دورة تدريبية: حوكمة الأمن السيبراني

أساسيات إدارة المخاطر والإمتثال في الأمن السيبراني

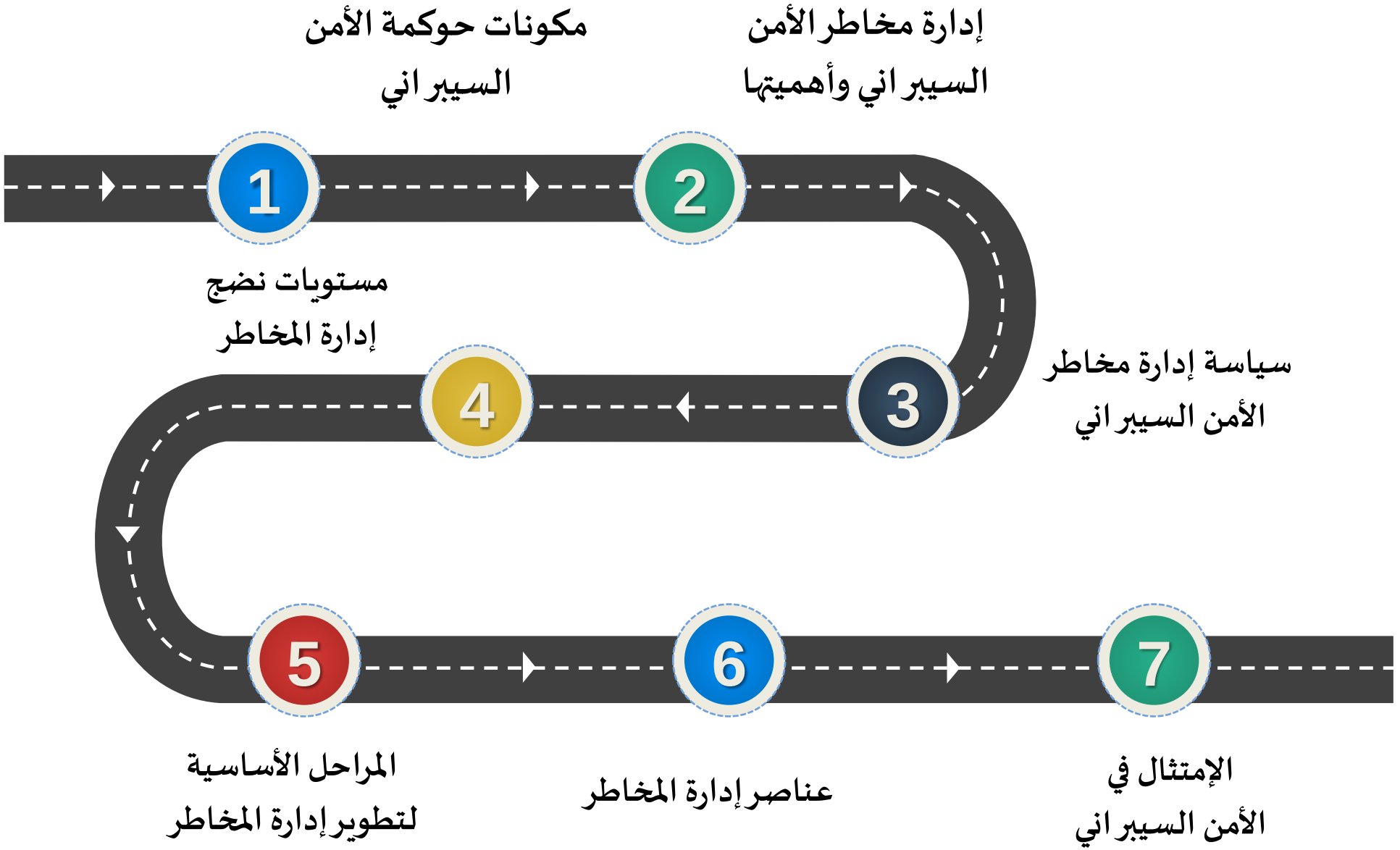
المحاضرة الخامسة (الجزء الأول)

د. غالب الشمري

أستاذ الذكاء الإصطناعي وعلم البيانات المساعد

جامعة الملك سعود

خارطة الطريق



حوكمة الأمن السيبراني

تتطلب حوكمة الأمن السيبراني وضع الأساس لسياسات وإجراءات الأمن السيبراني لكل منظمة، وذلك من خلال تحديد متطلبات الإمتثال التي تنطبق على المنظمة الخاضعة. هذه المتطلبات تحتاج إلى البحث وفهم الإلتزامات وأطر الإمتثال وتحديد المعايير المطلوب تنفيذها.

كما يجب تحليل الفجوات وتقييم قدرات الأنظمة للوصول للمستهدفات المرجوة، ويتطلب ذلك وضع إستراتيجية تأخذ في الإعتبار الإستحواذ، التطوير، الأمن، العلميات، الإدارة، وتخصيص الموارد البشرية، بما في ذلك تحديد وتوزيع الوظائف والأدوار والمسؤوليات. وأخيراً تحديث السياسات والعلميات والإجراءات ونشرها لتثقيف الموظفين وضمان إحترام الأمن السيبراني والحوكمة. لذلك يجب أن تكون السياسات متوافقة بشكل واضح مع أهداف المنظمة. يمكن إستخدام أطر إدارة المخاطر لتتبع الأنظمة عن طريق تحديد الضوابط والمخاطر التي يمكن مراقبتها وتعديلها بإستمرار مع نمو الأعمال.

عصف ذهني

من وجهة نظرك
ما هي المكونات الأساسية
لحوكمة الأمن السيبراني؟

مكونات حوكمة الأمن السيبراني

01 إستراتيجية الأمن السيبراني

02 إدارة الأمن السيبراني

03 سياسات وإجراءات الأمن السيبراني

04 أدواروومسؤوليات الأمن السيبراني

05 إدارة مخاطر الأمن السيبراني

مكونات حوكمة الأمن السيبراني

06 | الأمن السيبراني ضمن إدراة المشاريع المعلوماتية والتقنية

07 | الإلتزام بالتشريعات وتنظيمات ومعايير الأمن السيبراني

08 | المراجعة والتدقيق الدوري للأمن السيبراني

09 | الأمن السيبراني المتعلق بالموارد البشرية

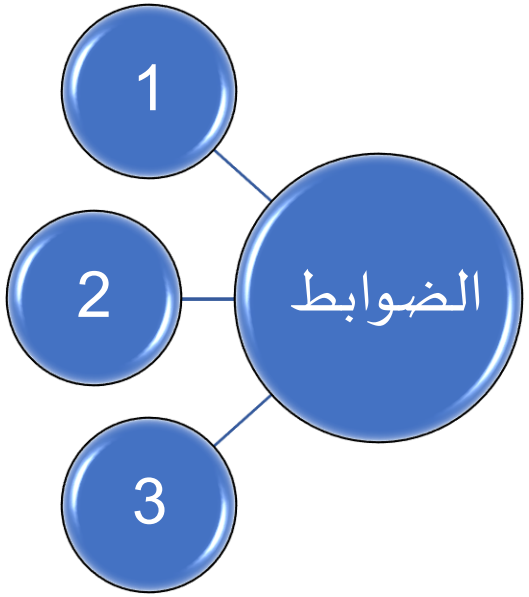
10 | برنامج التوعية والتدريب بالأمن السيبراني

عصف ذهني

من وجهة نظرك
ما هو الهدف الرئيسي من وضع
إستراتيجية للأمن السيبراني؟

إستراتيجية الأمن السيبراني

الهدف: ضمان إسهام خطط العمل للأمن السيبراني والأهداف والمبادرات والمشاريع داخل الجهة في تحقيق المتطلبات التشريعية والتنظيمية ذات العلاقة.



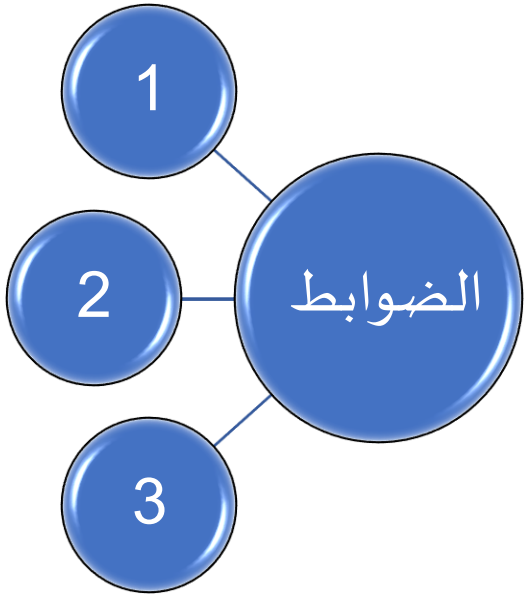
1. يجب تحديد وتوثيق واعتماد إستراتيجية الأمن السيبراني للجهة ودعمها من قبل القادة العليا ويشار له في هذه الضوابط باسم (صاحب الصالحية)، وأن تتماشى الأهداف الإستراتيجية للأمن السيبراني للجهة مع المتطلبات التشريعية والتنظيمية ذات العلاقة
2. يجب العمل على تنفيذ خطة عمل لتطبيق إستراتيجية الأمن السيبراني من قبل الجهة
3. يجب مراجعة إستراتيجية الأمن السيبراني على فترات زمنية مخطط لها (أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العالقة).

عصف ذهني

من وجهة نظرك
ما هي مهام إدارة الأمن
السيبر اني؟

إدارة الأمن السيبراني

الهدف: ضمان إلتزام ودعم صاحب الصلاحية للجهة فيما يتعلق بإدارة وتطبيق برامج الأمن السيبراني في تلك الجهة وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.



يجب إنشاء إدارة معنية بالأمن السيبراني في الجهة مستقلة عن إدارة تقنية المعلومات والإتصالات (ICT/IT) وفقاً للأمر السامي الكريم رقم 37140 وتاريخ 14 / 8 / 1438 هـ ويفضل ارتباطها مباشرة برئيس الجهة أو من ينيبه، مع الأخذ بالإعتبار عدم تعارض المصالح.

يجب أن يشغل رئاسة الإدارة المعنية بالأمن السيبراني والوظائف الإشرافية والحساسة بها مواطنون متفرغون وذو كفاءة عالية في مجال الأمن السيبراني.

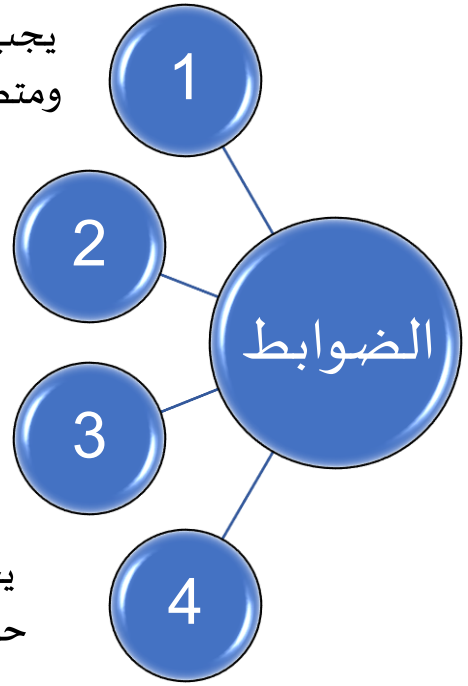
يجب إنشاء لجنة إشرافية للأمن السيبراني بتوجيه من صاحب الصلاحية للجهة لضمان التزام ودعم ومتابعة تطبيق برامج وتشريعات الأمن السيبراني، ويتم تحديد وتوثيق واعتماد أعضاء اللجنة ومسؤولياتها وإطار حوكمة أعمالها على أن يكون رئيس الإدارة المعنية بالأمن السيبراني أحد أعضائها.

عصف ذهني

من وجهة نظرك
ما هي الفائدة المرجوة من
سياسات وإجراءات
الأمن السيبراني؟

سياسات وإجراءات الأمن السيبراني

الهدف: ضمان توثيق ونشر متطلبات الأمن السيبراني والتزام الجهة بها، وذلك وفقاً لمتطلبات الأعمال التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.



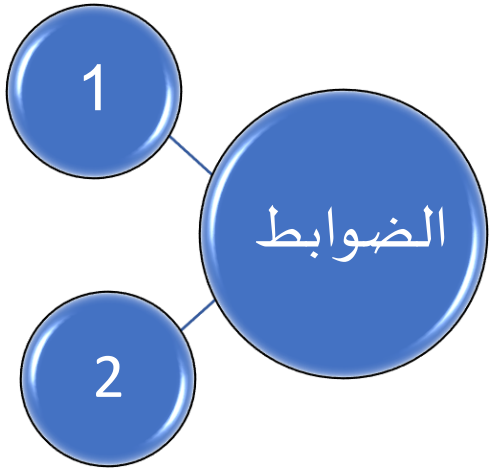
1. يجب على الإدارة المعنية بالأمن السيبراني في الجهة تحديد سياسات وإجراءات الأمن السيبراني وما تشمله من ضوابط ومتطلبات الأمن السيبراني، وتوثيقها واعتمادها من قبل صاحب الصلاحية في الجهة، كما يجب نشرها إلى ذوي العلاقة من العاملين في الجهة والأطراف المعنية بها.
2. يجب على الإدارة المعنية بالأمن السيبراني ضمان تطبيق سياسات وإجراءات الأمن السيبراني في الجهة وما تشمله من ضوابط ومتطلبات.
3. يجب أن تكون سياسات وإجراءات الأمن السيبراني مدعومة بمعايير تقنية أمنية (على سبيل المثال: المعايير التقنية الأمنية لجدار الحماية وقواعد البيانات، وأنظمة التشغيل، إلخ).
4. يجب مراجعة منهجية وإجراءات إدارة مخاطر الأمن السيبراني وتحديثها على فترات زمنية مخطط لها (أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية والمعايير ذات العالقة)، كما يجب توثيق التغييرات واعتمادها.

عصف ذهني

من وجهة نظرك
لماذا نحدد أدواروومسؤوليات
الأمن السيبر اني؟

أدواروومسؤوليات الأمن السيبراني

الهدف: ضمان تحديد أدوار ومسؤوليات واضحة لجميع الأطراف المشاركة في تطبيق ضوابط الأمن السيبراني في الجهة.



يجب على صاحب الصلاحية تحديد وتوثيق واعتماد الهيكل التنظيمي للحوكمة والأدوار والمسؤوليات الخاصة بالأمن السيبراني للجهة، وتكليف الأشخاص المعنيين بها، كما يجب تقديم الدعم اللازم لإنفاذ ذلك، مع الأخذ بالإعتبار عدم تعارض المصالح.

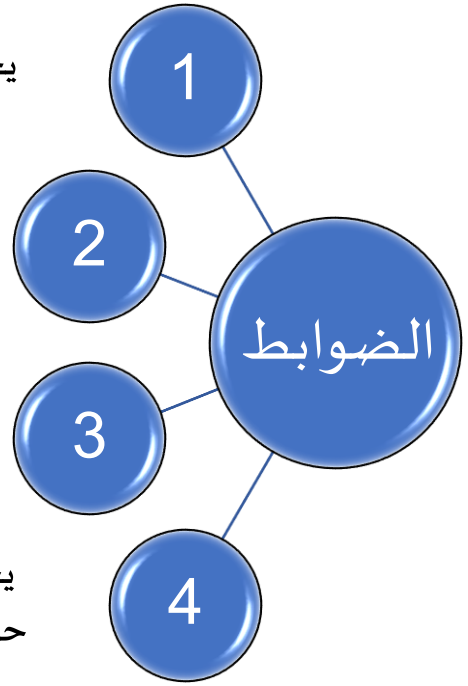
يجب مراجعة أدوار ومسؤوليات الأمن السيبراني في الجهة وتحديثها على فترات زمنية مخطط لها (أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العالقة).

عصف ذهني

من وجهة نظرك
هل هناك علاقة بين إدارة المخاطروالأمن السيبراني؟
أشرحها؟

إدارة المخاطر الأمن السيبراني

الهدف: ضمان إدارة مخاطر الأمن السيبراني على نحو ممنهج يهدف إلى حماية الأصول المعلوماتية والتقنية للجهة، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة والمتطلبات التشريعية والتنظيمية.



يجب على الإدارة المعنية بالأمن السيبراني في الجهة تحديد وتوثيق واعتماد منهجية وإجراءات إدارة مخاطر الأمن السيبراني في الجهة. وذلك وفقاً لإعتبارات السرية وتوافر وسلامة الأصول المعلوماتية والتقنية.

يجب على الإدارة المعنية بالأمن السيبراني تطبيق منهجية وإجراءات إدارة مخاطر الأمن السيبراني في الجهة.

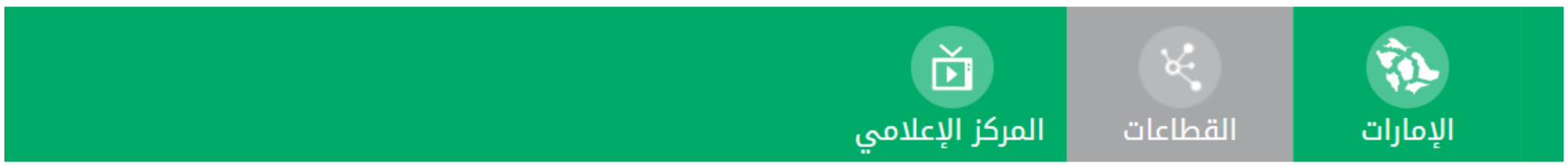
يجب تنفيذ إجراءات تقييم مخاطر الأمن السيبراني بحد أدنى في الحالات التالية:
المراحل المبكرة للمشاريع التقنية، قبل إجراء تغيير جوهري في البنية التحتية، عند التخطيط للحصول على خدمات طرف خارجي، عند التخطيط لإطلاق منتجيات وخدمات تقنية جديدة

يجب مراجعة منهجية وإجراءات إدارة مخاطر الأمن السيبراني وتحديثها على فترات زمنية مخطط لها (أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية والمعايير ذات العالقة)، كما يجب توثيق التغييرات واعتمادها.

الرؤية

طباعة إرسال مشاركة

القدرة والسرعة والمرونة والاحترافية في تنفيذ المهام وإدارة الأسطول الجوي بكفاءة حسب المتغيرات.



الرسالة

طباعة إرسال مشاركة

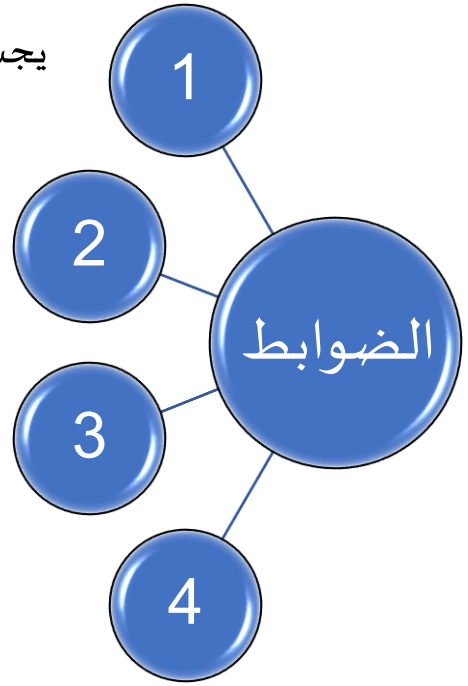
الحفاظ على الأمن الداخلي بالتعاون مع القطاعات الأمنية وتقديم الخدمات الإنسانية للمواطن والمقيم.

عصف ذهني

من وجهة نظرك
ما هو تأثير الأمن السيبراني على
إدارة المشاريع المعلوماتية؟

الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية

الهدف: التأكد من أن متطلبات الأمن السيبراني مضمنة في منهجية وإجراءات إدارة مشاريع الجهة لحماية السرية وسلامة الأصول المعلوماتية والتقنية للجهة ودقتها وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة.



يجب تضمين متطلبات الأمن السيبراني في منهجية وإجراءات إدارة المشاريع وفي إدارة التغيير على الأصول المعلوماتية والتقنية في الجهة لضمان تحديد مخاطر الأمن السيبراني ومعالجتها كجزء من دورة حياة المشروع التقني.

يجب أن تغطي متطلبات الأمن السيبراني لإدارة المشاريع والتغييرات على الأصول المعلوماتية والتقنية للجهة بحد أدنى: تقييم الثغرات ومعالجتها، وإجراء مراجعة للإعدادات والتحصين وحزم التحديثات.

يجب أن تغطي متطلبات الأمن السيبراني لمشاريع تطوير التطبيقات والبرمجيات الخاصة للجهة بحد أدنى: معايير التطوير الآمن للتطبيقات، إستخدام مصادر موثوقة ومرخصة، إجراء إختبار التحقق لمدى إستيفاء متطلبات الأمن السيبراني، وأمن التكامل بين التطبيقات.

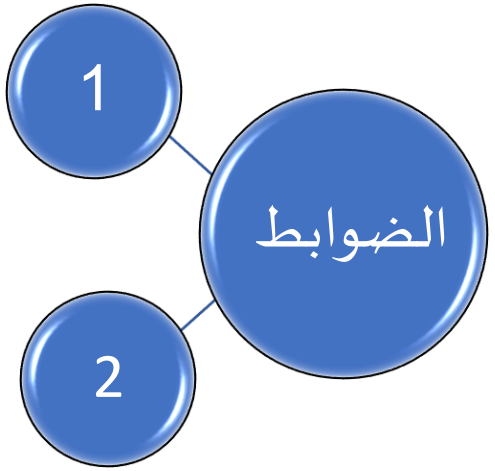
يجب مراجعة متطلبات الأمن السيبراني في إدارة المشاريع في الجهة دورياً.

عصف ذهني

من وجهة نظرك
هل يستلزم وضع تشريعات
وتنظيمات للأمن السيبر اني؟
ولماذا؟

الإلتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني

الهدف: ضمان التأكد من أن برنامج الأمن السيبراني لدى الجهة يتوافق مع المتطلبات التشريعية والتنظيمية ذات العلاقة.

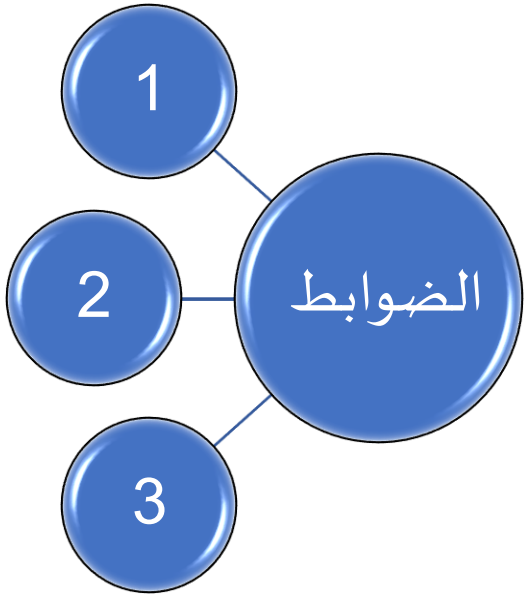


يجب على الجهة الإلتزام بالمتطلبات التشريعية والتنظيمية الوطنية المتعلقة بالأمن السيبراني

يجب على الجهة الإلتزام بمتطلبات الإتفاقيات أو والإلتزامات الدولية المعتمدة محلياً والتي تتضمن متطلبات خاصة بالأمن السيبراين

المراجعة والتدقيق الدوري للأمن السيبراني

الهدف: ضمان التأكد من أن ضوابط الأمن السيبراني لدى الجهة مطبقة وتعمل وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية الوطنية، والمتطلبات الدولية المُقرة تنظيمياً على الجهة.



يجب على الإدارة المعنية بالأمن السيبراني في الجهة مراجعة تطبيق ضوابط الأمن السيبراني دورياً.

يجب مراجعة وتدقيق تطبيق ضوابط الأمن السيبراني في الجهة، من قبل أطراف مستقلة عن الإدارة المعنية بالأمن السيبراني (مثل الإدارة المعنية بالمراجعة في الجهة). على أن تتم المراجعة والتدقيق بشكل مستقل يراعى فيه مبدأ عدم تعارض المصالح، وذلك وفقاً للمعايير العامة المقبولة للمراجعة والتدقيق والمتطلبات التشريعية والتنظيمية ذات العلاقة.

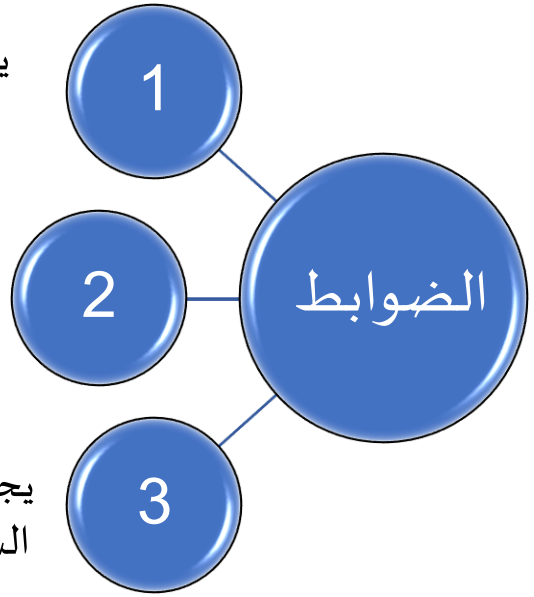
يجب توثيق نتائج مراجعة وتدقيق الأمن السيبراني، وعرضها على اللجنة الإشرافية للأمن السيبراني وصاحب الصلاحية. كما يجب أن تشتمل النتائج على نطاق المراجعة والتدقيق، والملاحظات المكتشفة، والتوصيات والإجراءات التصحيحية، وخطة معالجة الملاحظات.

عصف ذهني

من وجهة نظرك
ما هو تأثير الأمن السيبراني على
الموارد البشرية؟ مع ذكر مثال؟

الأمن السيبراني المتعلق بالموارد البشرية

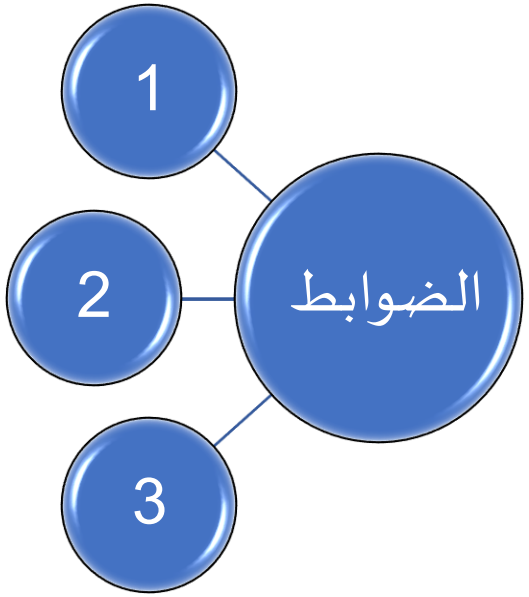
الهدف: ضمان التأكد من أن مخاطر ومتطلبات الأمن السيبراني المتعلقة بالعاملين (موظفين ومتعاقدين) في الجهة تعالج بفعالية قبل وأثناء وعند انتهاء/إنهاء عملهم، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العالقة.



1. يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني المتعلقة بالعاملين قبل توظيفهم وأثناء عملهم وعند انتهاء/إنهاء عملهم في الجهة.
2. يجب تطبيق متطلبات الأمن السيبراني المتعلقة بالعاملين في الجهة.
3. يجب أن تغطي متطلبات الأمن السيبراني قبل بدء علاقة العاملين المهنية بالجهة بحد أدنى: مسؤوليات الأمن السيبراني وبنود سرية المعلومات في عقود العاملين، وإجراء المسح الأمني للعاملين في وظائف الأمن السيبراني

الأمن السيبراني المتعلق بالموارد البشرية

الهدف: ضمان التأكد من أن مخاطر ومتطلبات الأمن السيبراني المتعلقة بالعاملين (موظفين ومتعاقدين) في الجهة تعالج بفعالية قبل وأثناء وعند انتهاء/إنهاء عملهم، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العالقة.



يجب أن تغطي متطلبات الأمن السيبراني قبل خلال علاقة العاملين المهنية بالجهة بحد أدنى:
التوعية بالأمن السيبراني، وتطبيق متطلبات الأمن السيبراني والإلتزام بها.

يجب مراجعة وإلغاء الصلاحيات للعاملين مباشرة بعد انتهاء/إنهاء
الخدمة المهنية لهم بالجهة.

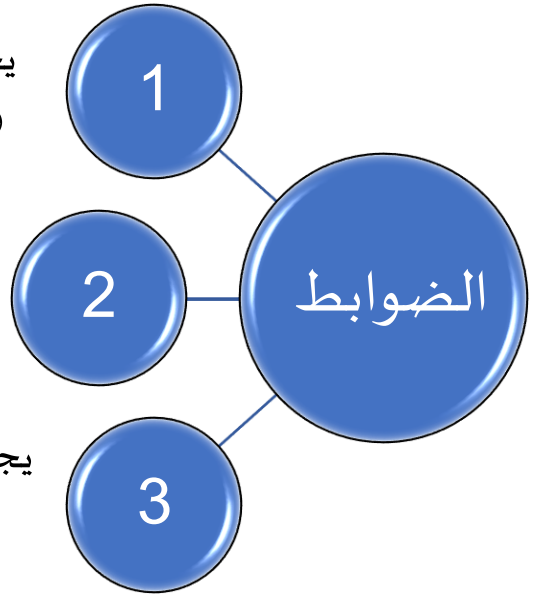
يجب مراجعة متطلبات الأمن السيبراني المتعلقة
بالعاملين في الجهة دورياً.

عصف ذهني

من وجهة نظرك
كيف يتم نشر الوعي بين موظفي الجهة حول مسؤولياتهم بما يتعلق بالأمن السيبراني؟

برنامج التوعية والتدريب بالأمن السيبراني

الهدف: ضمان التأكد من أن العاملين بالجهة لديهم التوعية الأمنية اللازمة وعلى دراية بمسؤولياتهم في مجال الأمن السيبراني. والتأكد من تزويد العاملين بالجهة بالمهارات والمؤهلات والدورات التدريبية المطلوبة في مجال الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة والقيام بمسؤولياتهم تجاه الأمن السيبراني.



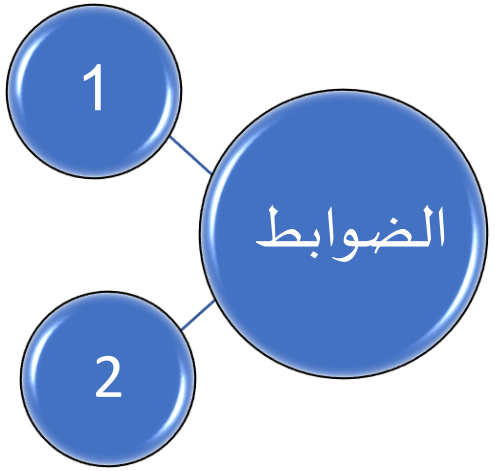
يجب تطوير واعتماد برنامج للتوعية بالأمن السيبراني في الجهة من خلال قنوات متعددة دورياً، وذلك لتعزيز الوعي بالأمن السيبراني وتهديداته ومخاطره، وبناء ثقافة إيجابية للأمن السيبراني

يجب تطبيق البرنامج المعتمد للتوعية بالأمن السيبراني في الجهة.

يجب أن يغطي برنامج التوعية بالأمن السيبراني كيفية حماية الجهة من أهم المخاطر والتهديدات السيبرانية وما يستجد منها، بما في ذلك: التعامل الآمن مع خدمات البريد الإلكتروني، الأجهزة المحمولة، وسائط التخزين، خدمات التصفح، ووسائل التواصل الاجتماعي.

برنامج التوعية والتدريب بالأمن السيبراني

الهدف: ضمان التأكد من أن العاملين بالجهة لديهم التوعية الأمنية اللازمة وعلى دراية بمسؤولياتهم في مجال الأمن السيبراني. والتأكد من تزويد العاملين بالجهة بالمهارات والمؤهلات والدورات التدريبية المطلوبة في مجال الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة والقيام بمسؤولياتهم تجاه الأمن السيبراني.



يجب توفير المهارات المتخصصة والتدريب الالزم للعاملين في المجاالت الوظيفية ذات العالقة المباشرة باألمن السيبراني في الجهة، وتصنيفها بما يتماشى مع مسؤولياتهم الوظيفية فيما يتعلق باألمن السيبراني، بما في ذلك:

يجب مراجعة تطبيق برنامج التوعية بالأمن السيبراني في الجهة دورياً.

إدارة المخاطر Risk Management وأهميتها

المخاطر هي حقيقة من حقائق الحياة، والإستعداد لها وتنمية القدرات لإداراتها هي الوسيلة لإكتساب ميزة تنافسية. تشير الدراسات في جامعة كورنيل Cornell University أن ما يقارب 35,000 قراراً يتم إتخاذه من قبل الفرد يومياً بشكل لا إرادي، من ضمنها 226 قراراً بشأن الغذاء وحده. هذه القرارات تزداد تعقيداً على مستوى المنظمات أخذاً بالإعتبار العوامل المؤثرة على تحقيق الأهداف، فالإتجاهات الاقتصادية والأحداث العالمية والتقنية المتغيرة المؤثرة تجعل المنظمات أكثر عرضة للخطر من أي وقت مضى.

أدى انهيار بعض أكبر الشركات الخاصة خلال العقد الماضي وتداعيات الأزمات العالمية إلى تسليط الضوء على الأهمية الكبرى لإدارة المخاطر باعتبارها أداة تتيح التعامل مع المخاطر المهمة ومعالجتها بشكل فعال. وعلى الرغم من أن مجال إدارة المخاطر قد نشأ أول الأمر في القطاع الخاص، الإ أن الكيانات في القطاع العام بدأت تهتم بشكل أكبر في دمج ممارسات إدارة المخاطر مع أنشطتها.

إدارة المخاطر Risk Management وأهميتها

هناك حاجة إلى نهج شمولي لإدارة المخاطر، والإنتقال من رد الفعل القائم على الإستجابة والإمتثال، إلى النظرة الإستباقية والتطلعية من أجل أن تكون إدارة المخاطر محركاً إستراتيجياً للأداء وإضافة قيمة في الجهة. إذ يقوم هذا النهج على تنفيذ عملية وآلية لإدارة المخاطر على نطاق الجهة، وجعل هذه العملية مسؤولية يتقاسمها الجميع، وإتاحة منهجية متسقة لتنفيذها لمواكبة تطورات الضغوط الخارجية المؤثرة واتخاذ خيارات مستنيرة من أجل النجاح والبقاء في المقدمة.

تعتبر إدارة المخاطر عنصر أساسي من عناصر الإدارة والمساءلة في المنظمات، وبما أنها تساعد على الإستعداد الأفضل للمستقبل والتعامل مع حالات عدم اليقين، فلا يمكن فصلها عن آليات تحديد الأولويات والتخطيط الإستراتيجي. وكون أن إدارة المخاطر تساعد على تقليل المخاطر المفاجئة، وتحديد الفرص، والحفاظ على استدامة الأعمال، من خلال الإستقراء المستمر للمستقبل وإختلاق أحداث وسيناريوهات «توقع الأسوأ»، فإنه من المهم الإشارة إلى أن المخاطر والفرص عاملان لا ينفصلان على الرغم من إختلاف تعريفهما. حيث تركز أدوات إدارة المخاطر الفعالة لتحديد المخاطر على الفرص بقدر ما تركز على المخاطر، علماً أن الإخفاق في رصد الفرص المتاحة لتحقيق أهداف الجهة هو خطر في حد ذاته. وينبغي التأكيد أن إدارة المخاطر لا تضمن إمكانية تحديد جميع المخاطر الهامة والتصدي لها وتحقيق الأهداف وإنما تعزز تلك الإمكانية.

فترة نقاش

من خلال ما سبق
ما هو المقصود بإدارة مخاطر
الأمن السيبراني؟

إدارة مخاطر الأمن السيبراني

"هي إستراتيجية شاملة لتحديد الأصول المعلوماتية مثل الأجهزة وبيانات العملاء والملكية الفكرية التي يتم إختراقها نتيجة الهجمات السيبرانية، ومن ثم يتم تقييم المخاطر المحتملة التي يمكن أن تؤثر على هذه الأصول لتطبيق عناصر التحكم الأمني السيبراني المناسبة"

سياسة إدارة مخاطر الأمن السيبراني الهيئة الوطنية للأمن السيبراني

نطاق العمل وقابلية التطبيق:

تغطي سياسة إدارة مخاطر الأمن السيبراني جميع الأصول المعلوماتية والتقنية وأنظمة وأجهزة التحكم للجهات، ,إجراءات العمل وتطبيقها على جميع العاملين في الجهة.

بنود سياسة إدارة مخاطر الأمن السيبراني:

- البنود العامة
- المراحل الرئيسية لإدارة المخاطر السيبرانية
- مستوى المخاطر المقبولة
- متطلبات أخرى

https://nca.gov.sa/cybersecurity_risk_management_policy_template_v1.0.docx

عصف ذهني

من وجهة نظرك
وضع أمثلة خاصة بالبنود العامة
لسياسة إدارة الأمن السيبراني؟

سياسة إدارة مخاطر الأمن السيبراني: البنود العامة

- يجب تطوير وتوثيق وإعتماد منهجية إدارة مخاطر الأمن السيبراني وإجراءاتها في الجهة ومواءمتها مع الإطار الوطني لمخاطر الأمن السيبراني، كما أنه يمكن إستخدام المعايير والأطر التوجيهية المعتمدة دولياً (NIST, ISO31000, ISO27005) في تطوير منهجية إدارة مخاطر الأمن السيبراني.
- يجب تغطية (تحديد الأصول ومعرفة أهميتها، تحديد وتقييم المخاطر سواءً للأعمال أو أصول أو العاملين، تحديد التهديدات والثغرات المتعلقة بالأمن السيبراني التي قد تؤثر على الأصول المعلوماتية والتقنية وتقييمها، تحديد أساليب التعامل مع المخاطر السيبرانية، ترتيب التدابير للحد من المخاطر السيبرانية حسب الأولوية ووفقاً لإجراءات محددة، تصنيف مستويات المخاطر السيبرانية وتعرفيها بناءً على مستوى التأثير وإحتمالية حدوث التهديد، إنشاء سجل مخاطر الأمن السيبراني لتوثيق المخاطر ومتابعتها، وأخيراً تحديد الأدوار والمسؤوليات لإدارة مخاطر الأمن السيبراني والتعامل معها) في منهجية إدارة مخاطر الأمن السيبراني.
- يجب تنفيذ تقييم المخاطر دورياً لضمان حماية الأصول المعلوماتية والتقنية والتعامل مع المخاطر حسب الأولوية.
- يجب أن تكون إدارة مخاطر الأمن السيبراني متوافقة مع إدارة المخاطر المؤسسية.

https://nca.gov.sa/cybersecurity_risk_management_policy_template_v1.0.docx

عصف ذهني

من وجهة نظرك
أذكر المراحل الرئيسية لإدارة
مخاطر الأمن السيبراني؟

سياسة إدارة مخاطر الأمن السيبراني: المراحل الرئيسية

https://nca.gov.sa/cybersecurity_risk_management_policy_template_v1.0.docx

سياسة إدارة مخاطر الأمن السيبراني: المراحل الرئيسية

تحديد المخاطر

يجب أن تُحدّد الإدارة المعنية بالأمن السيبراني الأحداث أو الظروف التي من الممكن أن تنتهك سريّة الأصول المعلوماتية والتقنية وسلامتها وتوافرها، ويشمل ذلك على وجه الخصوص تحديد الأصول المعلوماتية والتقنية، والتهديدات التي من المحتمل أن تتعرّض لها والثغرات ذات الصلة، والضوابط المعتمدة، ومن ثمّ تحديد الآثار الناتجة عن فقدان سريّة هذه الأصول وسلامتها وتوافرها.

https://nca.gov.sa/cybersecurity_risk_management_policy_template_v1.0.docx

سياسة إدارة مخاطر الأمن السيبراني: المراحل الرئيسية

تقييم المخاطر

- **يجب على الإدارة تنفيذ الإجراءات لتقييم مخاطر الأمن السيبراني، بحد أدنى ما يلي:**
  - في المراحل الأولية من المشاريع التقنية
  - قبل إجراء تغيير جوهري في البنة التقنية
  - عند التخطيط للحصول على خدمات طرف خارجي
  - عند التخطيط وقبل إطلاق منتجات أو خدمات جديدة
- **يجب إعادة تقييم المخاطر وتحديثها، على النحو التالي:**
  - دورياً لجميع الأصول المعلوماتية والتقنية، وسنوياً على الأقل للأنظمة الحساسة
  - بعد وقوع حادث متعلق بالأمن السيبراني ينتهك سلامة الأصول وتوافرها وسريتها
  - بعد الحصول على نتائج تدقيق مهمة أو معلومات إستباقية
  - في حال التغيير على الأصول المعلوماتية والتقنية

https://nca.gov.sa/cybersecurity_risk_management_policy_template_v1.0.docx

سياسة إدارة مخاطر الأمن السيبراني: المراحل الرئيسية

تقييم المخاطر

- **يجب أن تغطي عملية تقييم المخاطر ما يلي:**
  - تحليل المخاطر Risk Analysis: تقيم الإدارة إحتمالية وقوع التهديدات والأثار الناتجة عنها، وتستخدم نتائج التقييم لتحديد المستوى العام لهذه المخاطر، ويجب أن تعتمد الإدارة منهجية كمية ونوعية لإجراء التحليل.
  - تقدير المخاطر Risk Evaluation: تُقدر الإدارة حجم المخاطر السيبرانية بالتوافق مع معايير تقدير المخاطر المؤسسية المعتمدة في الجهة وتحديد أساليب التعامل معها حسب الأولوية.

https://nca.gov.sa/cybersecurity_risk_management_policy_template_v1.0.docx

سياسة إدارة مخاطر الأمن السيبراني: المراحل الرئيسية

معالجة المخاطر

- **يجب أن تحدد الإدارة خيارات معالجة المخاطر حسب القائمة التالية:**
  - معالجة المخاطر وتقليلها Risk Mitigation: من خلال تطبيق الضوابط الأمنية اللازمة لتقليل إحتمال الحدوث أو التأثير أو كليهما والتي تساعد في إحتواء المخاطر والمحافظة على مستويات مقبولة.
  - تجنب المخاطر Risk Avoidance: التخلص من الخطر بتجنب الإستمرار بمصدر الخطر.
  - مشاركة المخاطر أو تحويلها Risk Transfer: مشاركة المخاطر مع طرف ثالث لديه الإمكانيات في التعامل مع المخاطر بشكل أكثر فعالية أو التأمين على الأصول المعلوماتية والتقنية.
  - تقبل المخاطر وتحملها Risk Acceptance: مستوى الخطر المقبول ولكن يجب مراقبته بإستمرار في حال حدوث تغيير في التأثير.
- **يجب تحديد خيارات معالجة المخاطر وتوثيقها بناءً على نتائج تقييم المخاطر وتكلفة التنفيذ والمنافع المتوقعة.**

https://nca.gov.sa/cybersecurity_risk_management_policy_template_v1.0.docx

سياسة إدارة مخاطر الأمن السيبراني: المراحل الرئيسية

متابعة المخاطر

- **يجب أن تُعد الإدارة سجلاً للمخاطر وأن تحافظ عليه لتوثيق مخرجات عملية إدارة المخاطر، على أن يشمل بحد أدنى ما يلي:**
  - عملية تحديد المخاطر ونطاق المخاطر
  - المسؤول أو صاحب المخاطر ووصف للمخاطر بما في ذلك أسبابها وأثارها
  - تحليل للمخاطر السيبرانية يوضح التأثيرات ونطاقها الزمني، وتقييم وتصنيف للمخاطر وإحتماليه وقوعها
  - خطة التعامل مع المخاطر تتضمن التعامل معها والمسؤول عنها وجدولها الزمني ووصف للخطر المتبقي
- **يجب إستخدام مؤشر قياس الأداء KPI لضمان فعالية إدارة مخاطر الأمن السيبراني.**
- **يجب على الإدارة جمع الأدلة المتعلقة بحالة المخاطر السيبرانية ومراجعتها بشكل دوري.**

https://nca.gov.sa/cybersecurity_risk_management_policy_template_v1.0.docx

سياسة إدارة مخاطر الأمن السيبراني: مستوى المخاطر المقبول

- يجب تحديد معايير تقبل المخاطر وتوثيقها، وفقاً لمستوى المخاطر وتكلفة معالجة الخطر مقابل تأثيره.
- يجب تطبيق ضوابط إضافية من أقل تقليل المخاطر إلى مستوى مقبول في عدم إستيفاء الخطر المتبقي لمعايير تقليل المخاطر.
- في حال تجاوز معايير تقبل المخاطر، يتم التصعيد لصاحب الصلاحية لإتخاذ الإجراءات أو القرارات اللازمة.

https://nca.gov.sa/cybersecurity_risk_management_policy_template_v1.0.docx

سياسة إدارة مخاطر الأمن السيبراني: متطلبات أخرى

- يجب مراجعة منهجية وإجراءات إدارة مخاطر الأمن السيبراني وتحديثها على فترات زمنية مخطط لها (أو في حال حدوث تغييرات في المتطلبات التشريعية والتنظيمية والمعايير ذات العلاقة)، كما يجب توثيق التغييرات وإعتمادها.
- يجب مراجعة سياسة إدارة مخاطر الأمن السيبراني سنوياً، وتوثيق التغييرات وإعتمادها.

https://nca.gov.sa/cybersecurity_risk_management_policy_template_v1.0.docx

المبادئ الأساسية لإدارة المخاطر

توضح هذه المبادئ إرشادات حول خصائص إدارة المخاطر الفعالة ومشاركة قيمتها، تلك المبادئ ينبغي أخذها في الإعتبار عند إنشاء إطار وأجراءات إدارة المخاطر في الجهة.

01 الحوكمة والقيادة

02 التكامل

03 التعاون والحصول على معلومات

04 إجراءات إدارة المخاطر

05 التحسين والتطوير

المبادئ الأساسية لإدارة المخاطر: الحوكمة والقيادة

ينبغي أن تكون أنشطة إدارة المخاطر جزءً من حوكمة وقيادة الجهة، وأساسية في إدارتها وتوجيهها وضبط أعمالها على جميع المستويات التنظيمية، وعلى الجهة إعداد حوكمة إدارة مخاطر أمن سيبراني مناسب لطبيعة أعمالها ونطاقها وثقافتها والتي تتضمن تحديد أدوار ومسؤوليات الجهات العنية، وآلية ومنهجية إدارة مخاطرها الرئيسية وتكرار مراقبة ورفع تقارير عن حالة المخاطر.

المبادئ الأساسية لإدارة المخاطر: التكامل

يجب أن تكون إدارة المخاطر جزءً لا يتجزأ من جيمع الأنشطة التنظيمية التي تدعم إتخاذ القرار لتحقيق الأهداف الإستراتيجية للجهة والتي تتضمن الآتي:

- تحديد وإعداد إستراتيجية وخطط الجهة التنفيذية
- إعداد وتنفيذ برامج ومشاريع الجهة
- تحديد أولوية الموارد
- دعم الأعمال التشغيلية
- إدارة الأداء والأصول وكافة أنواعها

المبادئ الأساسية لإدارة المخاطر: التعاون والحصول على المعلومات

ينبغي على الجهة تصميم إطار عمل لإداة المخاطر يدعم الرؤية الشاملة لمخاطر الجهة ومتطلبات صنع القرار والحوكمة، وتنفيذ اجراءات إدارة المخاطر بشكل منتظم وتعاوني باالعتماد على معرفة وآراء الخبراء وأصحاب المصلحة.

المبادئ الأساسية لإدارة المخاطر: التحسين والتطوير

ينبغي على الجهة مراجعة وتحديث إطار إدارة المخاطر بشكل مستمر لضمان موائمة أنشطة إدارة المخاطر بحيث تتماشى مع التغييرات الخارجية والداخلية. كما ينبغي على الجهة أن تعمل بإستمرار على تحسين كفاية وفعالية إطار إدارة المخاطر. وفي سياق إنشاء إدارة المخاطر في أي جهة ينبغي القيام بتقييم القدرة الخاصة بالممارسات الحالة لإدارة المخاطر. وبناءً عليها يتم تقديم التوصيات اللازمة لتطوير قدرات إدارة المخاطر والوصول إلى مراجل نضج متقدمة.

عصف ذهني

مما سبق ذكره

ما المقصود بنضج إدارة المخاطر؟

مستويات نضج إدارة المخاطر

مستويات نضج إدارة المخاطر

مستوى النضج	
متكاملة	• يتم إحتساب مقاييس الخطر التي يمكن دمجها • معالجة متكاملة للمخاطر والحد الأمثل للتكاليف ذات الصلة • تنسيق أنشطة إدارة المخاطر في مجالات الأعمال • حدود تقبل وتحمل المخاطر محددة • تطبيق التقنية والأنظمة لأتمتة إجراءات إدارة المخاطر • مراقبة المخاطر على مستوى الجهة وقياسها والإبلاغ عنها • وجود خطط للطوارئ وإجراءات للتصعيد • تضمين مبادئ ومتطلبات إدارة المخاطر في أعمال ومشاريع الجهة
شاملة	• إجراء تقييم للمخاطر على مستوى الجهة وتنفيذ خطط معالجة المخاطر ذات الأولوية • إجراءات إدارة المخاطر معرفة وموثقة • توجد نظرة مستقبلية وآلية للمسائلة • إطار عمل مشترك وسياسة محددة، بالإضافة إلى وجود مخاطر موثقة ونهج استباقي واضح للمسألة • الإبلاغ عن أهم المخاطر الاستراتيجية التي تواجه الجهة للمناصب العليا • وجود أنشطة للتوعية • إدارة متخصصة في المخاطر ومشاركتها بين الأعضاء

مستويات نضج إدارة المخاطر

متطورة – الإدارة الذكية

- التركيز على خلق القيمة المضافة والحفاظ عليها
- تكون المخاطر مرتبطة بشكل واضح مع الأهداف الإستراتيجية
- القدرة على إدارة المخاطر بناءً على الأحداث السابقة والمرتقبة
- تضمين مناقشة المخاطر في التخطيط الإستراتيجي
- يوجد نظام إنذار مبكر لإبلاغ حول المخاطر التي تتجاوز حدود تقبل وتحمل المخاطر
- يوجد ربط لإدارة المخاطر مع مقياس الأداء والحوافز
- عملية منظمة لتقييم المخاطر وقياس المخاطر والإبلاغ عنها
- تستغل الجهة الفرص بطريقة انتقائية نظرًا لقدرتها على استغلال المخاطر
- إعداد نماذج المخاطر والسيناريوهات

عصف ذهني

من وجهة نظرك
ما هي المراحل الرئيسية لإدارة
المخاطرفي جهة معينة بشكل عام؟

المراحل الأساسية لتطوير إدارة المخاطر

تقييم الوضع الراهن لإدارة المخاطر في الجهة

1

- تقييم الوضع الراهن لممارسات إدارة المخاطر في الجهة وتحديد الفجوات
- مقارنة الوضع الراهن مع جدول مستويات النضج وتحديد مستوى النضج الحالي
- إعداد خطة تنفيذية لمعالجة الفجوات والوصول إلى مستويات النضج المطلوبة وبناء قدرات إدارة المخاطر في الجهة

تطوير إطار عمل والبنية التحتية لإدارة المخاطر

2

- فهم البيئة الداخلية والخارجية للجهة
- إعداد إستراتيجية إدارة المخاطر ومؤشرات تقييم الأداء
- تحديد أدوار ومسؤوليات أصحاب المصلحة والجهات المعنية في إدارة مخاطر الجهة
- تصميم وإعداد الهيكل التنظيمي والنموذج التشغيلي لإدارة المخاطر

المراحل الأساسية لتطوير إدارة المخاطر

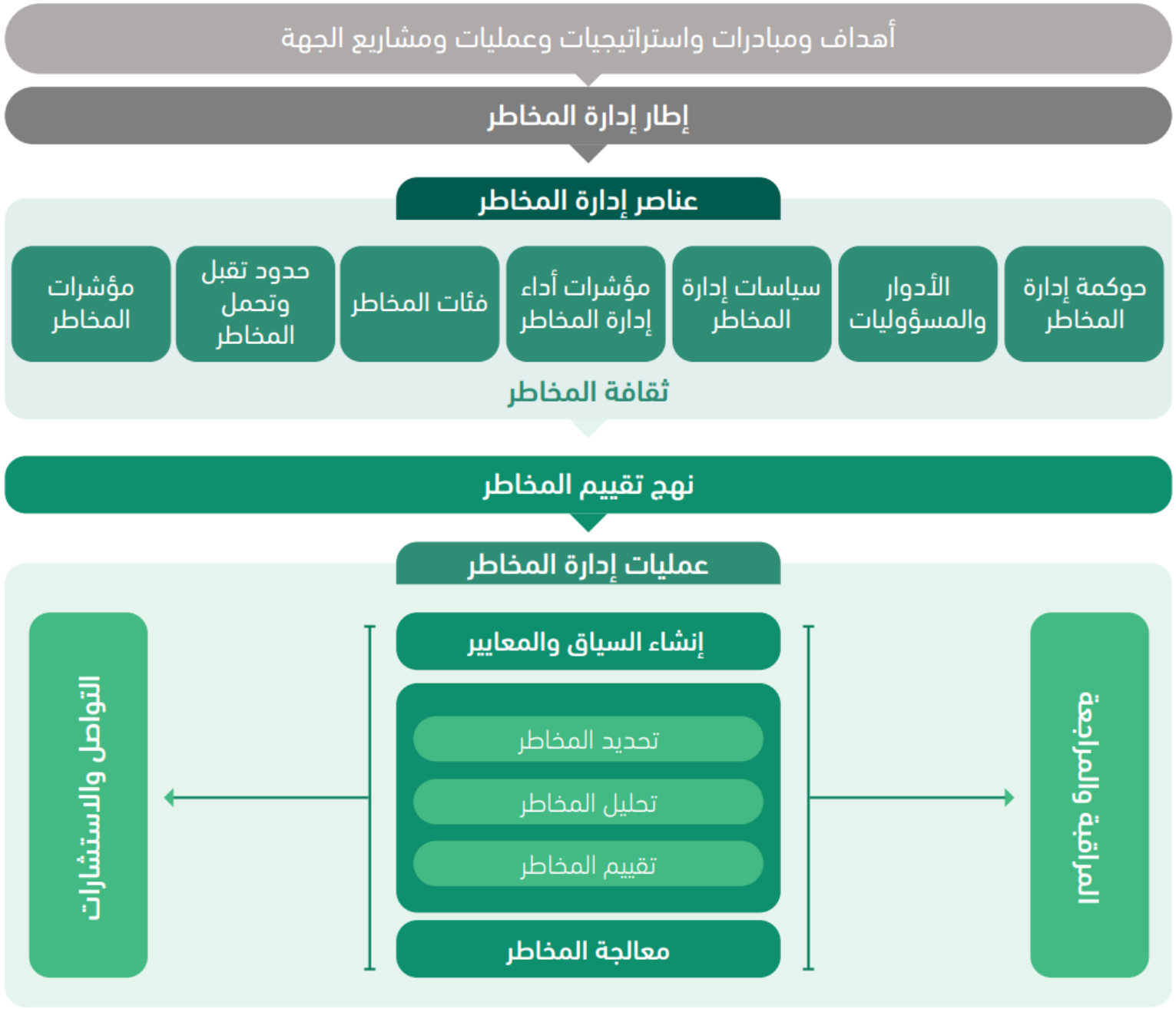
3 تحديد حدود تقبل وتحمل المخاطر وإعداد معايير تقييم المخاطر

- تحديد حدود تقبل وتحمل الجهة للمخاطر
- إعداد مقاييس آثار واحتمالية وقوع المخاطر بالإضافة إلى تقييم الضوابط الرقابية
- تحديد فئات المخاطر التي قد تتعرض لها الجهة

4 إعداد وتطوير سياسات وإجراءات عمل إدارة المخاطر

- إعداد سياسات إدارة المخاطر حسب المعيار المتبع في الجهة
- إعداد إجراءات عمل إدارة المخاطر تتضمن كافة تفاصيل عمليات إدارة المخاطر حسب المعيار المتبع
- تصميم وإعداد كافة نماذج التقارير وسجلات المخاطر

إطار
إدارة المخاطر



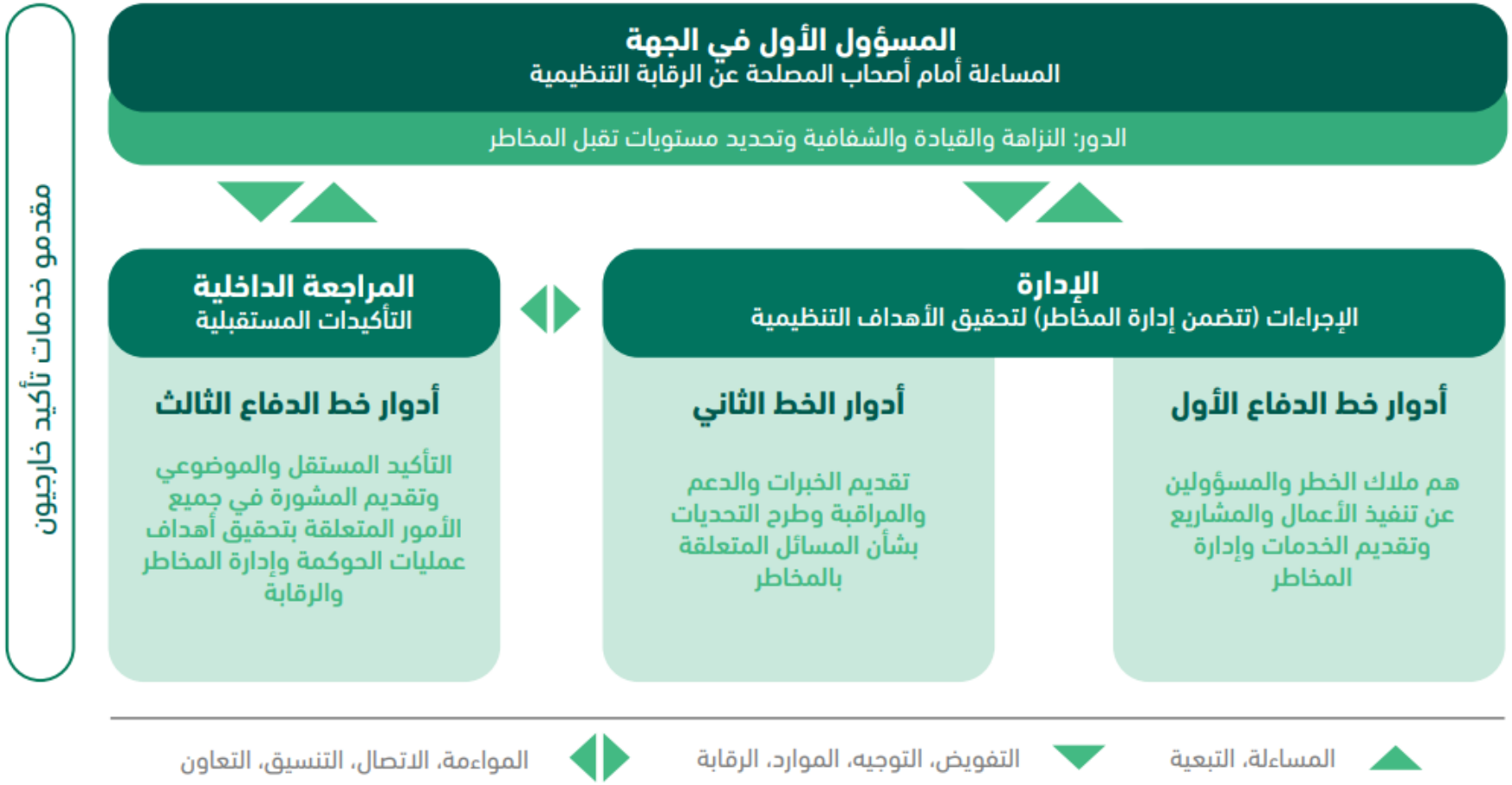
فترة نقاش

من وجهة نظرك
ما هي عناصر إدارة المخاطر؟

عناصر إدارة المخاطر: حوكمة إدارة المخاطر

حوكمة إدارة المخاطر تشمل أصحاب المصلحة الداخليين والخارجيين، على سبيل المثال: الموردين والعملاء والجهات الرقابية، والجهات الحكومية، وكبار التنفيذيين، وأعضاء الإدارة العليا، ولجان الحوكمة، وجميع الموظفين. ولضمان وجود نموذج حوكمة متين وفعال فمن المهم الأ يكون هناك تضارب مصالح في الأدوار والمسؤوليات، وأن ترتبط الأدوار والمسؤوليات بشكل واضح ومباشر بالصلاحيات، وينصح بتبني نموذج خطوط الدفاع الثلاثة المعتمد من معهد المراجعين الداخليين IIA حيث تعتبر الضوابط الداخلية والإدارة التنفيذية هي خط الدفاع الأول، وإدارة المخاطر وإدارة الإلتزام والإدارة القانونية وغيرها من الوظائف الرقابية هي خط الدفاع الثاني، وأخيراً المراجعة الداخلية هي خط الدفاع الثالث الذي يعطي ضمان مستقل عما قبله، وجميعها تملك علاقة متبادلة ومرجعية مباشرة للمسؤول الأول في الجهة. لذلك ينبغي للجهة تطوير الحوكمة المناسبة لإدارة المخاطر أخذاً بالإعتبار أهمية الفصل والإستقلالية لخط الدفاع الثاني وأهمية العلاقة المتبادلة مع الإدارة العليا واللجان المشتركة، وكذلك المرجعية المباشرة للمسؤول الأول في الجهة، والتأكد من أن مسؤولي المخاطر في الجهة يرفعون التوصيات للمسؤول عن إدارة المخاطر الذي يقوم بدوره بمخاطبة اللجان التي تتضمن أعضاء مستقلين قدر الإمكان وبرئاسة المسؤول الأول في الجهة.

عناصر إدارة المخاطر: حوكمة إدارة المخاطر



عصف ذهني

من وجهة نظرك
ما هي عناصر إدارة المخاطر؟

عناصر إدارة المخاطر: الأدوار والمسؤوليات

على الجهة تحديد الأدوار المعنية لإدارة المخاطر وتعيينها للجهات المسؤولة عن تنفيذها، على النحو التالي:

- المسؤول الأول في الجهة
- اللجنة الإشرافية على إدارة المخاطر
- إدارة المخاطر
- وحدات العمل / الفرق التشغيلية
- مسؤولي إدارة المخاطر

عناصر إدارة المخاطر: سياسة إدارة المخاطر

توضح سياسة إدارة المخاطر إلتزام قيادة الجهة المستمر لإدارة المخاطر، وتتضمن السياسة على سبيل المثال: غرض الجهة من إدارة مخاطرها، أهداف إدارة المخاطر ونطاق عملها، الجهات المعنية بإدارة المخاطر وأدوارهم ومسؤولياتهم والأحكام العامة التي يجب إتباعها في أنشطة وإجراءات إدارة المخاطر.

عناصر إدارة المخاطر: مؤشرات أداء إدارة المخاطر

على الجهة متابعة ومراقبة فعالية وكفاية أداء إدارة مخاطرها من خلال تحديد مؤشرات أداء رئيسية تعمل على تزويد قيادة الجهة بمعلومات دورية حول أداء وفعالية أنشطة وممارسات إدارة المخاطر المتبنى في الجهة. تهدف إجراءات تحديد ومراقبة مؤشرات أداء إدارة المخاطر إلى التحسين والتطوير المستمر لإدارة المخاطر ومعرفة مدى قدرة الجهة من تفادي الآثار السلبية للمخاطر وإستغلال الآثار الإيجابية الناتجة من الأحداث والمتغيرات والتي تعرف بالفرص.

عناصر إدارة المخاطر: تصنيف فئات المخاطر

ينبغي على الجهة تصنيف المخاطر إلى فئات حسب طبيعة عملها ونشاطها، مع الأخذ بالإعتبار المؤثرات الداخلية والخارجية، فتصنيف المخاطر يساعد على تحديد مصادر المخاطر التي قد تؤثر على أعمال الجهة لوضع خطط علاج لتخفيف أثرها أو الحد من حدوثها، بعض الأمثلة على فئات المخاطر كما يلي:

- المخاطر الإستراتيجية
- المخاطر المالية
- المخاطر التشغيلية
- مخاطر المشاريع
- مخاطر الأمن السيبراني وتقنية المعلومات
- مخاطر عدم الإلتزام

عناصر إدارة المخاطر: حدود تقبل وتحمل المخاطر

ينبغي أن تكون حدود تقبل وتحمل المخاطر واضحة لمساعدة الجهة على إتخاذ القرارات الصائبة التي تصب في تحقيق أهدافها الإستراتيجية، وتعتبر حدود تقبل وتحمل المخاطر أداة مساعدة لتقييم القرارات الإستراتيجية وتساهم في تحديد المخاطر المصاحبة للفرص الجديدة للجهة. أهم المعايير والممارسات المؤسسية العالية كالآتي:

- COSO 2017: حدود تقبل وتحمل المخاطر من خلال نوع ومقدار الخطر التي تكون الجهة على إستعداد لتقبله على نطاق واسع لتحقيق أهدافها.
- ISO 31000:2018 : ينبغي تحديد مقدار ونوع الخطر المحتمل لتحقيق أهداف الجهة. ومن الضروري وضع معيار لتقييم أهمية المخاطر ودعم عمليات إتخاذ القرارات وأن تكون متوافقة مع إدارة المخاطر ومتناسباً مع غرض ونطاق أنشطة الجهة.

عناصر إدارة المخاطر: حدود تقبل وتحمل المخاطر

بعض الإرشادات التي يفضل أخذها بالإعتبار عند تحديد حدود تقبل وتحمل المخاطر وهي كالآتي:

- ينبغي أن تعكس مفهوم إدارة المخاطر في الجهة ودورها في التأثير على ثقافتها وأنشطاتها
- ينبغي أن تحدد مستويات الأختلاف المقبولة الني تكون الجهة على إستعداد لقبولها لتحقيق أهدافها الإستراتيجية
- ينبغي أن تكون حدود تقبل وتحمل المخاطر واضحة بحيث يمكن تعميمها على نطاق واسع داخل الجهة ورصدها بشكل فعال ومتابعتها بشكل مستمر

عناصر إدارة المخاطر: حدود تقبل وتحمل المخاطر

تتعدد الطرق المتبعة لتحديد حدود تقبل وتحمل المخاطر، ومن أهمها الآتي:

- **العودة إلى الأحداث السابقة:** وهذه الطريقة تُمثل أهم الطرق وأكثرها عملية حيث يتم الرجوع للأحداث السابقة والسمات التاريخية للجهة لتحديد حدود تقبل وتحمل المخاطر والإستعداد للمخاطر المستقبلية
- **تحليل وتقييم المعلومات:** يتم تحليل المعلومات من مصادر مختلفة من خلال إجراء مقابلات مع المدراء وكبار التنفيذيين. إضافة إلى ذلك، يمكن الإعتماد على القوائم المالية والتقارير الداخلية ومعلومات الجهة لتحديد حدود تقبل وتحمل المخاطر للجهة.
- **مراجعة إستراتيجية الجهة وأهدافها:** يتم مراجعة إستراتيجية الجهة وتحليل حدود أهدافها ومؤشرات قياس أدائها لتحديد حدود تقبل وتحمل المخاطر.

عناصر إدارة المخاطر: حدود مؤشرات المخاطر

ينبغي على الجهة تطوير مؤشرات مخاطر رئيسية Key Risk Indicators لقياس أهم وأعلى المخاطر التي تتعرض لها. هذه المؤشرات عبارة عن نظام إنذار مبكر يطلق عندما يتجاوز تعرض الجهة لمستويات المخاطر المقبولة، مما يساعد إدارة المخاطر على مراقبة هذه المخاطر وإتخاذ الإجراءات المبكرة لمبع الأزمات أو التخفيف منها. كما أن مؤشرات المخاطر الرئيسية يجب أن تكون قابلة للقياس بحيث يتم تحديد حدود لكل مؤشر، وفي حال تعدي الحدود ينبغي إبلاغ الجهات المعنية داخل الجهة، كما أن المؤشرات ينبغي الأ تغطي جميع المخاطر التي تواجه الجهة، ولكن يتم التركيز على المؤشرات الأكثر أهمية لإدارة المخاطر.

تتلخص عملية تحديد المؤشرات في الخطوات الآتية:

- تحديد تعريف تفصيلي لأنواع المخاطر التي قد تتعرض لها الجهة حسب طبيعة أعمالها التشغيلية وتوجهاتها الإستراتيجية (تعرف بفئات المخاطر)
- تحديد أفضل المؤشرات القابلة لقياس مدى تعرض الجهة لتلك المخاطر المعرفة
- تحديد مستويات حدود التعرض لفئات المخاطر التي تتمثل على النحو التالي:

عناصر إدارة المخاطر: حدود مؤشرات المخاطر

- اللون **الأخضر** والأصفر تعتبر ضمن حدود تقبل الجهة للمخاطر وتكون مقبولة لحدآ ما، وبناء عليها يتم رفع تقارير وفق المستويات الوظيفية المحددة ضمن إطار إدارة المخاطر.

- اللون **البرتقالي** والأحمر تعتبر مؤشرات تتجاوز حدود تقبل وتحمل الجهة للمخاطر وتكون غير مقبولة، أي يجب على الجهة القيام بمعالجة مسببات تلك التعرضات بشكل فوري لتخفيضها ضمن الحدود المقبولة، ورفع تقارير بناء على المستويات الوظيفية المحددة ضمن إطار إدارة المخاطر.

حدود مؤشرات المخاطر

تصنيف فئات المخاطر	مؤشرات المخاطر الرئيسية	مقبول	مقبول جزئياً	تتجاوز حدود تقبل المخاطر	تتجاوز حدود تحمل المخاطر
المخاطر الاستراتيجية	انخفاض مستوى الناتج المحلي	< *0.1%	< 0.25%	<0.5%	>1%
المخاطر المالية	انخفاض الإيرادات	< 0.2%	<0.5%	<1%	>3%
المخاطر التشغيلية	فشل النظام	أقل من ساعتين	أقل من نصف يوم	أقل من يوم واحد	أكثر من يومين
	معدل دوران مرتفع للموظفين	<5%	<8%	<12%	>15%
مخاطر الأمن السيبراني وتقنية المعلومات	اختراق أمن سيبراني	-	-	نظام واحد حيوي و/ أو داعم للخدمات الحيوية	أكثر من نظام حيوي و/أو داعم للخدمات الحيوية

شكراً لإستماعكم وتفاعلكم

- فترة الأسئلة -