



دليل إرشادي

إدارة المخاطر في قطاع

الاتصالات وتقنية المعلومات

2022



وزارة الاتصالات
وتقنية المعلومات
MINISTRY OF COMMUNICATIONS
AND INFORMATION TECHNOLOGY

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

المحتويات

المقدمة	الأهداف	النطاق
4	5	5
إعداد وتطوير الدليل الإرشادي لإدارة المخاطر	المحور الأول: التزام القيادة	المحور الثاني: التخطيط والإعداد والتنفيذ
6	7	9
المحور الثالث: التقييم والمراجعة	المحور الرابع: المراقبة والتقييم	المحور الخامس: الإبلاغ والتواصل
11	16	17
المحور السادس: الاستدامة	الملحق أ: مراجع الممارسات والمعايير العالمية ذات الصلة	الملحق ب: مثال توضيحي لسجل المخاطر
18	19	19
الملحق ج: قوالب إدارة المخاطر	الملحق د: المصطلحات والتعريفات	
23	23	

المقدمة

إيماناً بأهمية زيادة مستوى نضج إدارة المخاطر وإدارة استمرارية الأعمال في قطاع الاتصالات وتقنية المعلومات، مما يدعم موثوقية التقنية الرقمية ويؤدي إلى المحافظة على استدامة قطاع الاتصالات وتقنية المعلومات وتعزيز أسس رقمية قوية ومتينة تتماشى مع أهداف رؤية 2030، تقدم هذه الوثيقة دليلاً إرشادياً يهدف إلى تعزيز نضج إدارة المخاطر في قطاع الاتصالات وتقنية المعلومات كجزء من المبادرات العديدة لوزارة الاتصالات وتقنية المعلومات.

الأهداف

يهدف الدليل الإرشادي لإدارة المخاطر إلى:



تحديد الإجراءات المعنية بإدارة المخاطر وفق معايير عالمية لضمان استجابة استباقية للتهديدات والمخاطر الحالية والمستجدة

تمكين الاقتصاد الرقمي من خلال تعزيز نضج إدارة المخاطر في قطاع الاتصالات وتقنية المعلومات بما يحقق مستهدفات رؤية 2030



تحسين عملية اتخاذ القرار من خلال برنامج شامل لإدارة المخاطر

بيان أهمية تحديد المخاطر في قطاع الاتصالات وتقنية المعلومات وتقديرها وإدارتها، والمساهمة بزيادة المنفعة لجميع أصحاب المصلحة في قطاع الاتصالات وتقنية المعلومات



المساهمة في تخفيف آثار المخاطر المحتملة على موارد ومنتجات وخدمات قطاع الاتصالات وتقنية المعلومات

تعزيز ثقافة الوعي بالمخاطر ونضج إدارة المخاطر في قطاع الاتصالات وتقنية المعلومات

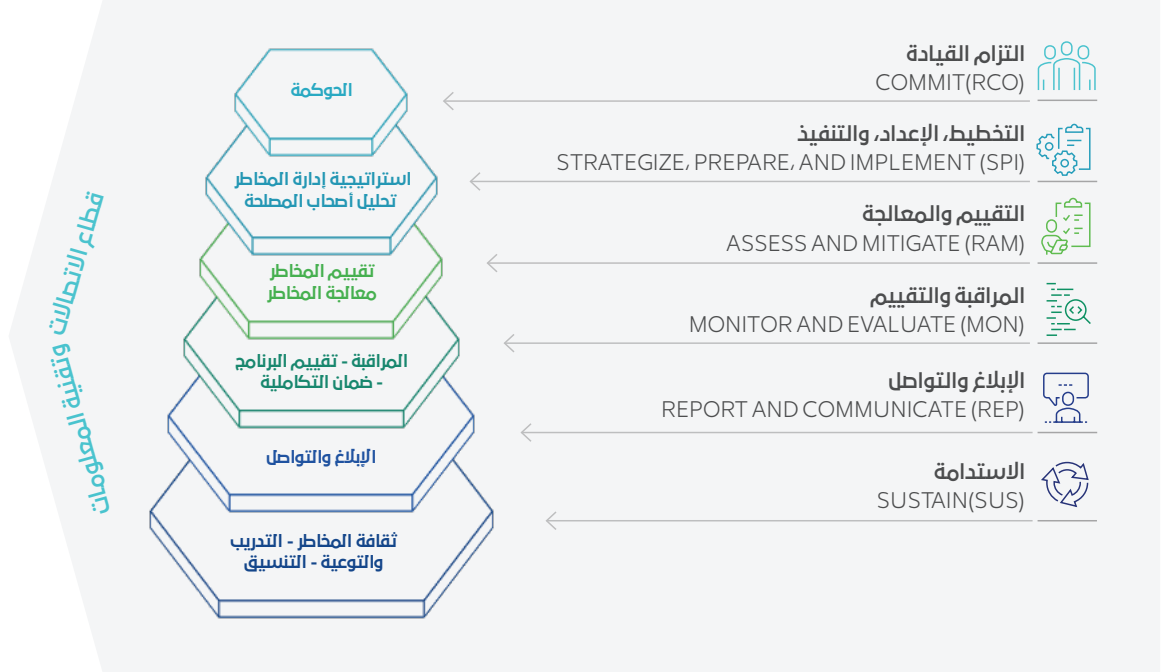
النطاق

إن المعلومات الواردة في هذه الوثيقة هي إرشادات عامة موجهة لقطاع الاتصالات وتقنية المعلومات. وتم أخذ السياسات والتنظيمات المعمول بها في القطاع وطبيعة أعمال الجهات بعين الاعتبار في إعداد الدليل بهدف رفع مستوى نضج إدارة المخاطر في القطاع وعمليات المواءمة المستقبلية مع أي تنظيمات ذات علاقة. ولا تحل هذه الوثيقة محل أي سياسات أو تنظيمات معتمدة.

إعداد وتطوير الدليل الإرشادي لإدارة المخاطر

تم إعداد وتطوير الدليل الإرشادي لإدارة المخاطر بناءً على أفضل الممارسات والمعايير العالمية ذات الصلة. ويوضح هيكل الدليل الإرشادي لإدارة المخاطر (رسم توضيحي 1) المجالات التي تدعمها محاور الدليل الإرشادي.

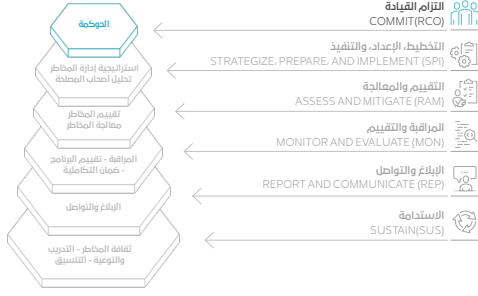
قطاع اتصالات وتقنية المعلومات
برنامج إدارة مخاطر فعال ومرن



رسم توضيحي 1: هيكل الدليل الإرشادي لإدارة المخاطر

نوصي الجهات الراغبة بتطبيق هذا الدليل الإرشادي باتباع الهيكل المذكور أعلاه وتطبيقه بما يتناسب مع طبيعة عمل الجهة المُطبقة للدليل من موارد ومنتجات وخدمات.

تحتوي الوثيقة على محاور الدليل الإرشادي المتعلقة بكل مجال من مجالات إدارة المخاطر المحددة.
الملحق (أ): مراجع الممارسات والمعايير العالمية ذات الصلة. الملحق (ب): مثال توضيحي لسجل المخاطر.
الملحق (ج): قوالب إدارة المخاطر. الملحق (د): المصطلحات والتعريفات.



المحور الأول: التزام القيادة

هدف المجال: تتطلب إدارة المخاطر التزام ودعم القيادة الداخلية لبرنامج إدارة المخاطر عبر إعداد وتطوير هيكل حوكمة لتحديد الأدوار والمسؤوليات في الجهة المُطبقة للدليل والإشراف عليها.

RCO001 - تتولى الإدارة العليا في الجهة المُطبقة للدليل المسؤولية عن برنامج إدارة المخاطر، وتلتزم بدعم برنامج إدارة المخاطر وتنفيذه وتحسينه باستمرار في حال رغبتها باتباع هذا الدليل الإرشادي، من خلال:

- < إنشاء رؤية قيادية مشتركة حول إدارة المخاطر.
- < تحديد أهداف إدارة المخاطر في الجهة المُطبقة للدليل.
- < التوافق مع الأهداف الاستراتيجية للجهة المُطبقة للدليل وقيمها وثقافتها.
- < تضمين منهجية إدارة المخاطر في الجهة المُطبقة للدليل.
- < توفير الموارد المطلوبة لتنفيذ ومتابعة المبادرات المحددة لبرنامج إدارة المخاطر.
- < تمكين آليات التواصل عن المخاطر من خلال القنوات المناسبة لزيادة الوعي وتشجيع ثقافة التركيز على المخاطر.
- < اعتماد برنامج إدارة المخاطر.

RCO002 - تتولى الإدارة العليا في الجهة المُطبقة للدليل المسؤولية عن ضمان الفصل في المهام بين إدارة المخاطر وبين المراجعة الداخلية والوحدات الرقابية الأخرى من قبل الإدارة العليا في الجهة المُطبقة للدليل.

RCO003 - تتولى الإدارة العليا في الجهة المُطبقة للدليل إنشاء لجنة توجيهية لإدارة المخاطر والتي بدورها تقوم بتوجيه برنامج إدارة المخاطر. وترفع اللجنة تقاريرها إلى الإدارة العليا في الجهة المُطبقة للدليل.

RCO004 - تمثيل هيكل الجهة المُطبقة للدليل والإدارات الهامة عن طريق تحديد أعضاء ممثلين لتلك الإدارات في اللجنة التوجيهية.

RCO005 - تتولى الإدارة العليا في الجهة المُطبقة للدليل إعداد ميثاق متكامل يتضمن الأدوار والمسؤوليات ونماذج الحوكمة ومصفوفة الصلاحيات المتعلقة بإدارة المخاطر من قبل الإدارة العليا في الجهة المُطبقة للدليل أو اللجنة التوجيهية لإدارة المخاطر.

RCO006 - تكليف أحد أعضاء الإدارة العليا، ممن لديهم المعرفة ذات الصلة بإدارة المخاطر، قيادة اللجنة التوجيهية.

RCO007 - تتولى الإدارة العليا في الجهة المُطبقة للدليل أو اللجنة التوجيهية في حال إنشائها المسؤولية عن إنشاء وتمكين إدارة للمخاطر تضم المهارات والكفاءات اللازمة لإعداد وتطوير برنامج إدارة المخاطر وتنفيذه ومراجعته وتحديثه وحوكمته.

RCO008 - من المفترض أن تتبع إدارة المخاطر من الناحية الوظيفية للجنة التوجيهية، في حال إنشائها، كما هو موضح في (رسم توضيحي 2).

RCO009 - تتولى الجهة المسؤولة عن إدارة المخاطر التأكد من مناسبة ترشيحات الإدارات المشاركة لسفراء برنامج إدارة المخاطر لتنسيق وتنفيذ الأنشطة والمهام المتعلقة بالبرنامج.

RCO010 - تتولى الإدارة العليا في الجهة المُطبقة للدليل اعتماد ميزانية رسمية سنوية لبرنامج إدارة المخاطر والأنشطة المرتبطة به، والعمل على تنفيذه وتحديثه وتحسينه.

RCO011 - تتولى الجهة المسؤولة عن إدارة المخاطر إعداد وتطوير برنامج إدارة المخاطر في الجهة المُطبقة للدليل بما يتوافق مع حجم الجهة المُطبقة للدليل ونطاق عملها وأهدافها ومصفوفة الصلاحيات بها.

RCO012 - تتولى الإدارة العليا في الجهة المُطبقة للدليل أو اللجنة التوجيهية في حال إنشائها اعتماد مخرجات برنامج إدارة المخاطر.

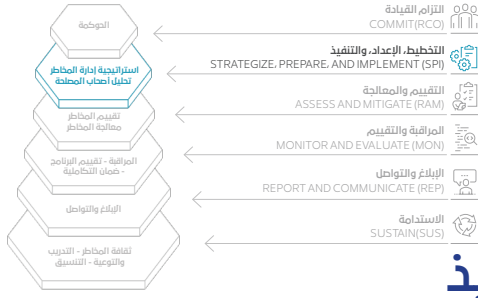
RCO013 - تتولى الجهة المسؤولة عن إدارة المخاطر إعداد وتطوير وتنفيذ ومشاركة سياسة إدارة المخاطر في الجهة المُطبقة للدليل، واعتمادها من قبل الإدارة العليا بشكل دوري أو عند حدوث تغييرات كبيرة في البيئة التشغيلية للجهة المُطبقة للدليل.

RCO014 - تتولى الجهة المسؤولة عن إدارة المخاطر إعداد دليل إجراءات منبثق من سياسة إدارة المخاطر.



رسم توضيحي 2: مثال على هيكلية برنامج إدارة المخاطر

مالك المخاطر هو شخص أو مجموعة من الأشخاص الذين يتحملون مسؤولية إدارة التهديدات ونقاط الضعف والوابط المُحددة لأحد المخاطر في الجهة المُطبقة للدليل ويكون مالك الخطر ذي صلة وظيفية مباشرة مع الخطر ولديه السلطة الكافية لاتخاذ الإجراءات التصحيحية المناسبة لتخفيف الخطر.



المحور الثاني: التخطيط والإعداد والتنفيذ

هدف المجال: تتطلب إدارة المخاطر الفعالة من الجهة المطبقة للدليل، الاستعداد للمخاطر التي قد تنشأ بسبب البيئة المتغيرة للمخاطر في القطاع، ويشمل ذلك تقييم معايير قبول الخطر وإعداد استراتيجية للمخاطر وخطة تنفيذها.

2.1 استراتيجية المخاطر وخطة التنفيذ

تتطلب التقنيات الناشئة والابتكار والتحولت المحتملة داخل قطاع الاتصالات وتقنية المعلومات من الشركة ضرورة المراجعة المستمرة للمستوى المقبول للمخاطر واستراتيجية المخاطر في الجهة المُطبقة للدليل. ولإتمام عملية استراتيجية المخاطر وخطة التنفيذ، يجب على الجهة اتباع الإجراءات التالية:

SPI001 - تتولى الإدارة العليا في الجهة المُطبقة للدليل تحديد معايير قبول الخطر (Risk Appetite).

SPI002 - اعداد وصياغة قوالب معايير قبول الخطر (Risk Acceptance Criteria) التي توضح مستوى المخاطر الذي تتقبله الجهة في سعيها لتحقيق أهدافها وغاياتها.

SPI003 - تتولى الإدارة العليا في الجهة المُطبقة للدليل مراجعة واعتماد معايير قبول الخطر والحدود القصوى لتحمل كل خطر.

SPI004 - تتولى الجهة المسؤولة عن إدارة المخاطر ومُلاك المخاطر إعداد مؤشرات المخاطر الرئيسية.

SPI005 - تتولى الجهة المسؤولة عن إدارة المخاطر إعداد استراتيجية وبرنامج إدارة المخاطر للجهة مع الأخذ بالاعتبار معايير قبول الخطر والحدود القصوى لتحمل الخطر.

SPI006 - تتولى الإدارة العليا في الجهة المُطبقة للدليل أو اللجنة التوجيهية لإدارة المخاطر في حال إنشائها اعتماد استراتيجية وبرنامج إدارة المخاطر وإخطار الأطراف المعنية بذلك.

SPI007 - مراجعة استراتيجية إدارة المخاطر بشكل دوري أو عند حدوث تغييرات كبيرة مع مراعاة التقنيات الناشئة والتحولت المحتملة في القطاع.

SPI008 - ترشيح سفراء المخاطر لتنسيق أنشطة مخاطر الإدارات والأقسام المختلفة المتعلقة ببرنامج إدارة المخاطر وتنفيذها من قبل مُلاك المخاطر وإبلاغها لإدارة المخاطر.

2.2. تحليل أصحاب المصلحة

تحديد أصحاب المصلحة الرئيسيين واستشارتهم بشأن المخاطر في الجهة المُطبقة للدليل. بحيث يتم أخذ مرنّيات أصحاب المصلحة بالاعتبار عند إعداد استراتيجيات المخاطر، وكذلك عند اتخاذ القرارات القائمة على المخاطر.

SPI009 - تتولى الجهة المسؤولة عن إدارة المخاطر إنشاء قائمة أصحاب المصلحة الرئيسيين، والتي تشمل جميع أصحاب المصلحة الداخليين والخارجيين، مثل:

◀ الوزارات والهيئات والمؤسسات العامة ذات العلاقة.

◀ مزودو الخدمات المعتمدون لدى الجهة المُطبقة للدليل.

◀ الموردون المهمون.

◀ الجهات المستفيدة من خدمات الجهة المُطبقة للدليل.

◀ أعضاء مجلس الإدارة والمستثمرون.

◀ وحدات العمل المختلفة وموظفو الجهة المُطبقة للدليل.

◀ الجهات الأخرى ذات الصلة.

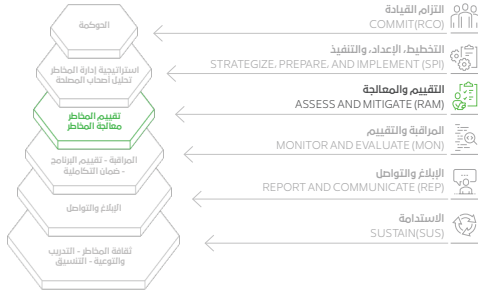
SPI010 - تتولى الجهة المسؤولة عن إدارة المخاطر تحديد أوجه الاعتماد المتبادل بين أصحاب المصلحة لضمان مواءمة الأهداف والخدمات والمنتجات من خلال إعداد مصفوفة أصحاب المصلحة التي تصنف أصحاب المصلحة حسب أهميتهم وتأثيرهم على الجهة المُطبقة للدليل.

SPI011 - تتولى الجهة المسؤولة عن إدارة المخاطر إعداد خطة التواصل مع أصحاب المصلحة بناءً على مصفوفة التواصل للحفاظ على الاتصال الدائم معهم وتقليل المخاطر من خلال:

◀ تحديد نوع الاتصال وقنوات الاتصال، ودورية ومدى تكرار الاتصال المطلوب.

◀ التشاور مع أصحاب المصلحة الرئيسيين لتحديد توقعاتهم لاستراتيجية المخاطر في الجهة المُطبقة للدليل والاعتبارات التي يجب أخذها من أجل إعداد الاستراتيجية.

◀ الحصول على مرنّيات دورية حول برنامج إدارة المخاطر من أصحاب المصلحة.



المحور الثالث: التقييم والمعالجة

هدف المجال: تقييم المخاطر ومعالجتها للتخفيف من حدتها أو استغلالها عن طريق تحويلها إلى فرص هو الأساس لبرنامج إدارة المخاطر ومفتاح لاستراتيجيات المخاطر المستقبلية.

يقسم مسار عملية تقييم ومعالجة المخاطر، بحسب أفضل الممارسات العالمية، إلى عدة مراحل، كما في (رسم توضيحي 3) التالي:



رسم توضيحي 3: مسار عملية تقييم ومعالجة المخاطر

3.1 تقييم المخاطر

يشمل تقييم المخاطر الأنشطة التي تسمح للجهة المُطبقة للدليل بتحديد المخاطر الحالية والمستجدة وتحليلها وتقديرها ومعالجتها.

RAM001 - تتولى الجهة المسؤولة عن إدارة المخاطر إعداد منهجية مُنظمة ومُوحددة لتقييم المخاطر بما يتوافق مع استراتيجية وبرنامج المخاطر واعتمادها من قبل الإدارة العليا أو اللجنة التوجيهية لإدارة المخاطر في حال إنشائها.

RAM002 - تشمل منهجية تقييم المخاطر العوامل التي تمنع أو تعيق الجهة المُطبقة للدليل من تحقيق أهدافها على المدى القصير والمتوسط والطويل حيث يمكن أن تتضمن العملية ما يلي:

< تحديد المخاطر.

< تحليل المخاطر.

< تقدير المخاطر.

RAM003 - تتولى الجهة المسؤولة عن إدارة المخاطر تحديد وتوثيق المخاطر على المستويات الاستراتيجية والتشغيلية ومستوى إجراءات العمل الحساسة.

RAM004 - تتولى الجهة المسؤولة عن إدارة المخاطر تقييم المخاطر بما يشمل موارد ومنتجات وخدمات الاتصالات وتقنية المعلومات المُقدّمة من الجهة المُطبقة للدليل، وفقاً لمنهجية تقييم المخاطر.

RAM005 - تتولى الجهة المسؤولة عن إدارة المخاطر تحديد دورية تكرار عملية تقييم المخاطر، بما في ذلك:

◀ مستوى المخاطر (المستوى الاستراتيجي والتشغيلي وإجراءات العمل الحساسة).

◀ التغييرات في البيئة الداخلية والخارجية للجهة المُطبقة للدليل.

◀ إطلاق المنتجات والخدمات الجديدة للاتصالات وتقنية المعلومات.

RAM006 - تتولى الجهة المسؤولة عن إدارة المخاطر إعداد وتوثيق وتحديث نتائج تقييم المخاطر في سجل مركزي للمخاطر. (من الممكن الاستعانة بنموذج سجل وتقييم ومعالجة المخاطر في الملحق ج.1 في هذه المرحلة).

RAM007 - تتولى الإدارة العليا في الجهة المُطبقة للدليل أو اللجنة التوجيهية لإدارة المخاطر مراجعة واعتماد نتائج تقييم المخاطر في حال إنشائها.

3.1.1 تحديد المخاطر

هي عبارة عن عملية حصر المخاطر الحالية أو المستجدة لإجراء تحليل المخاطر.

RAM008 - تتولى الجهة المسؤولة عن إدارة المخاطر التأكد من قيام مُلاك وسفراء المخاطر بتحديد المخاطر وبيان أسبابها وتأثيرها بما يتوافق مع منهجية تقييم المخاطر وأهداف الجهة المُطبقة للدليل.

RAM009 - تتولى الجهة المسؤولة عن إدارة المخاطر مراجعة واعتماد نتائج تحديد المخاطر بما يتوافق مع منهجية تقييم المخاطر.

RAM010 - تتولى الجهة المسؤولة عن إدارة المخاطر إعداد وتطوير إجراءات، ضمن عملية تحديد المخاطر، لضمان قيام إدارة الموارد البشرية بتحديد وتحنيف وتوثيق المهارات اللازمة التي تقوم بإدارة الخدمات والوظائف الهامة.

RAM011 - تتولى الجهة المسؤولة عن إدارة المخاطر إعداد وتطوير إجراءات، ضمن عملية تحديد المخاطر، لضمان تحديد أوجه الاعتماديات الحرجة داخل سلسلة قيم (Value chain) الاتصالات وتقنية المعلومات في الجهة المُطبقة للدليل من خلال تقييم الأثر وتحديد مدى توفر الاستراتيجيات اللازمة لتخفيف الخسارة المحتملة أو الحد من هذه الاعتماديات.

RAM012 - تتولى الجهة المسؤولة عن إدارة المخاطر إعداد وتطوير إجراءات، ضمن عملية تحديد المخاطر، لضمان قيام الجهة المُطبقة للدليل بتدليل سلسلة الإمداد لقطاع الاتصالات وتقنية المعلومات وتحديد الموردين الرئيسيين للحفاظ على الخدمات الرئيسية.

RAM013 - تتولى الجهة المسؤولة عن إدارة المخاطر التأكد من شمولية المخاطر المحددة لكافة أنواع الموارد والمنتجات وخدمات الاتصالات وتقنية المعلومات المقدمة من الجهة.

للحصول على تفاصيل أكثر عن بناء سجل للمخاطر، من الممكن الرجوع إلى المثال المرفق في **جدول 1**: مثال على سجل المخاطر في الملحق ب.

3.1.2 تحليل المخاطر

عملية قياس المخاطر الكامنة بناءً على احتمالية وأثر الخطر قبل أخذ الضوابط الحالية في الجهة المُطبقة للدليل بعين الاعتبار.

RAM014 - تتولى الجهة المسؤولة عن إدارة المخاطر التأكد من قيام مُلاك وسفراء المخاطر بإجراء تحليل للمخاطر وفقاً لمنهجية تقييم المخاطر المعتمدة من أجل:

◀ قياس المخاطر الكامنة التي تواجهها الجهة المُطبقة للدليل لكل خطر محدد، بما في ذلك الاحتمالية والتأثير والتصنيف الصحيح للخطر (كما هو موضح في **جدول 2**: مثال على مقياس التأثير و**جدول 3**: مثال على مقياس احتمالية حدوث التهديد و**جدول 4**: مثال على مصفوفة قياس المخاطر في الملحق ب).

◀ توثيق وتقييم الضوابط الحالية في الجهة المُطبقة للدليل (كما هو موضح في **جدول 5**: مثال على مقياس فعالية الضوابط الحالية في الملحق ب).

◀ التشاور مع أصحاب المصلحة الرئيسيين لفهم توقعاتهم.

RAM015 - تتولى الجهة المسؤولة عن إدارة المخاطر مراجعة واعتماد تحليل المخاطر بما يتوافق مع منهجية تقييم المخاطر.

3.1.3 تقدير المخاطر

عملية قياس المخاطر المتبقية بعد الأخذ بعين الاعتبار الضوابط الحالية للجهة المُطبقة للدليل.

RAM016 - تتولى الجهة المسؤولة عن إدارة المخاطر التأكد من قيام مُلّاك وسفراء المخاطر بإجراء تقدير للمخاطر وفقاً لمنهجية تقييم المخاطر المعتمدة من أجل:

ك تقييم فعالية وكفاءة الضوابط الحالية.

ك تقييم المخاطر المتبقية التي تواجهها الجهة المُطبقة للدليل لكل خطر محدد.

ك تحديد ما إذا كانت المخاطر المتبقية ضمن نطاق حدود تحمل الخطر.

ك تحديد استراتيجية الاستجابة للمخاطر.

RAM017 - تتولى الجهة المسؤولة عن إدارة المخاطر مراجعة واعتماد تقدير المخاطر بما يتوافق مع منهجية تقييم المخاطر.

3.2 معالجة المخاطر

عملية تخفيف حدة المخاطر المتبقية لمعالجتها.

RAM018 - تتولى الجهة المسؤولة عن إدارة المخاطر التأكد من قيام مُلّاك وسفراء المخاطر بإعداد وتطوير خطط معالجة المخاطر وفقاً لاستراتيجية الاستجابة للمخاطر وفق الخيارات التالية:

ك قبول المخاطر: قبول الخطر دون الحاجة لوضع ضوابط إضافية للحد من الأثر واحتمالية حدوثه ضمن الحد الأدنى المقبول للمخاطر.

ك تخفيف المخاطر: وضع ضوابط إضافية للحد من آثار المخاطر واحتمالية حدوثها جزئياً أو كلياً.

ك نقل المخاطر: تقليل أثر واحتمالية حدوث الخطر من خلال نقل أو مشاركة الخطر مع جهات خارجية كشركات التأمين.

ك إنهاء المخاطر: إنهاء الأنشطة المسببة للخطر في حال كان ضررها أكبر من منفعتها.

ك استغلال المخاطر: الاستعداد للمخاطر بوضع خطط للاستفادة منها وتحقيق الفرص الممكنة.

RAM019 - تقييم إدارة المخاطر لخطط معالجة المخاطر المقترحة من قبل مُلّاك وسفراء المخاطر وتقديم التوجيه فيما يتعلق بهذه الخطط.

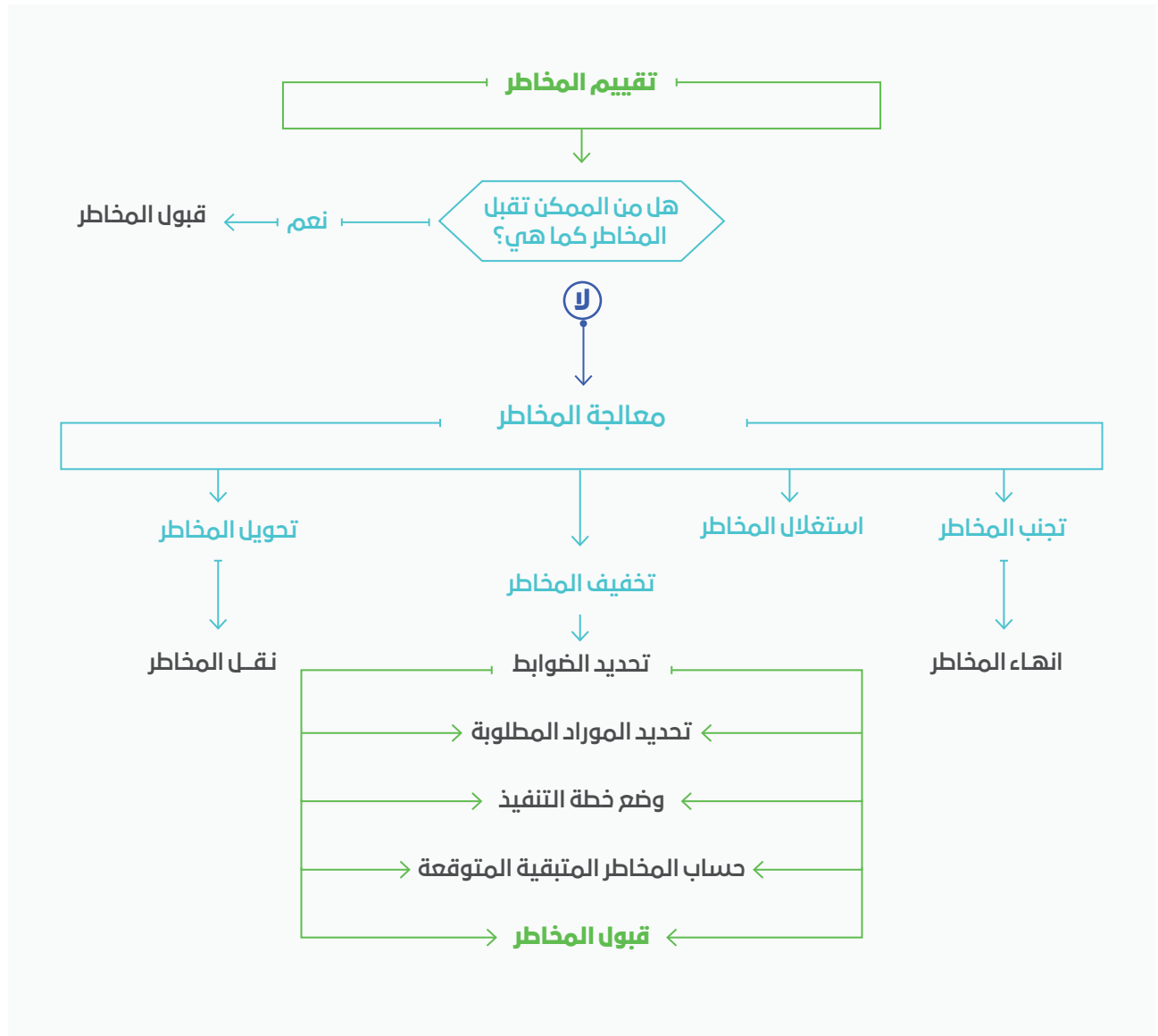
RAM020 - تتولى الإدارة العليا في الجهة المُطبقة للدليل أو اللجنة التوجيهية لإدارة المخاطر في حال إنشائها مراجعة واعتماد خطط معالجة المخاطر المقترحة، وتحديد المُلّاك والجهات المسؤولة عن تنفيذها.

RAM021 - تتولى الجهة المسؤولة عن إدارة المخاطر التأكد من قيام مُلّاك المخاطر بتوثيق خطط معالجة طارئة للمخاطر حال وقوعها.

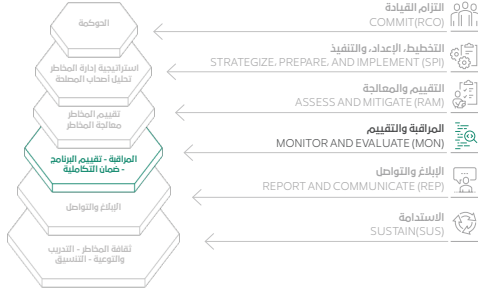
RAM022 - التأكيد من وجود خطط لاستمرارية الأعمال على مستوى الجهة لاستمرارية موارد ومنتجات وخدمات الاتصالات وتقنية المعلومات المقدمة فيها، والتي من الممكن إعدادها بالاستعانة بالدليل الإرشادي لإدارة استمرارية الأعمال في قطاع الاتصالات وتقنية المعلومات.

للحصول على تفاصيل أكثر عن تقدير ومقياس مستويات المخاطر، من الممكن الرجوع إلى المثال المرفق في **جدول 6: مثال على مقياس مستويات المخاطر في الملحق ب.**

تُعتبر عملية معالجة المخاطر من العمليات الهامة، حيث أن النتيجة المرجوة منها هي الوصول إلى مستوى مقبول لجميع المخاطر المتبقية، كما هو موضح في سير العملية التوضيحي المبين أدناه **(رسم توضيحي 4):**



رسم توضيحي 4: مسار عمل معالجة المخاطر



المحور الرابع: المراقبة والتقييم

هدف المجال: على الجهة المُطبِّقة للدليل مراقبة المخاطر والتقدم المحقق نحو إدارة المخاطر ضمن المستوى المقبول لديها.

4.1 المراقبة

تعزز مراقبة المخاطر ثقافة المخاطر داخل الجهة المُطبِّقة للدليل وتسمح بإدارة المخاطر المحددة بشكل استباقي والتكيف مع الظروف المتغيرة.

MON001 - تتولى الإدارة العليا في الجهة المُطبِّقة للدليل أو اللجنة التوجيهية لإدارة المخاطر في حال إنشائها مراقبة مؤشرات المخاطر وخطط معالجة المخاطر، والتغييرات في بيئة المخاطر الداخلية والخارجية، والامتثال للتشريعات والتنظيمات القانونية المفروضة على الجهة المُطبِّقة للدليل التي قد يؤدي عدم الالتزام بها إلى تبعات قانونية وغرامات مالية تختلف باختلاف مجال عمل الجهة المُطبِّقة للدليل.

MON002 - تتولى الجهة المسؤولة عن إدارة المخاطر مراقبة تنفيذ خطط معالجة المخاطر للتأكد من معالجة المخاطر المحددة بشكل فعال.

4.2 تقييم البرنامج

على الجهة المُطبِّقة للدليل تقييم فعالية برنامج إدارة المخاطر لتحديد التحسينات والتطويرات المطلوبة.

MON003 - تتولى الإدارة العليا في الجهة المُطبِّقة للدليل التأكد من وجود عملية محددة وموضوعية لتقييم برنامج إدارة المخاطر بشكل دوري.

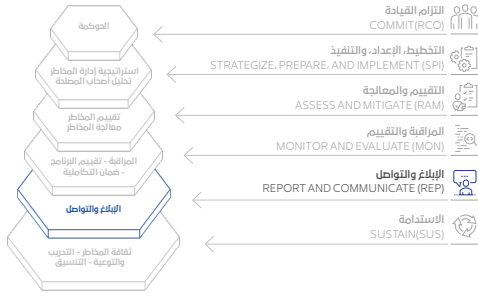
MON004 - تتولى الجهة المسؤولة عن إدارة المخاطر توثيق وتحليل وإبلاغ الدروس المستفادة من المخاطر التي حدثت والمتغيرات الداخلية والخارجية.

4.3 ضمان التكاملية

يشير ضمان التكاملية إلى نهج منسق على مستوى الجهة المُطبِّقة للدليل يتضمن مستويات مختلفة من التأكيد لتقليل المخاطر. ويساهم تعدد مستويات التأكيد في تعزيز المساءلة وضمن مراقبة المخاطر ومراجعتها على مستوى الجهة المُطبِّقة للدليل.

MON005 - تتولى الإدارة العليا في الجهة المُطبِّقة للدليل التأكد من وجود تكامل وتنسيق فعال بين خطوط الدفاع المختلفة.

MON006 - تتولى الجهة المسؤولة عن إدارة المخاطر إعداد وتطوير آلية لضمان التعاون بين إدارة المخاطر والمراجعة الداخلية والامتثال ووحدات الرقابة الأخرى لدعم بعضها البعض في تنفيذ مسؤوليات ضمان التكاملية.

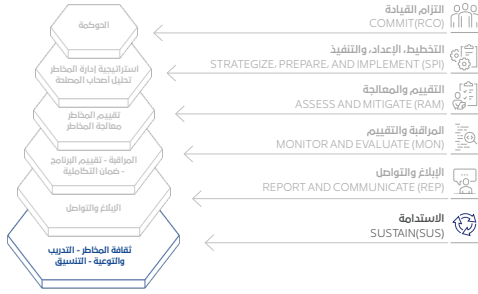


المحور الخامس: الإبلاغ والتواصل

هدف المجال: يؤدي الإبلاغ عن المخاطر والتواصل الفعّال إلى رفع الوعي العام حول المخاطر التي تواجه الجهة المُطبقة للدليل، وتعزيز التخفيف من المخاطر في الوقت المناسب، وتمكين اللجنة التوجيهية لإدارة المخاطر من الوفاء بالتزاماتها الإشرافية.

REPO01 - تتولى الجهة المسؤولة عن إدارة المخاطر إعداد وتطوير آلية للإبلاغ والتواصل عن المخاطر في برنامج إدارة المخاطر لأصحاب المصلحة.

REPO02 - تتولى الجهة المسؤولة عن إدارة المخاطر إعداد مصفوفة هلاحيات تنظم التواصل مع أصحاب المصلحة المعنيين في برنامج إدارة المخاطر.



المحور السادس: الاستدامة

هدف المجال: تساعد الاستدامة برنامج إدارة المخاطر على تمكين الجهة المُطبقة للدليل من زيادة نضج برنامج إدارة المخاطر لديها، ودمج إدارة المخاطر في ثقافة الجهة المُطبقة للدليل، بحيث تصبح جزءاً من العمليات التشغيلية اليومية.

6.1 ثقافة المخاطر

تعزز ثقافة المخاطر الالتزام والتعاون والوعي بين الموظفين وكافة أقسام الجهة المُطبقة للدليل.

RSU001 - تتولى الإدارة العليا في الجهة المُطبقة للدليل واللجنة التوجيهية لإدارة المخاطر في حال إنشائها تشجيع ودعم برنامج إدارة المخاطر من خلال قنوات التواصل المتاحة.

RSU002 - المشاركة والمساهمة بفاعلية في برنامج إدارة المخاطر من قبل أعضاء الإدارة العليا ومُلاك وسفراء المخاطر.

6.2 التدريب والتوعية

يهدف التدريب والتوعية إلى رفع ثقافة إدارة المخاطر وزيادة نضجها في الجهة المُطبقة للدليل.

RSU003 - تتولى الجهة المسؤولة عن إدارة المخاطر التنسيق مع الجهة المختصة في الجهة المُطبقة للدليل لإعداد وتنفيذ خطة التدريب على إدارة المخاطر بناءً على تقييم سنوي لاحتياجات التدريب.

RSU004 - تتولى الجهة المسؤولة عن إدارة المخاطر إعداد وتطوير وتنفيذ برنامج شامل للتوعية بإدارة المخاطر ومراجعتها وتحديثه بشكل دوري.

RSU005 - تتولى الجهة المسؤولة عن إدارة المخاطر تقييم فعالية برامج التدريب والتوعية الخاصة ببرنامج إدارة المخاطر وتحديثها بشكل دوري.

6.3 التنسيق

يعزز التنسيق بين برنامجي إدارة المخاطر وإدارة استمرارية الأعمال داخل الجهة المُطبقة للدليل من أداء كليهما؛ ويعود بالنفع على الجهة المُطبقة للدليل.

RSU006 - تتولى الجهات المسؤولة عن إدارة المخاطر وإدارة استمرارية الأعمال في حال تم تطوير البرنامجين داخل الجهة المُطبقة للدليل إعداد وتطوير آلية لضمان التعاون بين برنامجي إدارة المخاطر وإدارة استمرارية الأعمال لدعم بعضهما البعض في تنفيذ المسؤوليات ذات الصلة وترشيد الإنفاق، والاستفادة المثلى من الموارد.

الملحق أ: مراجع الممارسات والمعايير العالمية ذات الصلة

تم إعداد محاور الدليل الإرشادي ومجالات إدارة المخاطر المرتبطة به بناءً على الممارسات والمعايير والإرشادات الرائدة، ويشمل ذلك:

◀ لجنة المنظمات الراعية (COSO) - إطار إدارة المخاطر المؤسسية (2017).

◀ المنظمة الدولية للمعايير (ISO) - المعيار ISO 31000:2018 إرشادات إدارة المخاطر.

◀ معهد إدارة المخاطر IRM.

الملحق ب: مثال توضيحي لإدارة المخاطر

تبدأ عملية إدارة المخاطر بتحديد المخاطر عن طريق بناء سجل للمخاطر يحتوي على كافة خدمات الجهة المُطبقة للدليل وأصولها، ويعرض كافة أنواع المخاطر التي قد تؤثر عليها كما في الجدول التالي:

جدول 1: مثال على سجل المخاطر

الرقم	الخدمة	العملية المعنية بالخطر	الخطر	تصنيف الخطر	التفاهيل
مثال: 0001	إدارة الموارد البشرية - شؤون الموظفين	مثال: سجل الموظفين	مثال: تسريب معلومات حساسة من قاعدة بيانات معلومات الموظفين عن طريق هجوم سببراني	مخاطر سببرانية	مثال: تحتوي قاعدة البيانات هذه على كافة معلومات الموظفين في الجهة بما فيها بعض المعلومات السرية والحساسة والتي قد يؤدي تسريبها إلى آثار قانونية جسيمة وأثر على سمعة الجهة

عند الانتهاء من بناء سجل المخاطر، تبدأ عملية تحليل المخاطر التي تهدف للقيام بقياس فعال للمخاطر في الجهة، ويجب توثيق مقياس التأثير واحتمالية حدوث التأثير كجزء من منهجية تقييم المخاطر التي قد تختلف من جهة لأخرى. ويتم إعداد هذه المقاييس بما يناسب الجهة كما في المثال التالي:

جدول 2: مثال على مقياس التأثير

#	مستوى التأثير	وصف التأثير
1	منخفض جداً	أثر حدوث المخاطر محدود جداً ولا يترك أي تأثير ملموس على الجهة
2	منخفض	أثر حدوث المخاطر محدود وقد يترك تأثير طفيف على الجهة
3	متوسط	أثر حدوث المخاطر متوسط ومن المتوقع أن يترك تأثير سلبي على الجهة ولكنه أثر يمكن تداركه
4	مرتفع	أثر حدوث المخاطر عالي ومن المتوقع أن يترك تأثير سلبي واضح على الجهة ويحتاج لجهود كبيرة لتداركه
5	مرتفع جداً	أثر حدوث المخاطر عالي للغاية ومن المؤكد أن يترك تأثير جسيم وكبير على الجهة ويحتاج لجهود كبيرة جداً لتداركه

جدول 3: مثال على مقياس احتمالية حدوث التهديد

#	مستوى الاحتمالية	وصف الاحتمالية
1	نادر	من غير المتوقع حدوثه بتاتاً ولم يحدث خلال آخر 3 سنوات
2	من حين لآخر	من غير المحتمل حدوثه مع وجود احتمال ضئيل للحدوث ولم يحدث أكثر من مرة خلال آخر 3 سنوات
3	ممکن	من الممكن حدوثه أحياناً وقد حدث لمرة أو مرتين خلال آخر سنة
4	محتمل	من المحتمل حدوثه وقد حدث لمرة أو مرتين خلال آخر 6 أشهر
5	متكرر	من المتوقع حدوثه بشكل متكرر وقد حدث لأكثر من مرة خلال آخر 3 أشهر

بعد تحديد مستويات الاحتمالية والتأثير في منهجية إدارة المخاطر، يُقاس مستوى المخاطر الكامنة للمخاطر التي تم التوصل إليها في سجل المخاطر المعد مسبقاً عن طريق اعتماد المعادلة:
(قيمة مستوى الاحتمالية × قيمة مستوى التأثير = قيمة المخاطر الكامنة)
 للحصول على مصفوفة قياس المخاطر كما في المثال التالي:

جدول 4: مثال على مصفوفة قياس المخاطر

مصفوفة قياس المخاطر					مستوى الاحتمالية	
25	20	15	10	5	5	متكرر
20	16	12	8	4	4	محتمل
15	12	9	6	3	3	ممکن
10	8	6	4	2	2	من حين لآخر
5	4	3	2	1	1	نادر
5	4	3	2	1	مستوى التأثير	
مرتفع جداً	مرتفع	متوسط	منخفض	منخفض جداً		

كجزء من المنهجية المحددة لإدارة المخاطر، يتم تحديد آلية لكيفية قياس مدى فعالية الضوابط الحالية وأثرها على المخاطر الكامنة التي تم تحديد مستوياتها مسبقاً. ويوجد هناك دور كبير للضوابط الحالية في تخفيف مستوى المخاطر الكامنة مما يساهم بتحديد المستوى الفعلي للمخاطر المتبقية التي يجب التعامل معها. ويتم إعداد هذه المقاييس بما يناسب الجهة كما في المثال التالي:

جدول 5: مثال على مقياس فاعلية الضوابط الحالية

#	مستوى فاعلية الضوابط	نسبة فاعلية الضوابط	وصف فاعلية الضوابط
1	ممتاز	80% فأعلى	تعمل الضوابط بشكل فعال للغاية وليست بحاجة لأي تحسين
2	جيد	60% فأعلى	تعمل الضوابط بشكل فعال ولكن قد تكون بحاجة لبعض التحسين
3	متوسط	40% فأعلى	تعمل الضوابط بشكل مقبول ولكنها بحاجة لبعض التحسين
4	ضعيف	20% فأعلى	تعمل الضوابط بشكل دون المقبول وهي بحاجة للتحسين
5	غير مرضي	0% فأعلى	ضوابط غير فعالة وليست ذات أثر في تخفيف المخاطر

قيمة المخاطر المتبقية = قيمة المخاطر الكامنة - (نسبة فاعلية الضوابط الحالية × قيمة المخاطر الكامنة)

بعد تحديد قيمة المخاطر المتبقية عن طريق قياس فاعلية الضوابط الحالية على المخاطر الكامنة، يتم تحديد مستوى تلك المخاطر كجزء من مرحلة تقدير المخاطر بناءً على المستويات المحددة للمخاطر في منهجية إدارة المخاطر كما في المثال التالي:

جدول 6: مثال على مقياس مستويات المخاطر

مستوى الخطر	قياس الخطر المتبقي	الحاجة لضوابط إضافية
المخاطر المنخفضة	1-6	لا حاجة لوضع أي ضوابط إضافية
المخاطر المتوسطة	7-10	التخطيط لوضع ضوابط إضافية إن أمكن ذلك خلال فترة زمنية محددة
المخاطر المرتفعة	11-15	يجب التخطيط لوضع ضوابط إضافية خلال فترة زمنية محددة
المخاطر الشديدة	16-25	يجب وضع ضوابط إضافية بشكل فوري

إن جميع القيم والمستويات والوصف الخاص بها المذكورة في المثال هي مجرد أمثلة عامة يمكن الاستعانة بها في بناء منهجية إدارة المخاطر الخاصة بالجهة وهي غير ملزمة. ويجب على الجهة المعنية بإدارة المخاطر تحديد كافة المستويات ذات الصلة بحسب حاجة الجهة ومدى حساسية أعمالها وتأثير المخاطر عليها. (من الممكن الاستعانة بنموذج سجل وتقييم ومعالجة المخاطر في الملحق ج.1 في عملية تحديد وتحليل وتقدير ومعالجة المخاطر).

الملحق ج: قوالب إدارة المخاطر

تبدأ عملية إدارة المخاطر بتحديد المخاطر عن طريق بناء سجل للمخاطر يحتوي على كافة خدمات الجهة المُطبقة للدليل وأهولها، ويعرض كافة أنواع المخاطر التي قد تؤثر عليها كما في الجدول التالي:

#	اسم النموذج	التحميل
1	نموذج سجل وتقييم ومعالجة المخاطر	اضغط هنا لتحميل النموذج

الملحق د: المصطلحات والتعريفات

المصطلح	التعريف
Ministry of Communications and Information Technology (MCIT)	وزارة الاتصالات وتقنية المعلومات وهي الوزارة المسؤولة عن جميع وسائل الاتصال وتقنية المعلومات في المملكة العربية السعودية، وهي الجهة المعنية بوضع الخطط التطويرية لقطاع الاتصالات وتقنية المعلومات في المملكة.
القطاع ICT (Information & Communications Technology)	قطاع الاتصالات وتقنية المعلومات
National Transformation Program (NTP)	برنامج التحول الوطني
Committee of Sponsoring Organizations of the Treadway Commission (COSO)	لجنة رعاية المنظمات (إطار تقييم انظمة الرقابة الداخلية).
International Organization for Standardization (ISO)	المنظمة الدولية للمعايير (أيزو)
التأكيد (Assurance)	تقييم مستقل وموضوعي يوفر معلومات موثوقة لدعم اتخاذ القرار. ويمنح الثقة لهيئات الحوكمة والإدارة.
مصفوفة الصلاحيات (Authority Matrix)	قائمة أو جدول يحدد الصلاحيات الممنوحة للأطراف المختلفة في الجهة سواء كانت صلاحيات مالية أو ادارية أو تشغيلية. كما يبين نوع الصلاحيات الممنوحة سواء كانت اعداد أو مراجعة أو اعتماد أو إبلاغ.

المصطلح	التعريف
ضمان التكاملية (Combined Assurance)	نهج منسق (متكامل) يتم تطبيقه في الجهة للتأكد من أن المخاطر الرئيسية تدار بشكل مناسب داخل الجهة.
موارد ومنتجات وخدمات الاتصالات وتقنية المعلومات (Communication and Information Technology Resources, Products and Services)	الموارد والمنتجات والخدمات الخاصة بالاتصالات وتقنية المعلومات المقدمة من الجهة، والتي تهدف إلى تحقيق أهداف الجهة ومهامها على النحو المحدد في استراتيجيتها.
الامتثال (Compliance)	الالتزام والتصرف وفقاً للنظام القانوني أو التشريعي المحدد والمطبق على الجهة والذي قد يؤدي عدم الالتزام به إلى تبعات قانونية وغرامات مالية.
الضوابط (Controls)	أي تدابير أو إجراءات تعمل على تغيير المخاطر. وقد يشمل ذلك أي سياسة أو إجراء أو ممارسة أو عملية أو تقنية أو أسلوب أو طريقة. وتصبح إجراءات معالجة المخاطر بمثابة ضوابط بمجرد تنفيذها.
فاعلية الضوابط (Controls Effectiveness)	مقياس لقوة الضوابط التي يتم تنفيذها للتخفيف من المخاطر. فعلى سبيل المثال، قد تكون الضوابط الضعيفة غير فعالة في حالة وجود عوامل مهمة خارج نطاق سيطرة الجهة.
المجالات (Domains)	المجالات الموجودة في الدليل الإرشادي لإدارة المخاطر في قطاع الاتصالات وتقنية المعلومات والتي تساهم في النهج الشامل والمنظم لإدارة المخاطر.
إدارة المخاطر المؤسسية (Enterprise Risk Management)	نهج يتم تطبيقه على مستوى الجهة لإدارة جميع المخاطر التي تتعرض لها الجهة.
التأثير (Impact)	تأثير وعواقب المخاطر إذا وقعت.
الاتصالات وتقنية المعلومات (Information and Communications Technology)	مجموعة متنوعة من الأدوات والموارد التقنية المستخدمة لنقل المعلومات أو تخزينها أو إنشائها أو مشاركتها أو تبادلها.
المخاطر الكامنة (Inherent Risks)	هي المخاطر الكامنة في الاعمال دون الأخذ بالاعتبار فاعلية الضوابط الحالية.
مؤشرات المخاطر الرئيسية (Key Risk Indicators)	المقاييس التي يمكن مراقبتها باعتبارها مؤشرات رئيسية. وتستخدم لتقديم مؤشرات مبكرة لزيادة أو تراجع التعرض للمخاطر في مختلف مجالات الجهة.

المصطلح	التعريف
الوظائف الهامة (Key Positions)	وهي وظائف تساعد على تمكين استمرارية موارد الاتصالات وتقنية المعلومات ومنتجاتها وخدماتها والمساهمة في تحقيق الأهداف التنظيمية، وهي: <ul style="list-style-type: none"> < الوظائف القيادية < وظائف أمن المعلومات < الوظائف المتعلقة بإدارة الشبكات < الوظائف المتعلقة بإدارة البيانات والتطبيقات
الممارسات العالمية الرائدة (Leading Practices)	طريقة أو تقنية تم قبولها بشكل عام عوضاً عن البدائل الأخرى لأنها تحقق نتائج أهدت بمثابة طريقة قياسية لتنفيذ الأشياء، مثل ISO31000 وCOSO.
الاحتمالية (Likelihood)	أرجحية أو فرصة حدوث المخاطر. ويمكن تعريف الاحتمالية أو تحديدها أو قياسها بشكل موضوعي أو ذاتي ويمكن التعبير عنها إما نوعياً أو كمياً.
الهدف (Objective)	هدف شامل يتوافق مع السياسة التي تضعها الجهة لنفسها.
المخاطر التشغيلية (Operational Risks)	المخاطر الهامة التي تؤثر على قدرة الجهة على تنفيذ خططها الاستراتيجية.
العملية (Process)	مجموعة من الأنشطة المترابطة أو المتفاعلة التي تحول المدخلات إلى مخرجات.
مخاطر العمليات (Processes Risks)	المخاطر المرتبطة بالعمليات اليومية للجهة.
تنظيمي (Regulatory)	مصطلح مشابه لمصطلح قانوني أو تشريعي ولكن عادة ما تكون قواعد تفرضها الجهة التنظيمية وليس من خلال التشريعات الحكومية المباشرة.
المخاطر المتبقية (Residual Risks)	تشير إلى مستوى المخاطر المتبقية بعد الأخذ بالاعتبار فاعلية الضوابط الحالية.
الموارد (Resources)	جميع الموظفين، والمهارات، والبنية التحتية للتقنية، والمنتجات، والخدمات، والمباني، والإمدادات، والمعلومات التي يجب أن تتوفر لدى الجهة لاستخدامها، عند الحاجة، من أجل تسيير العمل وتحقيق أهدافها.
الخطر (Risk)	حدث غير متوقع يمكن أن يؤثر على أهداف الجهة إيجاباً أو سلباً.

المصطلح	التعريف
معايير قبول الخطر (Risk Acceptance Criteria)	تعبير مختصر عن مقدار ونوع المخاطر التي تتقبلها الجهة في إطار سعيها لتحقيق أهداف ونتائج أعمالها.
تقييم المخاطر (Risk Assessment)	عملية ممنهجة لتحديد المخاطر وتحليلها وتقديرها.
القدرة القطوى على تحمل المخاطر (Risk Capacity)	الحد الأقصى من المخاطر التي يمكن أن تتحملها الجهة قبل أن تتضرر بشكل يتعذر معه الإصلاح أو على الأقل عدم قدرتها على الاستمرار في العمل بنفس الطريقة كما كانت من قبل.
سفراء المخاطر (Risk Champions)	أفراد مسؤولون عن تضمين إدارة المخاطر في المجالات الوظيفية من خلال علاقاتهم الشخصية والمهنية الحالية، وهم مجموعة تتمتع بالخبرات التشغيلية المتنوعة للمساعدة في صياغة رؤية أكثر شمولية للمخاطر.
التعرض للمخاطر (Risk Exposure)	مقياس الخسارة المستقبلية المحتملة الناتجة عن نشاط أو حدث معين.
إدارة المخاطر (Risk Management)	تحديد المخاطر وتقييمها وترتيب أولوياتها يتبعها استخدام منسق واقتصادي للموارد لتقليل احتمالية أو تأثير الأحداث السلبية أو مراقبتها أو التحكم فيها أو لتحقيق أقصى قدر ممكن من الفرص.
الجهة المسؤولة عن إدارة المخاطر (Risk Management Function)	الجهة المسؤولة عن الإدارة اليومية المستمرة لبرنامج إدارة المخاطر والأنشطة المرتبطة به.
الجهة المطبقة للدليل	هي الجهة التي ستتبني الدليل الإرشادي بحسب تصنيفها، شركة أو مؤسسة تجارية أو صناعية تتعلق أعمالها بخدمات أو موارد أو منتجات تُقدم لقطاعات حكومية أو خاصة أو أفراد.
سياسة إدارة المخاطر (Risk Management Policy)	نوايا واتجاهات الجهة، وفقاً لما حددته رسمياً إدارتها العليا فيما يتعلق بإدارة المخاطر.
اللجنة التوجيهية لإدارة المخاطر (Risk Management Steering Committee)	لجنة من طائفي القرارات (مثل قادة الأعمال وخبراء التقنية وإدارة المخاطر المكلفون بإعداد السياسة الاستراتيجية واتخاذ قرارات إدارة المخاطر للجهة، وتوفير الموارد اللازمة لتحقيق جميع أهداف برنامج إدارة المخاطر.
هيكل إدارة المخاطر (Risk Management Tower)	رسم توضيحي للمفاهيم الأساسية المرتبطة بمجالات إدارة المخاطر الموضحة في هذا الدليل الإرشادي.
برنامج إدارة المخاطر (Risk Management Program)	يتألف برنامج إدارة المخاطر من الأنشطة والعمليات التي يمكن تطبيقها بشكل متساوٍ على المستويات الإستراتيجية أو المؤسسية أو المشاريع التشغيلية والمنتجة من سياسة إدارة المخاطر.

المصطلح	التعريف
مالك الخطر (Risk Owner)	شخص أو كيان تم منحه السلطة لإدارة مخاطر معينة ويكون مسؤولاً عن القيام بذلك.
استراتيجية المخاطر وخطة التنفيذ (Risk Strategy and Implementation Plan)	يتم إعداد استراتيجية المخاطر وخطة التنفيذ بالجهة لتفعيل تنفيذ سياسة إدارة المخاطر وتحديد جميع متطلبات إدارة المخاطر التي تحتاج الجهة إلى تنفيذها.
الإدارة العليا (Senior Management)	أعلى مستوى للمدراء في الجهة، مباشرة تحت الهيكل القيادي للجهة (أعلى سلطة).
الطرف المهتم / الطرف المعني / صاحب العلاقة (Stakeholder)	فرد أو مجموعة لها مصلحة في أداء أو نجاح الجهة، مثل العملاء والشركاء والموظفين والمساهمين والملوك والمجتمع المحلي وأول المستجيبين والحكومة والجهات التنظيمية.
استراتيجي (Strategic)	مستوى يتألف من الإدارة العليا وموظفين تابعين يتخذون قرارات تتفق مع استراتيجية الجهة لتوجيه برنامج إدارة المخاطر والإشراف عليه.
سلسلة الإمداد (Supply Chain)	سلسلة من العمليات المتضمنة في إنتاج وتوزيع منتج أو خدمة.
الاستدامة (Sustainability)	ترسيخ ثقافة المخاطر في الجهة من خلال مبادرات التدريب والتوعية المستمرة.
التحديات (Threats)	سبب محتمل لحادث غير مرغوب فيه يمكن أن يتسبب في ضرر للجهة.
خطة التواصل	وثيقة توضح احتياجات الاتصال الخاصة بأصحاب المصلحة.

