١-٢-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

تم تطوير الهيكل التنظيمي للأمن السيبراني بناءً على أفضل الممارسات والمعايير لتوفير الدعم اللازم لـ<الإدارة المعنية بالأمن السيبراني> لتمكينها من تنفيذ المهام الموكلة إليها بالشكل المطلوب. وتُعد إدارة الأمن السيبراني أحد الروافد الأساسية في <اسم الجهة> وهي المعنية بحماية الأصول المعلوماتية والتقنية من المخاطر السيبرانية.

الغرض من هذه الوثيقة هو تحديد وتوثيق الهيكل التنظيمي للحوكمة والأدوار والمسؤوليات الخاصة بالأمن السيبراني في <اسم الجهة>.

القواعد الإرشادية

1- التأكد من أن <الإدارة المعنية بالأمن السيبراني> مستقلة عن <الإدارة المعنية بتقنية المعلومات>.
2- التأكد من أن <الإدارة المعنية بالأمن السيبراني> مرتبطة برئيس الجهة أو من ينيبه في <اسم الجهة> بحيث يمكنه التأثير على القرارات الرئيسية المتعلقة بالأمن السيبراني في <اسم الجهة>.
3- التأكد من ان ارتباط <الإدارة المعنية بالأمن السيبراني> مختلف عن ارتباط <الإدارة المعنية بتقنية المعلومات> او <الإدارة المعنية بالتحول الرقمي> تنفيذا للأمر السامي الكريم رقم ٣٧١٤٠ بتاريخ ١٤٣٨/٨/١٤هـ، وهو مطلب تشريعي في الضابط رقم ١-٢-١ من الضوابط الأساسية للأمن السيبراني.
4- تجنب تعارض المصالح، ومن أمثلة تعارض المصالح ما يلي:
   4-1 إدارة صلاحية الأنظمة التقنية والمعلوماتية (أو الأنظمة التشغيلية) وإدارة عملياتها في الوقت ذاته.
   4-2 تطبيق متطلبات الأمن السيبراني والتأكد من الالتزام بها في الوقت ذاته.
   4-3 تعارض مصالح فريق مراقبة الأمن السيبراني مع فريق تشغيل عمليات الأمن السيبراني.
   4-4 تعارض مصالح فريق الاختبارات الأمنية مع فريق تطوير التطبيقات.
5- التأكد من وجود الأدوار التالية كحد أدنى في هيكلية الأمن السيبراني:
   5-1 حوكمة الأمن السيبراني.
   5-2 إدارة الالتزام بالأمن السيبراني.
   5-3 إدارة مخاطر الأمن السيبراني.
   5-4 إدارة استراتيجية الأمن السيبراني.
   5-5 صمود الأمن السيبراني.
   5-6 التوعية والتدريب بالأمن السيبراني.
   5-7 عمليات الأمن السيبراني (مراقبة الأمن السيبراني والاستجابة للحوادث).
   5-8 حماية البيانات والمعلومات.
   5-9 الأمن السيبراني للأنظمة التشغيلية OT/ICS (إن وجد).
6- قد تضاف الأدوار التالية إلى هيكلية الأمن السيبراني:
   6-1 معمارية الأمن السيبراني.

اختر التصنيف

2-6 خصوصية البيانات والمعلومات.
3-6 إدارة هويات الدخول والصلاحيات.
4-6 إدارة بنية الأمن السيبراني التحتية.
5-6 الأمن المادي.

حوكمة الأمن السيبراني

عناصر الهيكل التنظيمي لـ<اسم الجهة>

#	العنصر	الوصف
1	صاحب الصلاحية	يُعد صاحب الصلاحية (أو من ينيبه) أعلى سلطة في الجهة، وقد يكون مجلس الإدارة.
2	اللجنة الإشرافية للأمن السيبراني	اللجنة الإشرافية للأمن السيبراني هي مجلس حوكمة رفيع المستوى، وتتمثّل مسؤوليتها الأساسية في ضمان التزام تطبيق برامج وتشريعات الأمن السيبراني داخل <اسم الجهة> ودعمها ومتابعتها.
3	إدارة الأمن السيبراني	<الإدارة المعنية بالأمن السيبراني> هي المعنية بحماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات وما تقدمه من خدمات وما تحتويه من بيانات من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع. ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحو ذلك.
4	تقنية المعلومات	<الإدارة المعنية بتقنية المعلومات> هي المعنية بتشغيل البنية التحتية لتقنية المعلومات والشبكات، وتطوير البرمجيات والخدمات التقنية، وغير ذلك من أعمال.
5	الموارد البشرية	<الإدارة المعنية بالموارد البشرية> هي المعنية بشؤون العاملين داخل <اسم الجهة>.
6	الشؤون القانونية	<الإدارة المعنية بالشؤون القانونية> هي الإدارة المعنية بصياغة العقود والاتفاقيات وحفظ حقوق <اسم الجهة> القانونية.
7	المشتريات	<الإدارة المعنية بشؤون المشتريات> هي الإدارة المعنية بالتعاقد مع الموردين وعمليات الشراء وكذلك عقود الأطراف الخارجية في <اسم الجهة>.
8	الشؤون المالية	<الإدارة المعنية بالشؤون المالية> هي المعنية بإعداد الميزانية العامة لـ<اسم الجهة>.
9	التدقيق والمراجعة الداخلية	<الإدارة المعنية بالمراجعة الداخلية> هي المعنية بتدقيق ومراجعة تطبيق <اسم الجهة> للسياسات والإجراءات وكذلك المتطلبات التنظيمية والتشريعية ذات العلاقة.

#	العنصر	الوصف
10	إدارة استمرارية الأعمال	<الإدارة المعنية باستمرارية الأعمال> هي المعنية بجميع المسائل المتعلّقة باستمرارية الأعمال في <اسم الجهة>.
11	تقنية التشغيل	<الإدارة المعنية بتقنية التشغيل> (Operational Technology) هي المعنية بجميع المسائل المتعلّقة بالتقنية التشغيلية في <اسم الجهة>.
12	مكتب إدارة المشاريع	<مكتب إدارة المشاريع> هو المعني بجميع المسائل المتعلّقة بإدارة المشاريع في <اسم الجهة>، بما في ذلك مكاتب تحقيق الرؤية 2030 (إن وجدت).
13	وحدات الأعمال	تشمل جميع وحدات الأعمال والإدارات الأخرى في <اسم الجهة>.

هيكلية الأمن السيبراني

لتقوم <الإدارة المعنية بالأمن السيبراني> بعملها بالشكل المطلوب وبكفاءة عالية، تم توزيع المهام والأدوار في <الإدارة المعنية بالأمن السيبراني> بناءً على الوظائف التشغيلية لكل دور، مع الأخذ بعين الاعتبار مبدأ فصل المهام (Segregation of Duties) وتعارض المصالح (Conflict of Interest) وتم توزيعها كالتالي <يمكن اختيار أحد الخيارات أدناه>:

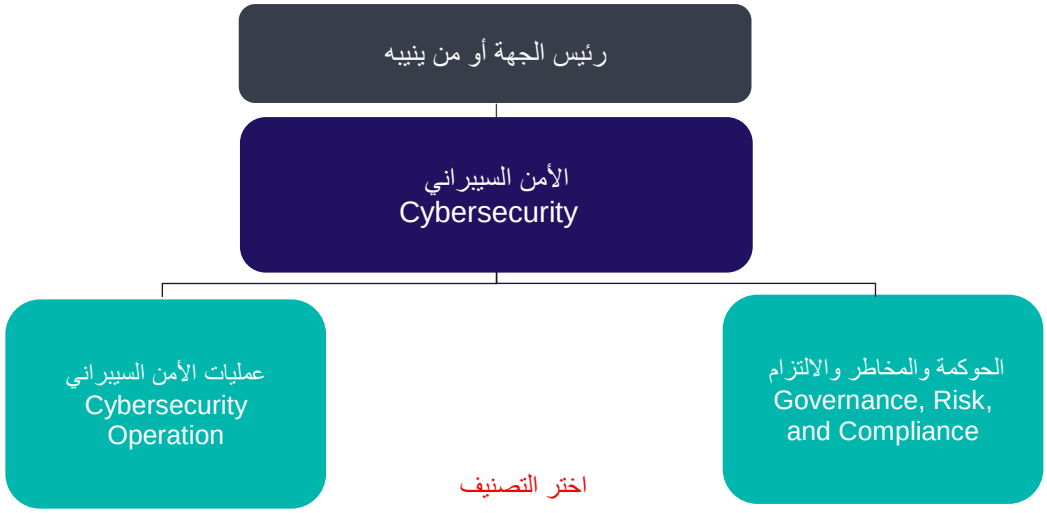
الهيكل التنظيمي <للإدارة المعنية بالأمن السيبراني>

الهياكل التنظيمية التالية المقترحة تعتبر اختيارية، يمكن اختيار الهيكل بناءً على ما يتناسب مع أعمال الجهة.

1- الخيار الأول

1-1 يتوافق هذا الهيكل التنظيمي للأمن السيبراني مع التنظيميات المحلية ويُركّز على المكوّنات الأساسية للأمن السيبراني.

2-1 يخلو هذا الهيكل التنظيمي للأمن السيبراني من التعقيد ويعتبر أسهل من ناحية الفهم والتنفيذ.



اختر التصنيف

الحوكمة والمخاطر والالتزام		
#	الأدوار	المسؤوليات
1	استراتيجية الأمن السيبراني ومكتب إدارة المشاريع Cybersecurity Strategy & PMO	ضمان إسهام خطط العمل للأمن السيبراني والأهداف والمبادرات والمشاريع الخاصة بـ<الإدارة المعنية بالأمن السيبراني> في تحقيق الالتزام بالمتطلّبات التشريعية والتنظيمية ذات العلاقة.
2	إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management	ضمان إدارة مخاطر الأمن السيبراني على نحوٍ منهجي يهدف إلى حماية الأصول المعلوماتية والتقنية الخاصة بـ<اسم الجهة>، وذلك وفقاً للسياسات والإجراءات التنظيمية المعتمدة في <اسم الجهة> والمتطلّبات التشريعية والتنظيمية ذات العلاقة.
3	إدارة الالتزام بالأمن السيبراني Cybersecurity Compliance Management	التأكّد من تنفيذ متطلبات الأمن السيبراني والالتزام بالتنظيمات والتشريعات ذات العلاقة.
4	التوعية والتدريب بالأمن السيبراني Cybersecurity Awareness and Training	التأكّد من أن العاملين في <اسم الجهة> لديهم الوعي الأمني اللازم وعلى دراية بمسؤولياتهم في مجال الأمن السيبراني. والتأكّد من تزويد العاملين في <اسم الجهة> بالمهارات والمؤهلات والدورات التدريبية المطلوبة في مجال الأمن السيبراني لحماية الأصول المعلوماتية والتقنية الخاصة بـ<اسم الجهة> والقيام بمسؤولياتهم تجاه الأمن السيبراني.
5	صمود الأمن السيبراني Cybersecurity Resilience	ضمان توافر متطلّبات صمود الأمن السيبراني في إدارة استمرارية أعمال <اسم الجهة>. وضمان معالجة وتقليل الآثار المترتبة على الاضطرابات في الخدمات الإلكترونية الحساسة في <اسم الجهة>، وأنظمة وأجهزة معالجة معلوماتها جراء الكوارث الناتجة عن الأحداث السيبرانية.
6	الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية Third-Party and Cloud Computing Cybersecurity	ضمان حماية الأصول المعلوماتية والتقنية من المخاطر السيبرانية المتعلقة بالأطراف الخارجية، والتأكد من تطبيق متطلّبات الأمن السيبراني للحوسبة السحابية والاستضافة وذلك وفقاً للسياسات والإجراءات التنظيمية المعتمدة في <اسم الجهة>، والمتطلّبات التشريعية والتنظيمية ذات العلاقة.

عمليات الأمن السيبراني		
#	الأدوار	المسؤوليات
1	إدارة الثغرات واختبار الاختراق	تقييم واختبار مدى فعالية قدرات تعزيز الأمن السيبراني في <اسم الجهة>، وفحص الثغرات التقنية واكتشافها وذلك من خلال عمل محاكاة لتقنيات وأساليب

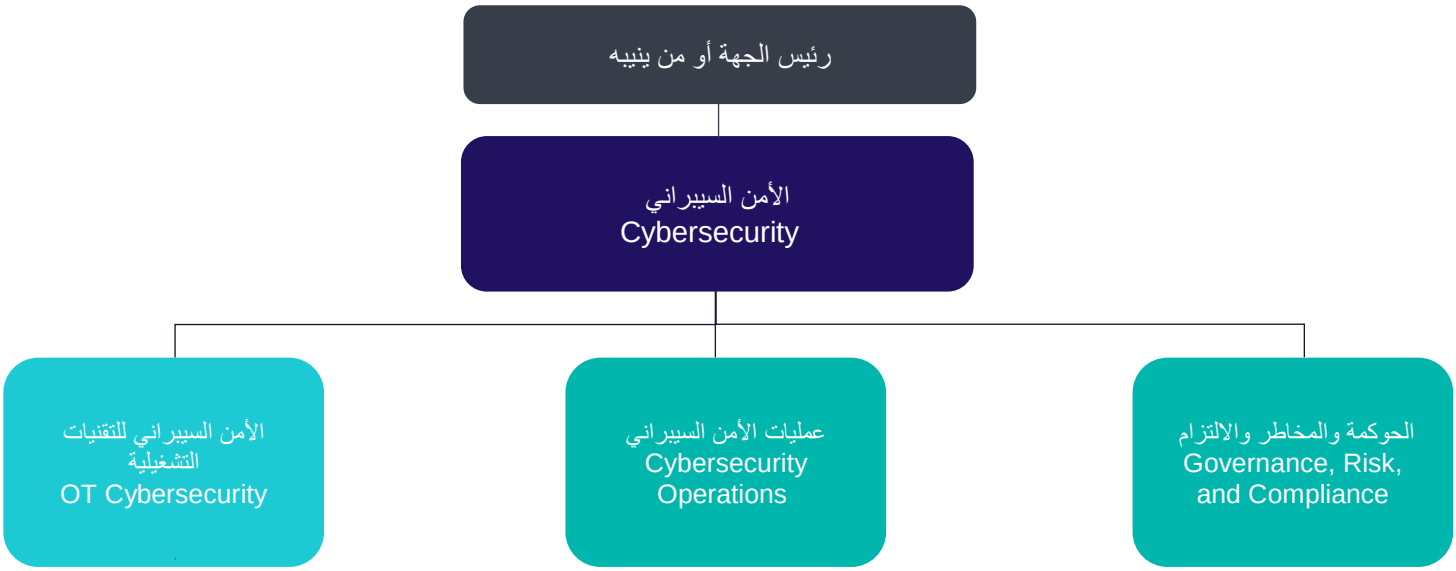
اختر التصنيف

	Vulnerability Management and Penetration Testing	الهجوم السيبراني الفعلية. واكتشاف نقاط الضعف الأمنية غير المعروفة والتي قد تؤدي إلى الاختراق السيبراني.
2	حماية البيانات والمعلومات Data and Information Protection	ضمان حماية سريّة بيانات ومعلومات <اسم الجهة> وسلامتها وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية المعتمدة في <اسم الجهة>، والمتطلّبات التشريعية والتنظيمية ذات العلاقة.
3	إدارة حوادث وتهديدات الأمن السيبراني Cybersecurity Incident and Threat Management	ضمان تحديد واكتشاف أحداث وتهديدات الأمن السيبراني في الوقت المناسب وإدارتها والتعامل معها بفاعلية لمنع أو تقليل الآثار السلبية الناجمة عنها على أعمال <اسم الجهة>.
4	مراقبة الأمن السيبراني Cybersecurity Monitoring	ضمان جمع وتحليل ومراقبة أحداث الأمن السيبراني لاكتشاف الهجمات السيبرانية في وقت مبكر بهدف منع أو تقليل الآثار السلبية الناجمة عنها على أعمال <اسم الجهة>.

2- الخيار الثاني

2-1 يُركّز هذا الهيكل التنظيمي للأمن السيبراني بشكل خاص على مسائل الخصوصية والشؤون القانونية.

2-2 يُتيح هذا الهيكل التنظيمي حماية سريّة وسلامة وتوافر أصول <اسم الجهة> المتعلّقة بأجهزة وأنظمة التحكم الصناعي (OT/ICS) ضد الهجمات السيبرانية.



الحوكمة والمخاطر والالتزام		
#	الأدوار	المسؤوليات
1	التخطيط الاستراتيجي وسياسة الأمن السيبراني Cybersecurity Strategic Planning and Policy	ضمان تطوير السياسات وخطط العمل و/أو تأييد التغييرات على السياسة بما يدعم مبادرات الأمن السيبراني أو التغييرات والتحسينات المطلوبة لدى <اسم الجهة>.
2	التوعية والتدريب بالأمن السيبراني Cybersecurity Awareness and Training	التأكّد من أن العاملين في <اسم الجهة> لديهم الوعي الأمني اللازم وعلى دراية بمسؤولياتهم في مجال الأمن السيبراني. والتأكّد من تزويد العاملين في <اسم الجهة> بالمهارات والمؤهلات والدورات التدريبية المطلوبة في مجال الأمن السيبراني لحماية الأصول المعلوماتية والتقنية الخاصة بـ<اسم الجهة> والقيام بمسؤولياتهم تجاه الأمن السيبراني.
3	إدارة المشاريع والاستحواذ Project Management and Acquisition	إدارة مشاريع الأمن السيبراني وتنسيقها ونشرها ودمجها، وتحمل مسؤولية نجاحها بشكل عام، وكذلك تقييم المشاريع لضمان التزامها بالمعايير المنشورة
4	إدارة المخاطر والالتزام بالأمن السيبراني Cybersecurity Risk and Compliance Management	الإشراف والتقييم وتقديم الدعم لعمليات التوثيق والتحقّق والقياس والتصريح اللازمة لضمان تلبية الأصول المعلوماتية والتقنية القائمة والجديدة لمتطلّبات الأمن السيبراني والمخاطر لدى <اسم الجهة>. كما تضمن هذه الإدارة التعامل مع المخاطر والالتزام بشكل مناسب والتأكّد من التزام الأطراف الداخلية والخارجية.
5	الأمن السيبراني لتطوير الأنظمة والبرمجيات System and Software Development Cybersecurity	ضمان إدراج المتطلّبات المتعلّقة بالأمن السيبراني ضمن دورة حياة تطوير الأنظمة والبرمجيات.
6	معمارية الأمن السيبراني Cybersecurity Architecture	تولي مسؤولية وضع التدابير الأمنية التقنية وفقاً لسياسات ومعايير <اسم الجهة>، وضمان مراجعة جميع تصاميم تقنية المعلومات واعتمادها من جانب الأمن السيبراني قبل تنفيذها.
7	حماية البيانات والمعلومات Data and Information Protection	ضمان حماية سريّة بيانات ومعلومات <اسم الجهة> وسلامتها وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية المعتمدة في <اسم الجهة>، والمتطلّبات التشريعية والتنظيمية ذات العلاقة.
8	أبحاث وتطوير الأمن السيبراني Cybersecurity Research and Development	استخدام هندسة البرمجيات والأنظمة وأبحاث الأنظمة البرمجية لتطوير قدرات جديدة وضمان تكامل الأمن السيبراني بشكل تام في الجهة، وإجراء أبحاث تقنية شاملة لتقييم الثغرات المحتملة في أنظمة الفضاء السيبراني.

اختر التصنيف

عمليات الأمن السيبراني		
#	الأدوار	المسؤوليات
1	التخطيط والاتصالات Planning and Communication	إنشاء قنوات الاتصال الملائمة مع الجهات المعنية ودعمها لضمان تنفيذ عمليات التنسيق والتعاون والتصعيد بشكل مناسب معها عند الضرورة، بالإضافة إلى الحفاظ على قنوات تبادل المعلومات المناسبة مع الإدارات والجهات الأخرى.
2	مراقبة الأمن السيبراني Cybersecurity Monitoring	ضمان جمع ومراقبة أحداث الأمن السيبراني لاكتشاف الهجمات السيبرانية في وقت مبكر بهدف منع أو تقليل الآثار السلبية الناجمة عنها على أعمال <اسم الجهة>.
3	المعلومات الاستباقية Cybersecurity Intelligence	توفير وتحليل معلومات منظمة حول الهجمات الأخيرة والحالية والمحتملة التي يمكن أن تشكل تهديداً سيبرانياً لـ<اسم الجهة>.
4	تحليل الأمن السيبراني Cybersecurity Analysis	استخدام التدابير الوقائية والمعلومات المجمّعة من مصادر مختلفة لتحديد وتحليل الأحداث التي تحدث أو قد تحدث في الشبكة والإبلاغ عنها، وذلك بهدف حماية المعلومات وأنظمة المعلومات والشبكات من التهديدات، وتحديد الثغرات ومدى إمكانية التعرّض لخطر استغلالها.
5	إدارة الثغرات Vulnerability Management	إجراء التقييمات بشأن التهديدات والثغرات، وتحديد الانحرافات عن الإعدادات المقبولة والسياسة المؤسسية والمحلية، وتقييم مستوى المخاطر، وتطوير و/أو تقديم التوصيات بالتدابير المضادة المناسبة للتخفيف منها في الظروف التشغيلية وغير التشغيلية.
6	الاستجابة لحوادث الأمن السيبراني Cybersecurity Incident Response	التعامل مع الكوارث أو الحالات الطارئة ضمن المجال ذي الصلة للتخفيف من التهديدات المباشرة والمحتملة، واستخدام مقاربات التخفيف والاستعداد والاستجابة والتعافي عند اللزوم للحفاظ على الممتلكات ومجال الأمن السيبراني بأقصى حدٍّ ممكن، ويتم كذلك التحقيق في جميع أنشطة الاستجابة ذات الصلة وتحليلها.
7	تحقيقات الأمن السيبراني Cybersecurity Investigation	تطبيق الأساليب التخطيطية والتقنيات والإجراءات الخاصة بمجموعة كاملة من أدوات وعمليات التحقيق التي تشمل على (سبيل المثال لا الحصر) أساليب المقابلات والاستجواب والرقابة، والمراقبة المضادة واكتشاف المراقبة، والموازنة المناسبة بين مزايا المراقبة مقابل جمع المعلومات الاستباقية.
8	التحليلات الجنائية الرقمية Digital Forensics	جمع الأدلة المتعلّقة بالحاسوب ومعالجتها وحفظها وتحليلها وتقديمها بما يدعم وسائل التخفيف من ثغرات الشبكة و/أو التحقيقات الجنائية أو الاحتيالية أو مكافحة التجسّس أو إنفاذ القانون.

الأمن السيبراني للتقنيات التشغيلية		
1	الأمن السيبراني للتقنيات التشغيلية OT Cybersecurity	ضمان إدارة الأمن السيبراني بشكل سليم وفعّال لحماية سريّة وسلامة وتوافر أصول <اسم الجهة> المتعلّقة بأجهزة وأنظمة التحكم الصناعي (OT/ICS) ضد الهجمات السيبرانية.

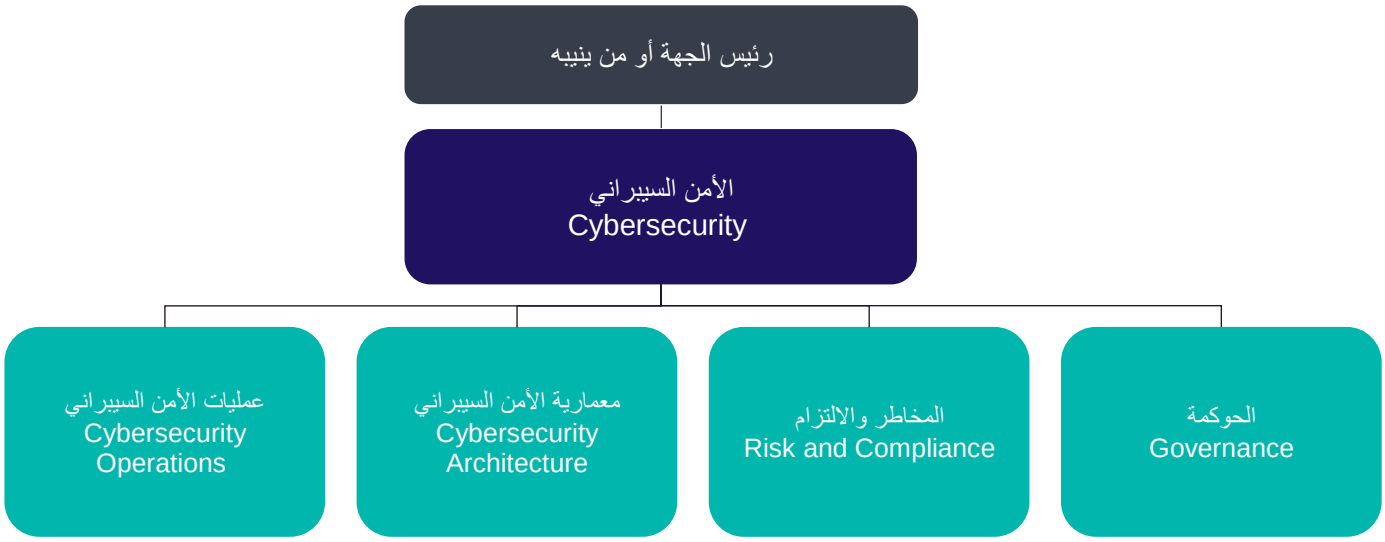
3- الخيار الثالث

1-3 يتولّى الهيكل التنظيمي للأمن السيبراني الإشراف على الميزانية، ويتحمّل مسؤولية التقنية الأمنية والقوة العاملة المعنية بتشغيل وإدارة هذه التقنية.

2-3 يتجنّب الهيكل التنظيمي للأمن السيبراني نقل التحكم بالتقنيات الأمنية والذي قد يُعرّض <اسم الجهة> إلى مخاطر غير مقبولة.

3-3 يُتيح الهيكل التنظيمي للأمن السيبراني استخدام تقنيات متطوّرة تُشجّع الابتكار السريع واعتماد الضوابط الأمنية الجديدة.

4-3 يُوفّر هذا الهيكل التنظيمي للأمن السيبراني مركز عمليات تشغيلي للأمن السيبراني، ويحظى فيه مدير مركز عمليات الأمن السيبراني على عدد أكبر من الموظفين والصلاحيات والسلطات.



الحوكمة		
#	الأدوار	المسؤوليات
1	إدارة ومراقبة سياسة الأمن السيبراني Cybersecurity Policy Control and Management	التأكّد من توثيق متطلّبات الأمن السيبراني والتزام <اسم الجهة> بها وفقاً للمتطلّبات التشريعية والتنظيمية ذات العلاقة.
2	نشر سياسة الأمن السيبراني والتوعية بها Cybersecurity Policy Communication and Awareness	التأكّد من نشر متطلّبات الأمن السيبراني وفقاً للمتطلّبات التشريعية والتنظيمية ذات العلاقة، وضمان أن العاملين في <اسم الجهة> لديهم الوعي الأمني اللازم وأنهم على دراية بمسؤولياتهم في مجال الأمن السيبراني.
3	الخصوصية وحماية البيانات Data Protection & Privacy	ضمان حماية سريّة بيانات ومعلومات <اسم الجهة> وسلامتها وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية المعتمدة فيها، ووفقاً للمتطلّبات التشريعية والتنظيمية ذات العلاقة. وكذلك تطوير برنامج الالتزام بالخصوصية وموظفي برنامج الخصوصية والإشراف عليهما، ودعم الالتزام بالخصوصية والحوكمة والسياسة واحتياجات الاستجابة للأحداث للمديرين التنفيذيين وفرقهم المتخصّصة بالخصوصية والأمن.
4	صمود الأمن السيبراني Cybersecurity Resilience	ضمان توافر متطلّبات صمود الأمن السيبراني في إدارة استمرارية أعمال <اسم الجهة>. وضمان معالجة وتقليل الآثار المترتبة على الاضطرابات في الخدمات الإلكترونية الحساسة للجهة وأنظمة وأجهزة معالجة معلوماتها جراء الكوارث الناتجة عن الأحداث السيبرانية.

المخاطر والالتزام		
#	الأدوار	المسؤوليات
1	إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management	ضمان إدارة مخاطر الأمن السيبراني على نحوٍ منهجي يهدف إلى حماية الأصول المعلوماتية والتقنية الخاصة بـ<اسم الجهة>، وذلك وفقاً للسياسات والإجراءات التنظيمية المعتمدة في <اسم الجهة> والمتطلّبات التشريعية والتنظيمية ذات العلاقة.
2	إدارة الالتزام بالأمن السيبراني Cybersecurity Compliance Management	التأكّد من تنفيذ ضوابط الأمن السيبراني والتزامها بسياسات وإجراءات <اسم الجهة> بالإضافة إلى التشريعات والأنظمة والاتفاقيات الوطنية والدولية.

اختر التصنيف

معمارية الأمن السيبراني		
#	الأدوار	المسؤوليات
1	الاستشارات التقنية المتعلّقة بالأمن السيبراني Technical Cybersecurity Consultancy	تولي مسؤولية وضع التدابير الأمنية التقنية وفقاً لسياسات ومعايير <اسم الجهة>، وضمان مراجعة جميع تصاميم تقنية المعلومات واعتمادها من جانب الأمن السيبراني قبل تنفيذها.
2	استشارات المشاريع Project Consultancy	إدارة مشاريع الأمن السيبراني وتنسيقها ونشرها ودمجها والمساءلة عن نجاحها بشكل عام، وكذلك تقييم المشاريع لضمان التزامها بالمعايير المنشورة.
3	الأمن السيبراني للتطبيقات Application Cybersecurity	ضمان إدراج المتطلّبات المتعلّقة بالأمن السيبراني ضمن دورة حياة تطوير الأنظمة والبرمجيات.

عمليات الأمن السيبراني		
#	الأدوار	المسؤوليات
1	الاستجابة لحوادث الأمن السيبراني وتحليلها Cybersecurity Incident Response and Forensics	التعامل مع الكوارث أو الحالات الطارئة ضمن المجال ذي الصلة للتخفيف من التهديدات المباشرة والمحتملة، واستخدام مقاربات التخفيف والاستعداد والاستجابة والتعافي عند اللزوم للحفاظ على الممتلكات والأمن السيبراني بأقصى حدٍّ ممكن، وكذلك التحقيق في جميع أنشطة الاستجابة ذات الصلة وتحليلها. بالإضافة إلى جمع الأدلة المتعلّقة بالحاسوب ومعالجتها وحفظها وتحليلها وتقديمها بما يدعم وسائل التخفيف من ثغرات الشبكة و/أو التحقيقات الجنائية أو الاحتيالية أو مكافحة التجسّس أو إنفاذ القانون.
2	مراقبة وتحليل الأمن السيبراني Cybersecurity Monitoring and Analysis	ضمان جمع وتحليل ومراقبة أحداث الأمن السيبراني لاكتشاف الهجمات السيبرانية في وقت مبكر بهدف منع أو تقليل الآثار السلبية الناجمة عنها على عمليات <اسم الجهة>.
3	إدارة الثغرات والتهديدات Vulnerability and Threat Management	ضمان اكتشاف الثغرات التقنية في الوقت المناسب ومعالجتها بشكل فعّال، وذلك لمنع أو تقليل احتمالية استغلال هذه الثغرات من قبل الهجمات السيبرانية وتقليل الآثار المترتبة على أعمال <اسم الجهة>. وضمان تحديد واكتشاف تهديدات الأمن السيبراني في الوقت المناسب وإدارتها والتعامل معها بفاعلية لمنع أو تقليل الآثار السلبية الناجمة عنها على عمليات <اسم الجهة>.

اختر التصنيف

4	البنية التحتية والعمليات المتعلّقة بالأمن السيبراني Cybersecurity Infrastructure and Operations	تولي مسؤولية تشغيل وإدارة وصيانة حلول الأمن السيبراني وتقنياته وبنيته التحتية وفقاً للمتطلّبات التشريعية والتنظيمية ذات العلاقة.

الأدوار والمسؤوليات

1- **راعي ومالك الوثيقة:** <رئيس الإدارة المعنية بالأمن السيبراني>.

2- **مراجعة الوثيقة وتحديثها:** <الإدارة المعنية بالأمن السيبراني>.

3- **تنفيذ الوثيقة وتطبيقها:** <الإدارة المعنية بالأمن السيبراني> و<الإدارة المعنية بالموارد البشرية>.