إدارة مخاطر أمن المعلومات

م . عبدالله آل عائض

م. عبدالله عمير آل عائض

ماجستير في الأمن السيبراني
بكالوريوس هندسة حاسب
مدير إدارة المخاطر و الالتزام بأحد المنظمات الشبه حكومية
خبرة تزيد عن 7 سنوات في مجال الأمن السيبراني (GRC)

LinkedIn : http://linkedin.com/in/eng-abdallah-o-alayed-276b66140

Email : aom0885@gmail.com

Mob. :٠٥٠٨٦٨٠٨٨٥

المحتوى

- **مقدمة عن إدارة المخاطر.**
- **مفهوم المخاطر.**
- **مفهوم إدارة المخاطر.**
- **هيكل وتنظيم إدارة المخاطر.**
  - سياسة إدارة المخاطر.
  - دور الإدارة العليا.
  - دور وحدات العمل.
  - دور وظيفة إدارة المخاطر.
  - دور المراجع الداخلي.
  - الموارد والتطبيق.
- **خطوات إدارة المخاطر.**
  - التخطيط.
  - التعرف على المخاطر وتحديدها.
  - تحليل المخاطر.
  - وصف المخاطر.
  - تقدير المخاطر.
  - تقييم المخاطر.
  - إعداد تقارير المخاطر والاتصالات.
  - معالجة المخاطر.
  - مراقبة ومراجعة عمليات إدارة المخاطر.
- **محددات (معوقات) إدارة المخاطر.**

مقدمة

- إن إدارة المخاطر التقليدية تركز على المخاطر الناتجة عن أسباب مادية أو قانونية (مثال: الكوارث الطبيعية أو الحرائق, الحوادث, الموت والدعاوى القضائية) ومن جهة أخرى فإن إدارة المخاطر المالية تركز على تلك المخاطر التي يمكن إدارتها باستخدام أدوات المقايضة المالية.
- إدارة المخاطر ليست وسيلة محصورة على المؤسسات والمنظمات العامة فقط، ولكنها أيضاً لكل الأنشطة طويلة وقصيرة الأمد. ويجب النظر للفوائد والفرص من إدارة المخاطر في علاقتها بأطراف المصلحة المختلفة المتأثرة وليس فقط في علاقتها بنشاط المنظمة.
- بغض النظر عن نوع إدارة المخاطر, فإن جميع المنظمات الكبرى وكذلك المجموعات والمنظمات الصغرى لديها فريق مختص بإدارة المخاطر.

المخاطر

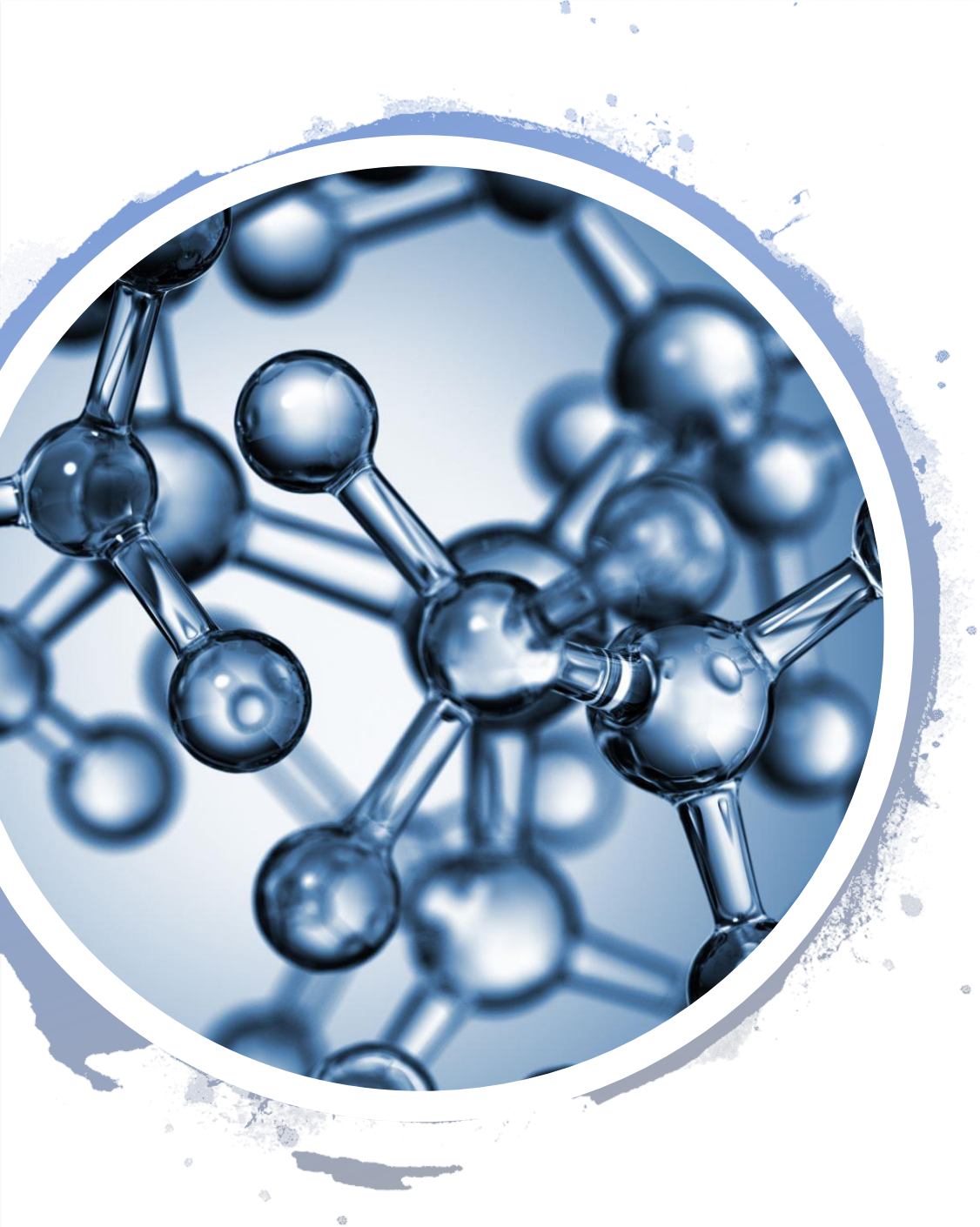
يمكن تعريف المخاطر بأنها مزيج مركب من احتمال تحقق الحدث ونتائجه.

المخاطر أيضا هى عبارة عن ربط بين احتمال وقوع حدث والآثار المترتبة على حدوثه.

يمكن أن تنتج المخاطر التي تواجه أي منظمة وأنشطتها من عوامل خارجية وداخلية. ويمكن تقسيمها أكثر إلى أنواع من الأخطار مثل إستراتيجية ، مالية ، تشغيلية ، بيئية ، أمنية ، سلامة ... الخ.

يتم الإشارة بازدياد إلى إدارة المخاطر على أساس ارتباطها بالجوانب الإيجابية والسلبية للخطر،

ولذلك يأخذ بعين الاعتبار المخاطر من حيث الجانبين السلبي والإيجابي.



تصنيف أنشطة المنظمة

- إستراتيجية
- تشغيلية
- مالية
- الإدارة المعرفية
- التوافق مع القوانين

إدارة المخاطر

التركيز الأساسي لإدارة المخاطر الجيدة هو التعرف على المخاطر ومعالجتها

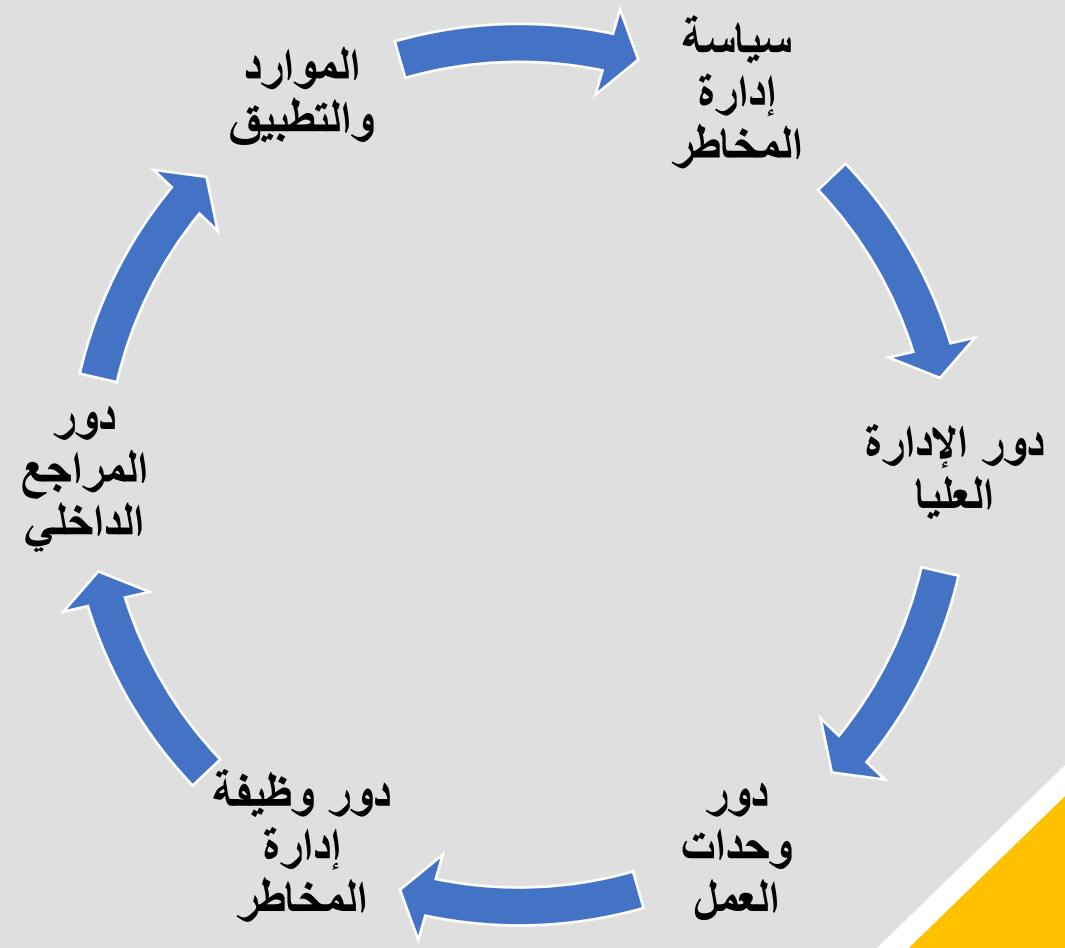
هي الإجراءات التي تتبعها المنظمات بشكل منظم لمواجهة الأخطار المصاحبة لأنشطتها، بهدف تحقيق المزايا المستدامة من كل نشاط

هي جزء أساسي في الإدارة الإستراتيجية لأي منظمة.

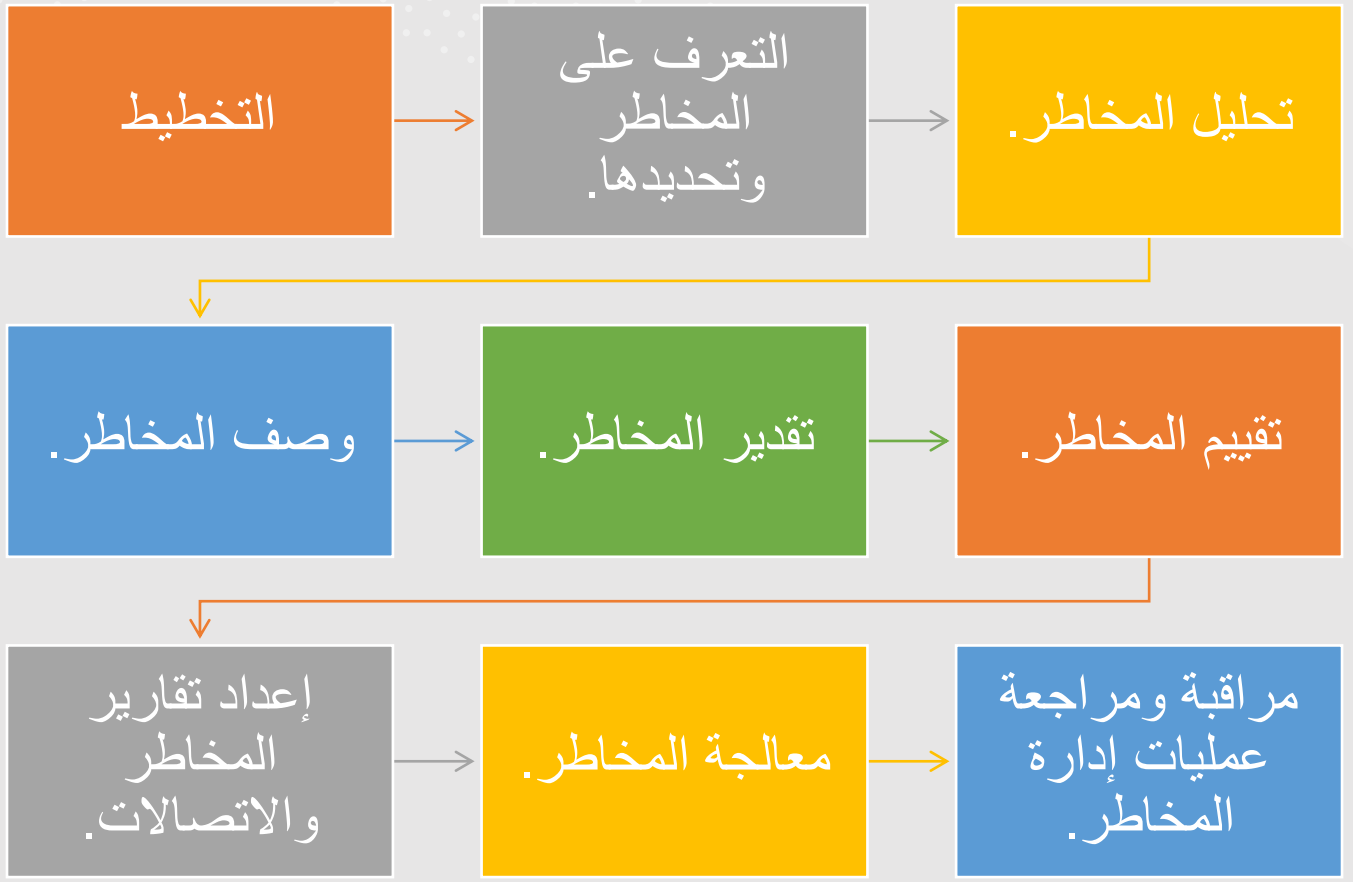
أنشطة إدارة المخاطر يجب أن تكون مستمرة ودائمة التطور وترتبط بإستراتيجية المنظمة وكيفية تطبيق تلك الإستراتيجية. ويجب أن تتعامل بطريقة منهجية مع جميع الأخطار التي تحيط أنشطة المنظمة في الماضي والحاضر وفي المستقبل على وجه الخصوص.

إدارة المخاطر تساعد علي فهم الجوانب الإيجابيه والسلبية المحتملة لكل العوامل التي قد تؤثر علي المنظمة، فهي تزيد من احتمال النجاح وتخفض كلا من احتمال الفشل وعدم التأكد من تحقيق الأهداف العامة للمنظمة .

هيكل وتنظيم إدارة المخاطر



خطوات عملية إدارة المخاطر



التعرف على المخاطر

- يتم التعرف على المخاطر عن طريق:
  - **التحديد المعتمد على الأهداف**
  - **التحديد المعتمد على السيناريو**
  - **التحديد المعتمد على التصنيف**
  - **مراجعة المخاطر الشائعة**

تحديد المخاطر

- التعرف على المخاطر ذات الأهمية.
- يمكن أن يبدأ التعرف إلى المخاطر من مصدر المشاكل أو المشكلة بحد ذاتها.
- عندما تعرف المشكلة أو مصدرها فإن الحوادث التي تنتج عن هذا المصدر أو تلك التي قد تقود إلى مشكلة يمكن البحث فيها.

تحليل المخاطر

تحديد تعرض المنظمة لعدم التأكد يتطلب معرفة جوهرية بالمنظمة والسوق التي تشارك فيه، والبيئة القانونية والاجتماعية والسياسية والثقافية التي تتواجد ضمنها، ويتطلب كذلك الفهم السليم لأهداف المنظمة الإستراتيجية والتشغيلية، ويشمل ذلك العوامل الحيوية لضمان نجاح المنظمة والفرص والتهديدات المرتبطة بتحقيق تلك الأهداف.

وصف المخاطر

- يهدف وصف المخاطر إلى عرض الأخطار التي تم تعريفها بأسلوب منهجي، (مثلا باستخدام جدول) ويمكن استخدام جدول منفصل لوصف المخاطر لتسهيل عملية وصف وفحص الأخطار، واستخدام أسلوب مصمم بطريقة جيدة ضروري للتأكد من إجراءات تعريف ووصف وفحص الأخطار بطريقة شاملة.
- إذا أخذنا في الحسبان نتائج واحتمالات كل خطر متضمنها الجدول، يصبح من الممكن إعطاء الأولوية للأخطار الرئيسية والتي تحتاج إلى التحليل بطريقة أكثر تفصيلا.
- يمكن تصنيف الأخطار التي تم تعريفها والمصاحبة للأنشطة ولاتخاذ القرارات إلى إستراتيجية، ومشروع (تكتيكية وتشغيلية).
- من الضروري دمج إدارة المخاطر ضمن مرحلة التصور للمشروعات وخلال مراحل تنفيذ مشروع معين .

جدول وصف المخاطر

المخاطر	مجال المخاطر	طبيعة المخاطر	توقعات الإدارة العليا	التقدير الكمي للمخاطر	التحمل (الميل للخطر)	أساليب المعالجة والتحكم في المخاطر	الأجراء المتوقع للتطوير	تطوير الإستراتيجية والسياسة
أسم الخطر	الوصف غير الكمي للأحداث، وحجمها، ونوعها، وعددها وعدم استقلاليتها	مثال : إستراتيجي، تشغيلي، مالي، معرفي أو قانوني ..	(أو أصحاب المصلحة وتوقعاتهم)	(الأهمية، والاحتمال)	توقعات لخسارة والتأثير المالي للخطر، (احتمال وحجم الخسائر على العوائد المتوقعة)	الوسائل الأولية التي يتم بواسطتها أداره المخاطر حالياً، ومستويات الثقة في أساليب التحكم المطبق	توصيات لتخفيض المخاطر	وتحديد الإدارة المسئولة عن تطوير الإستراتيجية والسياسة

تقدير المخاطر

- يمكن تقدير المخاطر بأسلوب كمي أو شبه كمي أو نوعي من حيث احتمال التحقق والنتائج المحتملة.
- النتائج من حيث التهديدات أو فرص النجاح قد تكون مرتفعة أو متوسطة أو منخفضة.
- قد تكون الاحتمالات مرتفعة أو متوسطة أو منخفضة إلا أنها تتطلب تعريفات مختلفة من حيث التهديدات وفرص النجاح.

خصائص تقدير المخاطر

يمكن استخدام نتائج عملية تحليل المخاطر لإعداد وصف لخصائص المخاطر والتي ستعطي بدورها تصنيف حسب الأهمية النسبية لكل خطر كما ستوفر أداة لترتيب مجهودات معالجة المخاطر حسب أولوياتها، وسيؤدي ذلك إلى ترتيب كل خطر تم تعريفه بحيث يعطي صورة لأهميته النسبية.

يسمح هذا الأسلوب برسم المخاطر على منطقة النشاط التي تتأثر به، وكذلك وصف إجراءات التحكم المطبقة، وتحديد المجالات التي قد يحتاج فيها زيادة استثمارات التحكم في المخاطر أو تخفيضها أو أعاده توزيعها.

تعريف المسئولية يساعد على التعرف على ملكية المخاطر، وتحديد أفضل الموارد الإدارية الواجب تخصيصها.

تقييم المخاطر

- يشمل تقييم المخاطر الأنشطة الرئيسية التالية:
  - تحديد الأصول وتصنيفها ؛
  - تحديد متطلبات العمل القانونية ذات الصلة بالأصول المحددة ؛
  - تقييم الأصول المحددة ، مع الأخذ في الاعتبار المتطلبات
  - تحديد التهديدات ونقاط الضعف للأصول المحددة ؛
  - تقييم احتمالية حدوث التهديدات ونقاط الضعف وتأثيرها ؛
  - حساب / قياس المخاطر.

تقييم المخاطر

- **تحديد الأصول وتصنيفها إلى مجموعات :**
  - المعدات
  - البرمجيات
  - الأشخاص
  - المعلومات
  - المواقع

تقييم المخاطر

- تحديد متطلبات العمل القانونية ذات الصلة بالأصول المحددة بناء على :
  - الأمن
  - حوكمة الشركات
  - التجارة الإلكترونية
  - سرقة الهوية و حماية البيانات
  - حماية الملكية الفكرية
  - قطاع الصناعة

تقييم المخاطر

- تقييم الأصول من خال عمل (BIA) و مدى تأثيرها على :
  - إفشاء المعلومات _ فقدان السرية
  - التعديل الغير مصرح به _ فقدان النزاهة
  - عدم التوافر _ فقدان التوافر

- ممكن أن تؤثر هذه الحوادث بشكل مباشر أو غير مباشر على المنظمة من خلال :
  - انقطاع الخدمة
  - فقدان البيانات التنظيمية
  - الإضرار بسمعة المنظمة
  - آثار مالية

تقييم المخاطر

- **تحديد التهديدات ونقاط الضعف**
  - يتم تصنيف التهديدات على النحو التالي :
    - متعمد
    - عرضي
    - بيئي / طبيعي
  - نقاط الضعف قد تكون مرتبطة بأحد المجالات التالية :
    - بالمنظمة
    - العمليات و الإجراءات
    - الأجهزة أو البرامج
    - الأمن الفيزيائي
    - الاعتماد على الأطراف الخارجية

تقييم المخاطر

- تقييم التهديدات (حسب المنهجية المستخدمة في المنظمة) :
  - من أجل حساب القيمة الفعلية للتهديد ، يجب تحديد وتقييم عوامل التهديد التالية:
  - **تأثير:** التأثير على الأصل بالتعرض للتهديد المذكور.
  - **احتمالا:** احتمال تأثير هذا التهديد على الأصل.
  - يجب أن يكون للتأثير قيمة أكبر من احتمال التهديد.

تقييم المخاطر

- تقييم الضعف (حسب المنهجية المستخدمة في المنظمة) :
  - من أجل حساب القيمة الفعلية للثغرة ، يجب تحديد ضوابط مطبقة يتم من خلالها تقييم نقاط الضعف

تقييم المخاطر

- حساب / قياس المخاطر :
- يتم حساب الخطر عن طريق المعادلة التالية :

قيمة مجموعة الأصول * قيمة التهديد * قيمة الضعف = الخطر

معالجة المخاطر

- تعتبر معالجة المخاطر بمثابة عملية اختيار وتطبيق إجراءات بغرض التغيير في المخاطر. وتتضمن معالجة المخاطر التخفيض (التحكم في المخاطر) كأحد أهم عناصرها، وتمتد أكثر إلى تجنب المخاطر، وتمويل المخاطر.....الخ (على سبيل المثال).
- يجب أن يقدم أي نظام لمعالجة المخاطر (كحد أدنى) ما يلي:
  - التشغيل الفعال والكفء للمنظمة.
  - الرقابة الداخلية الفعالة.
  - أتباع القوانين والتشريعات.
- ترتبط عملية فعالية تكلفة إجراءات التحكم في المخاطر بتكلفة تطبيق تلك الإجراءات بالمقارنة بالمزايا المتوقعة من تخفيض المخاطر.

طرق التعامل مع المخاطر

النقل

- وهي وسائل تساعد على قبول الخطر من قبل طرف آخر وعادة ما تكون عن طريق العقود أو الوقاية المالية. التأمين هو مثال على نقل الخطر عن طريق العقود. وقد يتضمن العقد صيغة تضمن نقل الخطر إلى جهة أخرى دون الالتزام بدفع أقساط التأمين.

التجنب

- وتعني محاولة تجنب النشاطات التي تؤدي إلى حدوث خطر ما. ومثال على ذلك عدم شراء ملكية ما أو الدخول في عمل ما لتجنب تحمل المسؤولية القانونية. إن التجنب يبدو حلا لجميع المخاطر ولكنه في الوقت ذاته قد يؤدي إلى الحرمان من الفوائد والأرباح التي كان من الممكن الحصول عليها من النشاط الذي تم تجنبه.

التقليص

- وتشمل طرق للتقليل من حدة الخسائر الناتجة. ومثال على ذلك شركات تطوير البرمجيات التي تتبع منهجيات للتقليل من المخاطر وذلك عن طريق تطوير البرامج بشكل تدريجي.

القبول

- وتعني قبول الخسائر عند حدوثها. إن هذه الطريقة تعتبر إستراتيجية مقبولة في حالة المخاطر الصغيرة والتي تكون فيها تكلفة التأمين ضد الخطر على مدى الزمن أكبر من إجمالي الخسائر. كل المخاطر التي لا يمكن تجنبها أو نقلها يجب القبول بها. وتعد الحرب أفضل مثال على ذلك حيث لا يمكن التأمين على الممتلكات ضد الحرب.

إعداد تقارير المخاطر والاتصالات (التقرير الداخلي)

تحتاج مستويات مختلفة داخل المنظمة إلى معلومات متنوعة عن عملية إدارة المخاطر :

- الإدارة العليا (مجلس الإدارة)
- وحدات العمل
- الأفراد

إعداد تقارير المخاطر والاتصالات (التقرير الخارجي)

تحتاج المنظمة إلى تقديم تقرير إلى أصحاب المصلحة بشكل منتظم موضحا سياسات إدارة المخاطر ومدى الفاعلية في تحقيق أهدافها

تتطلب السيادة التنظيمية الجيدة أن تتبنى المنظمات أسلوب منهجي في إدارة المخاطر بحيث:

يتأكد من تطبيق وسائل الرقابة الإدارية وأدائها بشكل كافي.	يتأكد من قيام مجلس الإدارة بتنفيذ واجباته الخاصة بإدارة الإستراتيجية وبناء القيم ومراقبة أداء المنظمة.	يحمي مصالح مختلف أطراف المصلحة في المنظمة.

إعداد تقارير المخاطر والاتصالات

يجب أن تكون إجراءات أعداد تقارير المخاطر واضحة ومتوفرة لدي أصحاب المصلحة في المنظمة.

يجب على معد التقارير الرسمية أن يتناول:

تطبيق نظم المتابعة والمراجعة.	تطبيق نظم الرقابة الأولية بغرض أداره الأخطار الهامة.	الإجراءات المستخدمة في تعريف الأخطار وكيفية التعامل معها بواسطة نظم أداره المخاطر.	أساليب الرقابة، خاصة المسئوليات الإدارية لأدارة المخاطر.

يجب تسجيل أي نقص كبير غير مغطي من قبل النظام أو أي نقص في النظام نفسه، وكذلك تحديد الخطوات التي تم اتخاذها بالفعل للتعامل مع هذا النقص.

مراقبة ومراجعة عمليات إدارة المخاطر

- تتطلب إدارة المخاطر الفعالة نظام لتقديم التقارير والمراجعة للتأكد من التعرف الفعال علي الأخطار وفحصها وأن إجراءات التحكم في المخاطر الملائمة قد تم اتخاذها. ويجب أجراء المراجعة الدورية للسياسة ومستويات التوافق مع القوانين، ومراجعة معايير الأداء لتحديد فرص التطوير.
- يجب أن تتأكد عملية الرقابة من تطبيق إجراءات التحكم المناسبة على أنشطة المنظمة، وأن الإجراءات قد تم فهمها وأتباعها.
- يجب على أي عمليات للرقابة والمراجعة أن تحدد فيما إذا كانت :
  - الإجراءات المتبعة قد أعطت النتائج المخطط له.
  - الإجراءات المتبعة والمعلومات التي تم جمعها بغرض فحص الأخطار كانت ملائمة.
  - التطوير المعرفي قد ساعد على الوصول إلى قرارات أفضل وتحديد الدروس المستفادة لفحص وإدارة الأخطار مستقبلا.

محددات (معوقات) إدارة المخاطر

- إذا تم تقييم المخاطر أو ترتيبها حسب الأولوية بشكل غير مناسب فإن ذلك قد يؤدي إلى تضييع الوقت في التعامل مع المخاطر ذات الخسائر التي من غير المحتمل أن تحدث.
- تمضية وقت طويل في تقييم وإدارة مخاطر غير محتملة يؤدي إلى تشتيت المصادر التي كان من الممكن أن تستغل بشكل مربح أكثر.
- إعطاء عمليات إدارة المخاطر أولوية عالية جدا يؤدي إلى إعاقة عمل المنظمة في إكمال مشاريعها أو حتى المباشرة فيها.
- من المهم أيضا الأخذ بعين الاعتبار حسن التمييز بين الخطورة والشك.

المراجع

- http://islamfin.go-forum.net/montada-f28/topic-t832.htm
- http://ar.wikipedia.org/wiki/%D8%A5%D8%AF%D8%A7%D8%B1%D8%A9_%D8%A7%D9%84%D9%85%D8%AE%D8%A7%D8%B7%D8%B1