العبيكان الخيرية

سياسة إدارة المخاطر

سياسة إدارة المخاطر

المادة (1): تمهيد

1) مع عدم الإخلال بما جاء في القوانين والأنظمة المعمول بها في المملكة العربية السعودية، ونظام الجمعيات والمؤسسات الأهلية، واللائحة التنفيذية لنظام الجمعيات والمؤسسات الأهلية، ومعايير حوكمة المؤسسات الأهلية، واللائحة الأساسية لمؤسسة عبدالرحمن بن ثنيان العبيكان الخيرية، تأتي هذه السياسة استكمالاً لها، دون أن تحل محلها، وتفسَّر في ضوئها.
2) تنطبق هذه السياسة على جميع العاملين في المؤسسة والمعنيين بإدارة المخاطر المرتبطة بأهداف عملهم.
3) الغرض من إدارة المخاطر هو دعم تحقيق أهداف المؤسسة، وتشجيع الابتكار واستغلال الفرص، وتطوير أساليب اتخاذ مختلف القرارات والتخطيط وتحديد الأولويات، وتحسين الأداء العام للمؤسسة. ولتحقيق ذلك يجب إحداث التكامل بين عمليات إدارة المخاطر ومختلف أنشطة وعمليات المؤسسة بكافة المستويات للحصول على معلومات أفضل تدعم اتخاذ قرارات أفضل تؤدي في النهاية إلى تعزيز الأداء، وعلاوة على ذلك تساعد المؤسسة على:
   أ) التنبؤ بالمخاطر مبكراً أو بشكل أوضح، مما يتيح مزيد من الخيارات لإدارة المخاطر والحد من الانحراف المحتمل في الأداء، والخسائر والأحداث أو حالات الفشل.
   ب) تحديد الفرص الحالية والجديدة والسعي وراء تحقيقها وفقاً لاستراتيجية المؤسسة وقابليتها للمخاطر.
   ج) فهم الانحرافات في الأداء واتخاذ ردود فعل سريعة عليها بمزيد من الاتساق.
   د) وضع رؤية شاملة للمخاطر تتسم بمزيد من التكامل والاتساق وإعداد التقرير بشأنها، مما يسمح للمؤسسة أن تخصص الموارد المحدودة بصورة أفضل.
   ه) تعزيز التعاون الثقة ومشاركة المعلومات في المؤسسة.
4) عملية إدارة المخاطر تبدأ بفهم بيئة عمل المؤسسة الداخلية والخارجية، ومن ثم تحديد المخاطر وتقييم شدتها والاستجابة لها، وتنتهي بالتقاط المعلومات المتعلقة بالمخاطر ومشاركتها في التوقيت المناسب مع كافة الأطراف المعنية كل حسب اختصاصاته ومسؤولياته، وتخلل هذه العملية أنشطة المراجعة وعمليات التعديل.
5) إدارة المخاطر ليست عملية ثابتة، فهي تطبق باستمرار على كامل أنشطة المؤسسة.
6) إدارة المخاطر يجب أن تكون جزء من أي قرار إداري على جميع المستويات الإدارية في المؤسسة.
7) لأغراض هذه السياسة؛ يتمّ تقييم المخاطر من حيث التأثير والاحتمال.

المادة (2): مكونات ومبادئ إدارة المخاطر

يتألف إطار إدارة المخاطر في المؤسسة من خمس مكونات مترابطة فيما بينها، وتتضمن تلك المكونات الخمسة عشرين مبدأً على النحو التالي:

المكون الأول: الحوكمة والثقافة: تحدد الحوكمة الجو العام السائد في المؤسسة فيما يتعلق بإدارة المخاطر، كما تحدد أدوار الرقابة والمسؤولية عنها. وتشمل ثقافة المؤسسة والأخلاقيات والآداب والسلوكيات والقيم المنشودة داخلها فيما يتعلق بالمخاطر.
وتشمل المبادئ المتعلقة بالحوكمة والثقافة ما يلي:

1) **الدور الإشرافي لمجلس الأمناء: يجب أن يكون لدى المؤسسة مجلس أمناء مستقل وموضوعي يتمتع بالخبرة والسلطة الوافيتين للإشراف على المؤسسة وإدارتها أثناء سعيها لتحقيق استراتيجيتها وأهدافها.**
2) **الهيكلية التشغيلية: يجب على المؤسسة إنشاء هيكلية تحدد بوضوح خطوط المسؤولية والمساءلة، وينبغي أن تعمل الهيكلية التنظيمية المصممة تصميماً جيداً على موازنة القوى في المؤسسة وتيسير بيئة عمل سلسة داخلها مع الحفاظ على خطوط تبعية تتسم بالفاعلية.**
3) **الثقافة: يجب على المؤسسة إنشاء ثقافة أخلاقية ومعايير سلوكية تحدد الأفعال المنشودة من قبل جميع العاملين فيها، وينبغي أن يقوم مجلس الأمناء بمراقبة مدى الامتثال لتلك المعايير والثقافة.**
4) **الالتزام بالقيم الأساسية: يجب على المؤسسة تبليغ الثقافة الأخلاقية، والمعايير السلوكية، والقيم الأساسية للمؤسسة بصورة فاعلة إلى جميع العاملين في المؤسسة. ويحدد مجلس الأمناء والإدارة التنفيذية في المؤسسة النهج في أعلى الهرم، ويجب أن يظهروا تمسكهم بالقيم الأساسية للمؤسسة. كما ينبغي إعطاء الأولوية العليا للقيم الأساسية عند اتخاذ جميع القرارات الهامة، مثل القرارات المتعلقة باختيار العاملين في المؤسسة وأعضاء مجلس الأمناء.**
5) **رأس المال البشري: يجب على المؤسسة أن تضع سياسات وممارسات للموارد البشرية تعمل على المحافظة على رأسمالها البشري وتطويره. وتشمل تلك السياسات والممارسات العديد من الجوانب مثل التوظيف والتعيين والتوجيه والتدريب وتقييم الأداء والترقية والتعويضات والإجراءات التأديبية. وتوضح هذه الممارسات مستوى النزاهة والقيم الأخلاقية والكفاءة المتوقعة من جميع العاملين في المؤسسة.**

المكون الثاني: الاستراتيجية وتحديد الأهداف: يشمل التخطيط الاستراتيجي دراسة سياق الأعمال في المؤسسة، وتحديد قابليتها للمخاطرة، ووضع الاستراتيجية التي تتوافق مع درجة الاستعداد لتقبل المخاطر وتدعم رسالة المؤسسة ورؤيتها وقيمها الأساسية. ثم بعد ذلك، يتم تحديد أهداف العمل لوضع الاستراتيجية موضع التنفيذ.
وتشمل المبادئ المتعلقة بالاستراتيجية وتحديد الأهداف ما يلي:

6) **تحليل سياق العمل: يجب على المؤسسة دراسة الآثار المحتملة لسياق العمل على محفظة المخاطر، من خلال فهم سياق العمل عند وضع الاستراتيجية التي تدعم رسالتها**

ورؤيتها وقيمها الأساسية، وملاحظة تأثير سياق العمل على محفظة المخاطر في المؤسسة في ثلاثة مراحل: الأداء في الماضي والحاضر والمستقبل.

7) قابلية المخاطر: يجب على المؤسسة أن تحدد قابليتها للمخاطر وذلك كجزء من عملية التخطيط.

8) الاستراتيجيات البديلة: في ضوء سياق الأعمال وقابلية المؤسسة للمخاطرة، يجب على المؤسسة تقييم الاستراتيجيات البديلة وتأثيراتها المحتملة على المخاطر التي يمكن أن تتعرض لها. حيث يجب أن تتوافق الاستراتيجية التي تم اختيارها مع رسالة المؤسسة ورؤيتها وقيمها الأساسية، بالإضافة إلى قابليتها للمخاطرة.

9) الأهداف: يجب على المؤسسة الاعتماد على استراتيجيتها في تحديد أهداف العمل، ويجب أن تعمل بحيث تيسر أهداف العمل تحقيق الاستراتيجية مع أخذ المخاطر في الاعتبار.

المكون الثالث: الأداء: يشمل تنفيذ إدارة المخاطر على مستوى المؤسسة الخطوات المتمثلة في تحديد المخاطر، وتقييمها، وتحديد أولوياتها، والاستجابة لها، بالإضافة إلى إعداد تصور شامل للمخاطر المحتملة.

وتشمل المبادئ المتعلقة بالأداء ما يلي:

10) تحديد المخاطر: يجب على المؤسسة أن تحدد المخاطر التي تؤثر على تحقيق الاستراتيجية وأهداف العمل.

11) تقييم شدة المخاطر: يجب على المؤسسة أن تقيم شدة المخاطر.

12) ترتيب المخاطر وفقاً لأولوياتها: يجب على المؤسسة أن ترتب المخاطر وفقاً لأولوياتها، والذي يجب أن يكون الأساس لاختيار الاستجابات المناسبة للمخاطر.

13) تنفيذ الاستجابات للمخاطر: يجب على المؤسسة أن تحدد وتختار الاستجابات المناسبة للمخاطر.

14) وضع الرؤية الشاملة للمخاطر: يجب على المؤسسة أن تطور نظرة أوسع نطاقاً (على مستوى المؤسسة) عن المخاطر لتسلط الضوء على مدى شدة المخاطر المختلفة التي تواجهها وأوجه الترابط فيما بينها.

المكون الرابع: المراجعة والتعديل: يجب على المؤسسة أن تقوم بشكلٍ منهجي بمراجعة وتعديل أدائها بما في ذلك ممارسات إدارة المخاطر على مستوى المؤسسة.

وتشمل المبادئ المتعلقة بالمراجعة والتعديل ما يلي:

15) تقييم التغيرات الجوهرية: يجب على المؤسسة أن تقوم بتقييم جميع التغيرات في البيئة الداخلية أو الخارجية وفي سياق العمل والتي يمكن أن تؤثر على استراتيجيتها الحالية أو المستقبلية وعلى أهداف عملها.

16) مراجعة المخاطر والأداء: يجب على المؤسسة أن تقوم باستعراض أداءها والمخاطر التي تواجهها وتأخذها دائما بعين الاعتبار.

17) تحسين إدارة المخاطر: يجب على المؤسسة أن تقوم بالتحسين المستمر على عمليات إدارة المخاطر على مستوى المؤسسة.

المكون الخامس: المعلومات والاتصالات والتقارير: يجب على المؤسسة أن تقوم بصورة منهجية بالتقاط المعلومات المتعلقة بالمخاطر ومشاركتها في التوقيت المناسب مع كافة المعنيين في المؤسسة.

وتشمل المبادئ المتعلقة بالمعلومات والاتصالات والتبليغ ما يلي:

18) الاستفادة من أنظمة المعلومات والتكنولوجيا: يجب على المؤسسة أن تستفيد من أنظمة المعلومات والتكنولوجيا لدعم عمليات إدارة المخاطر على مستوى المؤسسة.

19) مشاركة المعلومات المتعلقة بالمخاطر: يجب على المؤسسة أن تستخدم قنوات ووسائل التواصل المختلفة مع جميع أصحاب المصالح لتدعم إدارة المخاطر فيها.

20) إعداد التقارير حول المخاطر، والبيئة الأخلاقية، والأداء: يجب على المؤسسة أن تعد تقارير عن المخاطر، والبيئة الأخلاقية، والأداء على مستويات متعددة من المؤسسة.

المادة (3): تحديد المخاطر

1) التوجه العام في المؤسسة هو أنه لا يوجد أي مخاطرة يمكن إهمالها.

2) عند تحديد المخاطر للإدارات والأقسام ووحدات العمل في المؤسسة؛ يجب:

أ) إشراك كل من لديه معرفة تفصيلية بكيفية عمل المؤسسة، وأهدافها ورسالتها واستراتيجيتها، وهيكلها التشغيلي، وطبيعة، وحجم أنشطتها، وأعمالها.

ب) أخذ وتحديد جميع العمليات الرئيسية والعمليات الفرعية المهمة التي تساهم في تحقيق أهداف المؤسسة، فضلاً عن تحديد المخاطر التي أجريت على مستوى الإدارات المساندة مثل المحاسبة والمالية والموارد البشرية، إلخ.

3) يجب أن يقوم جميع أعضاء الإدارة التنفيذية ومديري الإدارات في المؤسسة (كل حسب اختصاصه ونطاق عمله) ببذل قصارى جهدهم لتحديد المخاطر الهامة التي تتعرض لها المؤسسة (على المستوى الكلي للمؤسسة، وعلى مستوى إداراتها وأقسامها، وعلى مستوى مختلف مواقع العمل) أو المحتمل أن تتعرض لها في المستقبل، ولتحقيق ذلك يمكن استخدام الآليات التالية لتحديد المخاطر:

أ) عقد اجتماعات العصف الذهني على مختلف المستويات الإدارية في المؤسسة بهدف التفكير في كل أنواع المخاطر المختلفة، وطرح سيناريوهات عامة وأخرى تفصيلية.

ب) إجراء المسوح واستقصاء الرأي بما يناسب كل إدارة/موقع على حدة.

ج) إجراء المقابلات الشخصية وعقد ورش العمل.

د) تحليل تدفق العمليات.

ه) استنتاج الترابط المحتمل بين الأنواع المختلفة للمخاطر.

و) استخلاص مؤشرات قياس المخاطر (Key Risk Indicators).

ز) تتبع الأحداث التي وقعت في الماضي وكان لها تأثير سلبي، وتتبع الخسائر الناتجة عن تلك الأحداث، بهدف التنبؤ بوقوع تلك الأحداث في المستقبل.
ح) استخدام التقييمات التي يقوم بها خبراء من خارج المؤسسة.
ط) نتائج أنشطة المراجعة الداخلية ومراجعة الحسابات الخارجية.

4) بعد الانتهاء من عملية تحديد المخاطر؛ تقوم المؤسسة بتسجيلها في سجل يسمى "سجل المخاطر"، يتضمن وصف طبيعة كل مخاطرة، هذا ويتم تعديل هذا السجل بصفة دورية وفقاً للتغيرات في بيئة عمل المؤسسة الداخلية والخارجية.

المادة (4): تقييم شدة المخاطر

1) لكل مخاطرة على حدة، تقوم المؤسسة بقياسها أو تقديرها من خلال:

أ) تقدير احتمال وقوع المخاطرة. يستخدم في هذا الصدد مقياس من ثلاثة مستويات (يمكن استخدام خمسة مستويات):

- المستوى الأول يعبر عن احتمال مرتفع لوقوع/تحقق المخاطرة (High Probability) ويرمز له بالحرف H.
- المستوى الثاني يعبر عن احتمال متوسط لوقوع/تحقق المخاطرة (Medium Probability) ويرمز له بالرمز M.
- المستوى الثالث يعكس احتمالاً منخفضاً لوقوع/تحقق المخاطرة (Low Probability) ويرمز له بالرمز L.

ويشير كل مستوى من المستويات السابقة إلى طبيعة مختلفة لاحتمال وقوع المخاطرة وتختلف من مخاطرة لأخرى حسب طبيعة كل مخاطرة.

ب) تقدير الأثر المتوقع عند وقوع المخاطرة. يستخدم في هذا الصدد مقياس من ثلاثة مستويات (يمكن استخدام خمسة مستويات):

- المستوى الأول يعبر عن أثر مرتفع عند وقوع/تحقق المخاطرة (High Impact) ويرمز له بالحرف H.
- المستوى الثاني يعبر عن أثر متوسط عند وقوع/تحقق المخاطرة (Medium Impact) ويرمز له بالرمز M.
- المستوى الثالث يعكس أثراً منخفضاً لوقوع/تحقق المخاطرة (Low Impact) ويرمز له بالرمز L.

ويشير كل مستوى من المستويات السابقة إلى طبيعة مختلفة لأثر وقوع المخاطرة وتختلف من مخاطرة لأخرى حسب طبيعة كل مخاطرة.

في الملحق رقم 1 تفاصيل إضافية حول كيفية تقدير احتمال وتقدير الأثر المتوقع عند وقوع المخاطرة باستخدام خمسة مستويات.

2) بناء على ما سبق؛ يتمّ تقييم المخاطر بضرب مستوى التأثير بمستوى الاحتمال.

3) بناء على نتائج قياس المخاطر أو تقديرها يتم تحديد موقعها في مصفوفة المخاطر على النحو التالي:

مستوى التأثير

مستوى الاحتمالية	1	2	3
1	منخفض	منخفض	متوسط
2	منخفض	متوسط	متوسط
3	متوسط	متوسط	مرتفع

4) عند تقييم المخاطر يجب الأخذ بعين الاعتبار ما يلي:

أ) إذا كانت المؤسسة معرضة لمخاطرة يحتمل أن تكون لها تأثير كبير للغاية على عملياتها، فيجب النظر في هذه المخاطرة والتركيز عليها وتقييمها بغض النظر عن مدى احتمالية حدوثها.

ب) يمكن لمخاطرة ذات تأثير منخفض أن تتغير إلى مخاطرة مرتفعة التأثير بسبب العلاقة المحتملة بين المخاطر مما قد يثير حدوث مخاطر أخرى.

ج) يمكن لمخاطرة واحدة منخفضة أن يكون لديها تأثير يؤدي إلى مخاطر أخرى بحيث التأثير التراكمي يصبح مرتفع.

د) معرفة أنه في الحالات النادرة تحدث أحداث غير محتملة يكون أثرها مرتفع جداً، وفي أوقات أخرى لا تحدث أحداث محتملة إطلاقاً.

5) بناء على نتائج قياس المخاطر أو تقديرها وموقعها في مصفوفة المخاطر يتم توزيع المخاطر حسب نوعها على الوظائف الإدارية بالمؤسسة، ويتم تصنيفها.

6) تقوم المؤسسة بتضمين سجل المخاطر نتائج قياس المخاطر أو تقديرها وتوزيعها وتصنيفها، وتقوم بعمل مراجعة للسجل بصفة دورية بهدف تحديثه.

المادة (5): الاستجابة للمخاطر

1) التوجه العام في المؤسسة هو أنه لكل مخاطرة يتم تحديدها يجب تحديد مسؤول عن فاعلية الاستجابة لها، ويجب أن يكون هذا الشخص لديه الصلاحيات والإمكانيات اللازمة لإدارتها، وإذا كان غير قادر على ذلك، فلا بد أن يتم تعيين مسؤول أعلى منه لإدارة المخاطرة. المسؤول عن إدارة المخاطرة يجب أن يوفر ويوثق جميع المعلومات المتعلقة بهذه المخاطرة بالتنسيق مع وحدة إدارة المخاطر.

2) تقوم المؤسسة باختيار الاستجابة المناسبة لكل مخاطرة سلبية (تهديد - Threat) على حدة بهدف تقليل احتمال وقوعها أو تقليل الأثر المتوقع عند وقوعها أو تقليلهما معاً.

3) تقوم المؤسسة باختيار الاستجابة المناسبة لكل مخاطرة إيجابية (فرصة - Opportunity) على حدة بهدف زيادة احتمال وقوعها أو زيادة الأثر المتوقع عند وقوعها أو زيادتهما معاً.
4) اختيار الاستجابة المناسبة مبني على تحليل المنافع المتوقعة منها وتكلفة تطبيقها.
5) تتعدد خيارات الاستجابة للمخاطر السلبية، حيث أنها تشتمل على واحدة أو أكثر من الخيارات التالية:
أ) تجنب المخاطر. يتم تجنب المخاطرة من خلال اتخاذ بعض الإجراءات التي تزيل المخاطرة بشكل جذري، مثل استخدام طرق مختلفة لتنفيذ العمل، أو تكنولوجيا مختلفة، أو إلغاء مشروع معين والتي تجعل المخاطرة غير موجودة.
ب) تقليل المخاطر. يتم من خلال وضع ضوابط رقابية وقائية أو كاشفة أو تصحيحية أو توجيهية أو رادعة بهدف توفير تأكيد معقول بتحقيق أهداف المؤسسة التالية:
- حماية الأصول والحد من وقوع الأخطاء (المقصودة وغير المقصودة) واكتشافها فور وقوعها.
- موثوقية جميع المعلومات والبيانات التي تستخدمها المؤسسة.
- فاعلية وكفاءة الأحداث والعمليات أو الظروف التي تتأثر بها المؤسسة بما في ذلك استخدام الموارد بكفاءة وبشكل ملائم.
- التقيد بالأنظمة والتعليمات والسياسات.

ج) تحويل المخاطر. تقوم عملية تحويل المخاطر على أساس نقل عبء المخاطر من الطرف المعرض لها بصورة مباشرة إلى طرف آخر متخصص في إدارة هذا النوع من المخاطر، نظير مقابل مادي. يمكن تحويل المخاطر من خلال التحوط.
د) توزيع المخاطر. يتم توزيع المخاطر من خلال تنويع الاستثمارات في عدد من الأصول ذات الارتباط السلبي المرتفع.
ه) قبول المخاطر في حال كان أكبر ضرر متوقع إذا ما تحققت سوف تكون أقل من أي بديل لإدارتها.
6) تتعدد خيارات الاستجابة للمخاطر الإيجابية – الفرص - حيث أنها تشتمل على واحدة أو أكثر من الخيارات التالية:
أ) استغلال الفرصة من خلال الاستثمار فيها لزيادة عوائد المؤسسة أو تحسين الأداء.
ب) مشاركة الفرصة مع آخرين في حال عدم وجود إمكانية لاستغلالها بشكل منفرد.
ج) تعزيز احتمالية و/أو أثر الفرصة من خلال ادخال تعديلات في بعض الأنشطة أو العمليات أو الممارسات.
7) عند اختيار الاستجابة المناسبة للمخاطر يؤخذ في الاعتبار كل من التالي:
أ) قابلية المؤسسة للمخاطر.
ب) يمكن أن تؤدي عملية الاستجابة للمخاطر إلى مخاطر جديدة تحتاج إلى إدارة.

ج) التوازن بين أنواع الضوابط الرقابية المختلفة (الوقائية والكاشفة والتصحيحية والتوجيهية والرادعة).
د) النظر في إمكانية مشاركة أصحاب المصلحة.
ه) لا تعتبر خيارات الاستجابة للمخاطر بالضرورة حصرية أو مناسبة في جميع الظروف.
و) إن تبرير الاستجابة للمخاطر أوسع من الاعتبارات الاقتصادية فقط، وينبغي أن يأخذ في الاعتبار جميع التزامات المؤسسة، والالتزامات الطوعية، وآراء أصحاب المصلحة.
ز) أن يتم اختيار خيارات الاستجابة للمخاطر وفقاً لأهداف المؤسسة ومعايير المخاطر والموارد المتاحة.

المادة (6): المحافظة والمراجعة المستمرة لنظام إدارة المخاطر

1) تضمن المؤسسة المحافظة والمراجعة المستمرة لنظام إدارة المخاطر، وأن التغيرات في بيئة عملها الداخلية والخارجية تتم دراستها وأخذها في الاعتبار في عملية إدارة المخاطر.
2) تتحقق المؤسسة من أن عملية إدارة المخاطر والمعلومات التي تم جمعها خلالها كانت ملائمة، وأن التطور المعرفي لدى جميع العاملين لديها أو لصالحها قد ساعد على الوصول إلى قرارات أفضل.
3) تقوم المؤسسة بالتحقق من التوافق مع القوانين والأنظمة والسياسات ذات الصلة بإدارة المخاطر.

المادة (7): المسؤولين عن نظام إدارة المخاطر

1) وحدة إدارة المخاطر[1]: بشكل عام تقوم الوحدة بتقديم المساعدة لجميع العاملين في المؤسسة فيما يتعلق بعملية إدارة المخاطر التي تبدأ بالمكون الثاني في إطار إدارة المخاطر (الاستراتيجية وتحديد الأهداف) وتنتهي بالمكون الرابع (المراجعة والتعديل)، ولعمل ذلك يجب على وحدة إدارة المخاطر عمل التالي بالتنسيق مع جميع إدارات وأقسام المؤسسة:
أ) إعداد خطة عمل سنوية لمتابعة عملية إدارة المخاطر الواردة في سجل المخاطر.
ب) تحديد المخاطر التي تتعرض لها المؤسسة (على المستوى الكلي للمؤسسة، وعلى مستوى إداراتها وأقسامها، وعلى مستوى مختلف مواقع العمل) أو المحتمل أن تتعرض لها في المستقبل.

(1) حيث أنه لا يوجد في الهيكل التنظيمي الحالي في المؤسسة وحدة مستقلة لإدارة المخاطر؛ جميع مسؤوليات الوحدة يتم توزيعها بين وحدة المراجعة الداخلية والإدارة التنفيذية.

ج) تقييم مستمر للمخاطر المتأصلة، وتقييم المخاطر المتبقية بناء على نتائج تقييم فاعلية الاستجابات المحددة والمعتمدة لها.
د) توثيق جميع المعلومات المتعلقة بالمخاطر، وتحديث سجل المخاطر بانتظام.
ه) تقديم الارشاد والتوجيه لجميع العاملين فيما يتعلق بإدارة المخاطر.
و) تنظيم لقاءات وملتقيات وغيرها من الآليات التي يتم فيها مشاركة المعلومات حول المخاطر.
ز) إعداد تقارير دورية ترفع للمدير التنفيذي وللجنة المراجعة بنتائج أعمال وأنشطة الوحدة.

2) العاملون: جميع العاملين معنيون في نجاح نظام إدارة المخاطر في المؤسسة، وجميعهم لهم دور في إدارة المخاطر كل حسب اختصاصه ونطاق عمله. ويجب على جميع العاملين:
أ) في حال معرفة أي مخاطرة جديدة (غير معروفة سابقاً) في نطاق عملهم واختصاصاتهم، المشاركة بإدلاء المعلومات حول هذه المخاطرة للمدير المباشر لتقدير الحاجة إلى تضمينها في سجل المخاطر وتحديد الاستجابة المناسبة لها.
ب) الإبلاغ فوراً عن كل الحوادث والحوادث الوشيكة بهدف مراجعة تقييم مخاطر تكرار حدوثها مرة أخرى وتقييم ملائمة الاستجابات الخاصة بالوقاية منها أو الخاصة بالكشف عنها إن لزم الأمر.
ج) التعاون مع جميع العاملين في وحدة إدارة المخاطر[1] ووحدة إدارة المراجعة الداخلية، وتوفير كافة المعلومات التي يحتاجونها في سبيل تنفيذ أعمالهم وأنشطتهم.

3) المديرون: جميع مديري الأقسام والإدارات في المؤسسة مسؤولون عن التأكد من أن جميع العاملين معهم على دراية بأحدث المعلومات حول إدارة المخاطر، وأن يقوموا بتوصيل المعلومات حول المخاطر المعروفة لديهم لموظفيهم، ليتم توضيحها وعنونتها عند تحقيق الأهداف.

4) المدير التنفيذي: بشكل عام هو المسؤول الأول عن تطبيق سياسة ونظام إدارة المخاطر في المؤسسة، ومتابعة المخاطر الاستراتيجية والتشغيلية والمالية والامتثال التي تتعرض أو قد تتعرض لها المؤسسة والتي تم تحديدها عن طريق مديري الإدارات في المؤسسة. يجب على المدير التنفيذي غرس مزيد من الشفافية والوعي بالمخاطر في جميع أنشطة المؤسسة من خلال اتخاذ الإجراءات التالية:
أ) وضع تصور عام عن المخاطر التي قد تواجه المؤسسة وإنشاء بيئة ملمة بثقافة الحد من المخاطر على مستوى المؤسسة، وطرحها بشفافية مع مجلس الأمناء وغيرهم من أصحاب المصالح.

(1) في الهيكل التنظيمي الحالي في المؤسسة لا يوجد وحدة لإدارة المخاطر مستقلة عن الإدارة التنفيذية للمؤسسة.

ب) الحرص على الالتزام بمستوى المخاطر المعتمد من مجلس الأمناء.
ج) مساعدة جميع العاملين على التكيف مع بيئة العمل الداخلية والخارجية.
د) تشجيع كافة العاملين في المؤسسة على تصعيد الموضوعات والمخاوف دون أن يخشوا العقوبة.
ه) توضيح القواعد والمسؤوليات والتواصل بشأنيها بهدف تحقيق الاستراتيجية وأهداف العمل، بما في ذلك مسؤولية إدارة المخاطر.
و) المواءمة بين القيم الأساسية والسلوكيات واتخاذ مختلف القرارات وبين نماذج الحوافز والمكافآت.
ز) تفعيل المساءلة في جميع المستويات الإدارية والالتزام بها.

5) يقوم المدير التنفيذي بتقديم تقرير دوري لمجلس الأمناء يحتوي على معلومات عن الظروف العامة لنظام إدارة المخاطر، وعن أي مخاطر ناشئة وجوهرية تتطلب عمل استجابة مناسبة لها.
6) المراجعة الداخلية: دراسة وتقييم نظم إدارة المخاطر والرقابة الداخلية في المؤسسة، والتركيز على المخاطر الهامة، ومراجعة عمليات إدارة المخاطر داخل المؤسسة، والتأكد من فاعلية الاستجابات المناسبة، وتقديم توصيات لتطوير الأداء في المؤسسة وتحسين فاعلية وكفاءة نظم الرقابة الداخلية وإدارة المخاطر.
7) لجنة المراجعة: تقوم اللجنة على أساس منتظم بالاجتماع الدوري مع مدير وحدة المراجعة الداخلية ومدير وحدة إدارة المخاطر بهدف مراجعة ومتابعة الأمور التالية ومن ثم رفع تقارير دورية بالنتائج لمجلس الأمناء:
أ) طبيعية المخاطر (المقبولة وغير المقبولة) التي تواجهها المؤسسة.
ب) قدرة المؤسسة على تحمل الخسائر المرتبطة بالمخاطر السلبية (التهديدات) أو إدارة تلك المخاطر.
ج) تكلفة المحافظة على نظام شامل لإدارة المخاطر والمنافع المرتبطة به.
د) هيكل وتنظيم نظام إدارة المخاطر بالمؤسسة.
8) مجلس الأمناء: الدور الأساسي لمجلس الأمناء هو الرقابة على نظام إدارة المخاطر ككل. وبشكل خاص يجب على مجلس الأمناء:
أ) في حالة استلام معلومات تفيد بوجود عيوب وقصور في النظام؛ القيام بالتواصل مع الإدارة التنفيذية في المؤسسة لعمل اللازم، والتواصل مع لجنة المراجعة لمتابعة الأمر.
ب) وضع نظم سليمة لإدارة المخاطر والرقابة الداخلية ومراجعتها وتوجيهها بناءً على فهم وتحليل طبيعة وحجم المخاطر التي تواجه أنشطة المؤسسة للحد منها أكبر قدر مستطاع، فضلاً عن تعزيز السلوك المهني والقيم الأخلاقية ووضع سياسات وآليات بشأن الحد من حالات تعارض المصالح وأساليب معالجتها والتعامل معها.

ج) تحديد قابلية المؤسسة للمخاطر.
د) اعتماد سياسة إدارة المخاطر بالمؤسسة وتحديد المقاييس المعينة لتطويرها بشكل منتظم.

9) باقي أصحاب المصالح:
أ) أصحاب المصالح لديهم دور مهم في إدارة المخاطر من خلال التواصل مع المعنيين في المؤسسة في حال وجد لديهم أي ملاحظات أو اقتراحات أو معلومات يرون أهمية أخذها في الاعتبار.
ب) يجب أن يتم بشكل دوري الحصول على رأي واقتراحات أصحاب المصالح عن نظام إدارة المخاطر في المؤسسة من خلال عمل مسوحات.

المادة (8): الإفصاح عن المعلومات المتعلقة بإدارة المخاطر

تفصح الإدارة التنفيذية في المؤسسة في تقرير دوري لمجلس الأمناء (يفضل أن يكون سنوي) عن المعلومات الواردة أدناه:

1) هيكل تحديد مسؤولية كل وظائف إدارة المخاطر.
2) تحليل عن أبرز المخاطر التي تواجه المؤسسة.
3) أبرز عمليات الاستجابة للمخاطر وطرق إدارة المخاطر.
4) التغيرات التي تحدث لنظام إدارة المخاطر بالمؤسسة وأسبابها.

المادة (9): اعتماد ونشر وتنفيذ ومراجعة السياسة

1) تُعتمد هذه السياسة وأي تعديل لاحق عليها من مجلس الأمناء، ويتم العمل بها من تاريخ الاعتماد.
2) يتم الرجوع للجنة المراجعة عند الحاجة لتفسير أي من المواد التي وردت في هذه السياسة.
3) يقوم المدير التنفيذي بعمل مراجعة دورية لهذه السياسة (بحد أدنى مرة واحدة كل ثلاث سنوات) وكلما دعت الضرورة، وذلك لضمان تماشيها مع القوانين والأنظمة المعمول بها في المملكة العربية السعودية، ونظام الجمعيات والمؤسسات الأهلية، واللائحة التنفيذية لنظام الجمعيات والمؤسسات الأهلية، ومعايير حوكمة المؤسسات الأهلية، واللائحة الأساسية للمؤسسة، ومن ثم يقوم برفع تقرير بنتائج المراجعة إلى مجلس الأمناء.
4) يبلغ بهذه السياسة جميع أعضاء مجلس الأمناء ولجنة المراجعة والمدير التنفيذي بالإضافة إلى جميع العاملين المعنيين في المؤسسة، وينشر ملخصاً لها على موقع المؤسسة الإلكتروني.

ملحق رقم 1

كيفية تقدير احتمال وتقدير الأثر المتوقع عند وقوع المخاطرة باستخدام خمسة مستويات

أولاً: تقدير احتمال وقوع المخاطرة

المستوى	احتمالية الحدوث	الوصف
1	من غير المرجح / مستبعد (احتمال ضعيف جداً)	• نادرة للغاية في الأشهر الـ 24 المقبلة • قد تحدث فقط في الظروف الاستثنائية • احتمالية الحدوث أقل من ##% خلال السنة القادمة
2	نادر / غير مستبعد (احتمال ضعيف)	• من غير المحتمل أن يحدث في غضون 24 شهر • قد تحدث فقط في ظروف خاصة • احتمالية الحدوث من ##% إلى ##% خلال السنة القادمة
3	ممكن (احتمال متوسط)	• إمكانية حدوث في الأشهر الـ 24 شهراً المقبلة • قد تحدث أحياناً • احتمالية الحدوث من ##% إلى ##% خلال السنة القادمة
4	متكرر / مرجح (احتمال كبير)	• إمكانية حدوث في الأشهر الـ 12 شهراً المقبلة • قد تحدث من حين لآخر • احتمالية الحدوث من ##% إلى ##% خلال السنة القادمة
5	تقريباً متأكد / مؤكد (احتمال كبير جداً)	• تكرار الحدوث خلال الـ 12 شهراً القادمة • قد تحدث بشكل متواتر • احتمالية الحدوث أكثر من ##% خلال السنة القادمة

ثانياً: تقدير الأثر المتوقع عند وقوع المخاطرة[1]

المستوى	الأثر/التأثير	طبيعة ومدى التأثير
1	غير جوهري (أثر غير ملموس)	• لا يوجد تأثير على أداء الأعمال • لا يؤدي إلى انقطاع عن العمل • لا يوجد تأثير على السمعة • أقل من ### ريال سعودي • انحراف أقل من ##% في الموازنة المعتمدة • وجود مؤشرات محتملة على أن الأنظمة الحيوية و / أو الداعمة للخدمات الحيوية هي هدف للهجوم أو الانتهاكات المهمة لسياسة أمن المعلومات • تأثير محدود المستوى على أنشطة وأنظمة المؤسسة غير الحرجة، مع تأثير ضئيل على مؤشرات الأداء الاستراتيجية (مثال مؤشر أداء استراتيجي واحد)
2	منخفض (أثر صغير)	• يمكن استيعاب العواقب في ظل ظروف التشغيل العادية • تأثير محتمل على أداء الأعمال • انقطاع عن العمل يحل خلال اليوم • التأثير المحتمل على السمعة • من ### إلى ### ريال سعودي • انحراف أقل من ##% إلى ##% في الموازنة المعتمدة • وجود مؤشرات جادة على أن الأنظمة الحيوية و / أو الداعمة للخدمات الحيوية هي هدف للهجوم أو الانتهاكات المهمة لسياسة أمن المعلومات • تأثير منخفض على الوظائف الداخلية والأنظمة غير الحرجة، مع تأثير منخفض على مؤشرات الأداء الاستراتيجية (مثال ثلاث مؤشرات أداء استراتيجية)
3	معتدل (أثر متوسط)	• هناك بعض التأثير على السمعة • سوف يتأثر أداء الأعمال وثقة الجمهور وأصحاب المصلحة • انقطاع عن العمل لمدة يوم • من ### إلى ### ريال سعودي

المستوى	الأثر/التأثير	طبيعة ومدى التأثير
		• انحراف أقل من ##% إلى ##% في الموازنة المعتمدة • وجود محاولات هجوم على الأنظمة الحيوية و / أو الداعمة للخدمات الحيوية بهدف تعطيلها أو تسريب أو المعلومات أو العبث بها • تعطل جزئي للعمليات والأنظمة الغير حرجة، مع انحراف متوسط عن مستويات الأداء الاستراتيجية المستهدفة (مثال: خمس مؤشرات أداء استراتيجية) • استلام تنبيه من الجهات الحكومية المختصة
4	مرتفع (أثر كبير)	• سيتأثر أداء العمل على المدى القصير • انقطاع عن العمل لعدة أيام • تتأثر السمعة على المدى القصير • سوف تتطلب الأحداث والمشاكل اهتمام الإدارة التنفيذية ومجلس الإدارة بالمؤسسة • من ### إلى ### ريال سعودي • انحراف أقل من ##% إلى ##% في الموازنة المعتمدة • وقوع هجوم على الأنظمة الحيوية و / أو الداعمة للخدمات الحيوية وحدوث تأثير محدود على الخدمات، سرية البيانات ودقتها • تعطل تشغيلي أو تقني جزئي لواحد أو أكثر من عمليات أو أنظمة المؤسسة الحرجة، مع تأثير مرتفع على مؤشرات الأداء الاستراتيجية توبيخ غير علني من الجهات الحكومية المختصة
5	مرتفع جداً (أثر كارثي)	• تدني خطير في السمعة • تدهور في الأمور التشغيلية • انقطاع عن العمل لأجل غير معلوم • سوف تتطلب الأحداث والمشاكل اهتمام معزز من قبل الإدارة التنفيذية ومجلس الإدارة بالمؤسسة • أكثر من ### ريال سعودي • انحراف أكثر من ##% في الموازنة المعتمدة

المستوى	الأثر/التأثير	طبيعة ومدى التأثير
		• وقوع هجوم على الأنظمة الحيوية و / أو الداعمة للخدمات الحيوية وحدوث تأثير مدمر على الخدمات، سرية البيانات ودقتها • تعطل تشغيلي أو تقني كامل لواحد أو أكثر من عمليات أو أنظمة المؤسسة الحرجة، مع تأثير عالي على مؤشرات الأداء الاستراتيجية (مثال: عشر مؤشرات أداء استراتيجية أو أكثر) • توبيخ علني من الجهات الحكومية المختصة

ثالثاً: مفاتيح تقييم المخاطر

من 1 إلى 2	منخفض (مخاطر منخفضة)	تعتبر مخاطر روتينية، ويكتفى بعمل الاستجابات الموجودة ضمن سياسات وإجراءات العمل المعتمدة
من 3 إلى 7	متوسط (مخاطر متوسطة)	تعتبر مخاطر مقبولة، وتحتاج متابعة دورية من المسؤول عنها حتى تبقى ضمن المستويات المقبولة
من 8 إلى 14	كبير (مخاطر كبيرة)	تعتبر مخاطر كبيرة وتحتاج متابعة مستمرة من الإدارات المعنية، ويجب عمل الاستجابات المناسبة وتقييمها دورياً
من 15 إلى 25	عالي (مخاطر بليغة)	تعتبر مخاطر غير مقبولة وتحتاج متابعة مستمرة من أعلى المستويات الإدارية في المؤسسة، ويجب عمل الاستجابات المناسبة في أسرع وقت وتخصيص موازنة خاصة بها

رابعاً: تحديد موقع المخاطر في مصفوفة المخاطر

		الأثر/التأثير				
		غير جوهري	منخفض	معتدل	مرتفع	مرتفع جداً
الاحتمالية	من غير المرجح	منخفض	منخفض	متوسط	متوسط	متوسط
	نادر	منخفض	متوسط	متوسط	كبير	كبير
	ممكن	متوسط	متوسط	كبير	كبير	عالي
	متكرر	متوسط	كبير	كبير	عالي	عالي
	تقريباً متأكد	متوسط	كبير	عالي	عالي	عالي