



وزارة الاتصالات
وتقنية المعلومات
MINISTRY OF COMMUNICATIONS
AND INFORMATION TECHNOLOGY

سياسة إدارة المخاطر للشركات المرخصة في قطاع الاتصالات وتقنية المعلومات

2020



المحتويات

2	المقدمة
2	الغرض
2	الأهداف
2	النطاق
3	المسؤوليات
3	تطبيق السياسة
4	1. إعداد وتطوير سياسة إدارة المخاطر
5	2. التزام القيادة
5	3. التخطيط والإعداد والتنفيذ
6	1-3 استراتيجية المخاطر وخطة التنفيذ
6	2-3 تحليل أصحاب المصلحة
7	4. التقييم والمعالجة
7	1-4 تقييم المخاطر
7	1-1-4 تحديد المخاطر
8	2-1-4 تحليل المخاطر
8	3-1-4 تقدير المخاطر
8	2-4 معالجة المخاطر
9	5. مراقبة وتقييم البرنامج
9	1-5 المراقبة
9	2-5 تقييم البرنامج
9	3-5 ضمان التكاملية
9	6. الإبلاغ والتواصل
10	7. الاستدامة
10	1-7 ثقافة المخاطر
10	2-7 التدريب والتوعية
10	3-7 التنسيق
11	الملحق أ: مراجع الممارسات والمعايير العالمية ذات الصلة
12	الملحق ب: الاختصارات
13	الملحق ج: المصطلحات والتعريفات



المقدمة

اعتمد مجلس الوزراء رؤية 2030 عام 2016 لتحقيق المملكة رؤيتها المتمثلة في أن تكون "العمق العربي والإسلامي وقوة استثمارية رائدة ومحور ربط القارات الثلاث". وهذه الرؤية الطموحة والجديرة بالثناء تدعمها ثلاث ركائز تتمثل في "مجتمع حيوي واقتصاد مزدهر ووطن طموح". ولتحقيق أهداف رؤية 2030، تم وضع برامج تنفيذية، مثل برنامج التحول الوطني الذي يهدف إلى تحقيق التميز في الأداء الحكومي، وتعزيز الممكّنات الاقتصادية، والارتقاء بمستوى الخدمات المعيشية.

طورت وزارة الاتصالات وتقنية المعلومات عدة مبادرات تهدف إلى تحقيق مستهدف تنمية الاقتصاد الرقمي ضمن برنامج التحول الوطني (2)، ومن ضمن أهداف هذه المبادرات زيادة مستوى نضج إدارة المخاطر وإدارة استمرارية الأعمال في قطاع الاتصالات وتقنية المعلومات، مما يدعم موثوقية التقنية الرقمية ويؤدي إلى تحقيق الاستدامة وتعزيز أسس رقمية قوية ومتينة تتماشى مع أهداف رؤية 2030.

يقود مركز إدارة المخاطر واستمرارية الأعمال في وزارة الاتصالات وتقنية المعلومات المبادرات التي تخص إدارة المخاطر واستمرارية الأعمال والصمود ضمن برنامج التحول الوطني (2). انبثق من هذه المبادرات مشروع إعداد وتطوير سياسة إدارة المخاطر في قطاع الاتصالات وتقنية المعلومات التي يجب تطبيقها بشكل استباقي لتخفيف آثار المخاطر المحتملة على موارد ومنتجات وخدمات قطاع الاتصالات وتقنية المعلومات.

الغرض

تحدد هذه الوثيقة الحد الأدنى من سياسات إدارة المخاطر للشركات المرخصة في قطاع الاتصالات وتقنية المعلومات لتبني وتعزيز إدارة المخاطر.

الأهداف

أهداف سياسة إدارة المخاطر:

- تمكين الاقتصاد الرقمي من خلال تطبيق سياسة إدارة المخاطر للشركات المرخصة في قطاع الاتصالات وتقنية المعلومات بما يحقق مستهدفات رؤية 2030.
- تحديد نهج منظم يمكن الشركات المرخصة في قطاع الاتصالات وتقنية المعلومات من تضمين إدارة المخاطر، وبالتالي ضمان استجابة استباقية للتهديدات والمخاطر الحالية والمستجدة.
- بيان أهمية تحديد مخاطر قطاع الاتصالات وتقنية المعلومات وتقديرها وإدارتها، والذي سيؤدي إلى تعظيم المنفعة لجميع أصحاب المصلحة في قطاع الاتصالات وتقنية المعلومات.
- رفع مستوى التبني والامتثال لسياسات إدارة المخاطر.
- تحسين عملية اتخاذ القرار من خلال برنامج شامل لإدارة المخاطر.
- تعزيز ثقافة الوعي بالمخاطر ونضج إدارة المخاطر في قطاع الاتصالات وتقنية المعلومات.

النطاق

تنطبق سياسة إدارة المخاطر على الشركات المرخصة في قطاع الاتصالات وتقنية المعلومات التي يجب أن تتبنى بنودها المنصوص عليها في هذه الوثيقة.

نحث الشركات الأخرى في قطاع الاتصالات وتقنية المعلومات على تبني وتطبيق بنود السياسة لتخفيف آثار المخاطر المحتملة على موارد ومنتجات وخدمات الاتصالات وتقنية المعلومات.



المسؤوليات

تنقسم الأنشطة المتعلقة بإدارة سياسة المخاطر إلى نشاطين؛ (1) المراجعة والتحديث المستمر للسياسة و(2) تنفيذ هذه السياسة من قبل الأطراف المعنية ذات الصلة.

يلخص (الجدول 1) أدوار مختلف الأطراف المعنية في مراجعة وتنفيذ هذه السياسة.

الجدول 1: إدارة السياسة

الأنشطة المتعلقة بإدارة سياسة إدارة المخاطر		الأطراف المعنية
التنفيذ	المراجعة والتحديث	
A	R	وزارة الاتصالات وتقنية المعلومات
R*	C + I	هيئة الاتصالات وتقنية المعلومات
R	C + I	الشركات المرخصة في قطاع الاتصالات وتقنية المعلومات
لا ينطبق	I	وحدة المخاطر الوطنية

شرح الرموز: المسؤولية = R المساءلة = A الاستشارة = C الإعلام/الاطلاع = I وضع اللوائح = R*

تطبيق السياسة

على الشركات المرخصة في قطاع الاتصالات وتقنية المعلومات مسؤولية تطبيق بنود السياسة المنصوص عليها في هذه الوثيقة.

يقوم مركز إدارة المخاطر واستمرارية الأعمال في وزارة الاتصالات وتقنية المعلومات بمتابعة تبني وامتنال الشركات المرخصة في قطاع الاتصالات وتقنية المعلومات لهذه السياسة.

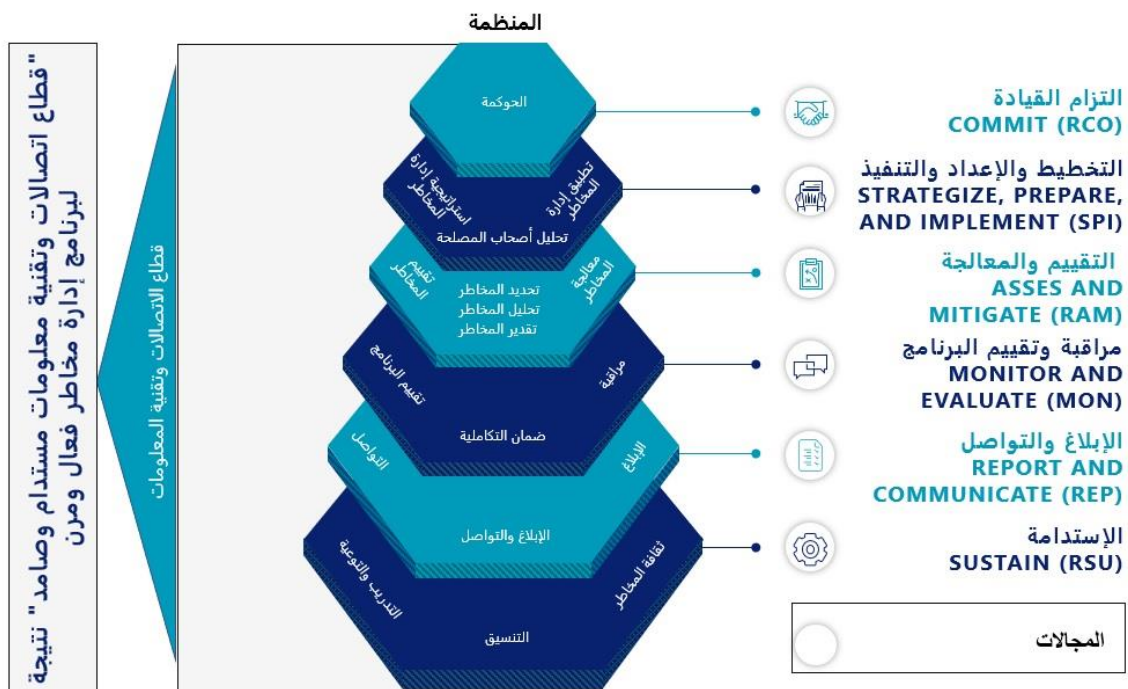
1. إعداد وتطوير سياسة إدارة المخاطر

تم إعداد وتطوير سياسة إدارة المخاطر بناءً على:

- تحليل الوضع الحالي للقطاع.
- أفضل الممارسات والمعايير العالمية ذات الصلة.
- الدراسات المعيارية والمقارنة.
- تحديد ودراسة الفجوات.
- دراسة موارد ومنتجات وخدمات قطاع الاتصالات وتقنية المعلومات.

يوضح هيكل إدارة المخاطر (الشكل 1) المجالات التي تدعمها بنود السياسة.

الشكل 1: هيكل إدارة المخاطر



تحتوي الوثيقة على:

1. بنود السياسة المتعلقة بكل مجال من مجالات إدارة المخاطر المحددة.
2. الملحق (أ) مراجع الممارسات والمعايير العالمية ذات الصلة.
3. الملحق (ب) الاختصارات.
4. الملحق (ج) المصطلحات والتعريفات.



2. التزام القيادة

هدف المجال: تتطلب إدارة المخاطر التزام ودعم القيادة لبرنامج إدارة المخاطر عبر إنشاء هياكل حوكمة لتحديد الأدوار والمسؤوليات في الشركة والإشراف عليها.

RCO 001 - تتولى أعلى سلطة في الشركة المسؤولية عن برنامج إدارة المخاطر، وتلتزم بدعم برنامج إدارة المخاطر وتنفيذه وتحسينه باستمرار، من خلال:

- أ- إنشاء رؤية قيادية مشتركة حول المخاطر.
- ب- التوافق مع أهداف الشركة وقيمها وثقافتها.
- ج- توفير الموارد المطلوبة لتنفيذ ومتابعة برنامج إدارة المخاطر.
- د- تمكين آليات التواصل عن المخاطر من خلال القنوات المناسبة لزيادة الوعي وتشجيع ثقافة التركيز على المخاطر.
- هـ- اعتماد سياسة إدارة المخاطر.

RCO 002 - يجب على أعلى سلطة في الشركة ضمان الفصل في المهام بين الجهة التي تتولى إدارة المخاطر وبين المراجعة الداخلية ووحدات الرقابة الأخرى.

RCO 003 - يجب على أعلى سلطة في الشركة إنشاء لجنة توجيهية لإدارة المخاطر والتي بدورها تقوم بتوجيه برنامج إدارة المخاطر، وترفع اللجنة تقاريرها إلى أعلى سلطة في الشركة.

RCO 004 - يجب على اللجنة التوجيهية إعداد ميثاق يتضمن الأدوار والمسؤوليات ونماذج الحوكمة.

RCO 005 - يجب تمثيل هيكل الشركة والإدارات الهامة ذات العلاقة في اللجنة التوجيهية.

RCO 006 - يجب أن يتولى أحد أعضاء الإدارة العليا، ممن لديهم المعرفة ذات الصلة بإدارة المخاطر قيادة اللجنة التوجيهية.

RCO 007 - يجب على اللجنة التوجيهية إنشاء وتمكين جهة لإدارة المخاطر تضم المهارات والكفاءات اللازمة لإعداد وتطوير برنامج إدارة المخاطر وتنفيذه ومراجعته وتحديثه.

RCO 008 - يجب على أعلى سلطة في الشركة تقييم واعتماد ميزانية رسمية سنوية لبرنامج إدارة المخاطر والأنشطة المرتبطة به، والعمل على تنفيذه وتحديثه وتحسينه.

RCO 009 - يجب على الجهة التي تتولى إدارة المخاطر إعداد وتطوير برنامج إدارة المخاطر في الشركة بما يتوافق مع حجمها ونطاق عملها وأهدافها ومصفوفة الصلاحيات بها.

RCO 010 - يجب اعتماد برنامج إدارة المخاطر من قبل اللجنة التوجيهية.

RCO 011 - يجب أن تتبع الجهة التي تتولى إدارة المخاطر من الناحية الوظيفية للجنة التوجيهية.

RCO 012 - يجب على الجهة التي تتولى إدارة المخاطر التأكد من مناسبة ترشيحات الإدارات المشاركة لسفراء برنامج إدارة المخاطر لتنسيق وتنفيذ الأنشطة والمهام المتعلقة بالبرنامج.

RCO 013 - يجب على الجهة التي تتولى إدارة المخاطر إعداد وتطوير وتنفيذ ومشاركة سياسة إدارة المخاطر المعتمدة بالشركة سنوياً أو عند حدوث تغييرات كبيرة في بيئتها التشغيلية.

RCO 014 - يجب على الجهة التي تتولى إدارة المخاطر إعداد دليل إجراءات منبثق من سياسة إدارة المخاطر.

3. التخطيط والإعداد والتنفيذ

هدف المجال: تتطلب إدارة المخاطر الفعالة من الشركة الاستعداد للمخاطر التي قد تنشأ بسبب البيئة المتغيرة للمخاطر في القطاع، ويشمل ذلك تقييم المستوى المقبول للمخاطر وإعداد استراتيجيات للمخاطر وخطة تنفيذها.



3-1 استراتيجية المخاطر وخطة التنفيذ

تحتم التقنيات الناشئة والابتكار والاضطرابات المحتملة داخل قطاع الاتصالات وتقنية المعلومات على الشركة ضرورة المراجعة المستمرة للمستوى المقبول للمخاطر واستراتيجية المخاطر بالشركة.

SPI 001 - يجب على أعلى سلطة في الشركة تحديد قدرة الشركة القصوى على تحمل المخاطر (Risk Capacity).

SPI 002 - يجب على اللجنة التوجيهية بالتعاون مع الجهة التي تتولى إدارة المخاطر إعداد المستوى المقبول للمخاطر (Risk Appetite) الذي يوضح مستوى المخاطر الذي تتقبله الشركة في سعيها لتحقيق أهدافها وغاياتها، والحدود القصوى لتحمل كل خطر (Risk Tolerance).

SPI 003 - يجب على أعلى سلطة في الشركة مراجعة واعتماد المستوى المقبول للمخاطر والحدود القصوى لتحمل كل خطر.

SPI 004 - يجب على الجهة التي تتولى إدارة المخاطر وملأك المخاطر إعداد مؤشرات المخاطر الرئيسية.

SPI 005 - يجب على الجهة التي تتولى إدارة المخاطر إعداد استراتيجية وبرنامج إدارة المخاطر للشركة مع الأخذ في الاعتبار المستوى المقبول للمخاطر والحدود القصوى لتحمل الخطر.

SPI 006 - يجب على اللجنة التوجيهية لإدارة المخاطر اعتماد استراتيجية وبرنامج إدارة المخاطر وإخطار الأطراف المعنية بذلك.

SPI 007 - يتعين على اللجنة التوجيهية لإدارة المخاطر مراجعة استراتيجية إدارة المخاطر سنوياً أو عند حدوث تغييرات كبيرة مع مراعاة التقنية الناشئة والاضطرابات المحتملة في القطاع.

SPI 008 - يجب على ملاك المخاطر ترشيح سفراء المخاطر لتنسيق أنشطة مخاطر الإدارات والأقسام المتعلقة ببرنامج إدارة المخاطر وتنفيذها وإبلاغها للجهة التي تتولى إدارة المخاطر.

3-2 تحليل أصحاب المصلحة

يجب تحديد أصحاب المصلحة الرئيسيين واستشارتهم بشأن المخاطر في الشركة. ويتم أخذ مريثات أصحاب المصلحة في الاعتبار عند إعداد استراتيجيات المخاطر، وكذلك عند اتخاذ القرارات القائمة على المخاطر.

SPI 009 - يجب على الجهة التي تتولى إدارة المخاطر تحديد أصحاب المصلحة الرئيسيين ويجب أن تشمل:

- أ- وزارة الاتصالات وتقنية المعلومات.
- ب- هيئة الاتصالات وتقنية المعلومات.
- ج- الموردون المهمون.
- د- مقدمو خدمات الاتصالات وتقنية المعلومات.
- هـ- مزودو خدمات البنية التحتية.
- و- الهيئات التشريعية والتنظيمية الأخرى ذات الصلة.

SPI 010 - يجب على الجهة التي تتولى 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 واهتمامهم وتأثيرهم على الشركة.

SPI 011 - يجب على الجهة التي تتولى إدارة المخاطر بناءً على مصفوفة أصحاب المصلحة إعداد خطة أصحاب المصلحة للحفاظ على العلاقات وتقليل المخاطر من خلال:

- أ- تحديد نوع الاتصال، وقنوات الإتصال، والتكرار المطلوب.
- ب- التشاور مع أصحاب المصلحة الرئيسيين لتحديد التوقعات والاعتبارات من أجل إعداد استراتيجية المخاطر للشركة.
- ج- الحصول على مريثات دورية ومناسبة حول برنامج إدارة المخاطر من أصحاب المصلحة من خلال المشاركة والتغذية الراجعة.



4. التقييم والمعالجة

هدف المجال: تقييم المخاطر ومعالجتها للتخفيف من حدتها أو استغلالها داخل الشركة هو الأساس لبرنامج إدارة المخاطر ومفتاح لاستراتيجيات المخاطر المستقبلية.

1-4 تقييم المخاطر

يشمل تقييم المخاطر الأنشطة التي تسمح للشركة بتحديد المخاطر الحالية والمستجدة وتحليلها وتقديرها ومعالجتها.

RAM 001 - يجب على الجهة التي تتولى إدارة المخاطر إعداد منهجية منظمة وموحدة لتقييم المخاطر بما يتوافق مع استراتيجية وبرنامج المخاطر واعتمادها من قبل اللجنة التوجيهية لإدارة المخاطر.

RAM 002 - يجب أن تغطي منهجية تقييم المخاطر العوامل التي تمنع أو تعيق الشركة من تحقيق أهدافها على المدى القصير والمتوسط والطويل على أن تتضمن المنهجية ما يلي:

- أ- تحديد المخاطر.
- ب- تحليل المخاطر.
- ج- تقدير المخاطر.

RAM 003 - يجب على الجهة التي تتولى إدارة المخاطر تحديد وتوثيق المخاطر على المستويات الاستراتيجية والتشغيلية ومستوى إجراءات العمل الحساسة.

RAM 004 - يجب على الجهة التي تتولى إدارة المخاطر تقييم المخاطر بما يشمل موارد ومنتجات وخدمات الاتصالات وتقنية المعلومات، وفقاً لمنهجية تقييم المخاطر.

RAM 005 - يجب على الجهة التي تتولى إدارة المخاطر تحديد دورية تكرار عملية تقييم المخاطر بما في ذلك:

- أ- مستوى المخاطر (المستوى الاستراتيجي والتشغيلي وإجراءات العمل الحساسة).
- ب- التغيرات في البيئة الداخلية والخارجية للشركة.
- ج- إطلاق منتجات وخدمات الاتصالات وتقنية المعلومات الجديدة.

RAM 006 - يجب على الجهة التي تتولى إدارة المخاطر إعداد وتوثيق وتحديث نتائج تقييم المخاطر في سجل مركزي للمخاطر.

RAM 007 - يجب على اللجنة التوجيهية لإدارة المخاطر مراجعة واعتماد نتائج تقييم المخاطر.

1-1-4 تحديد المخاطر

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

RAM 008 - يجب على الجهة التي تتولى إدارة المخاطر التأكد من قيام ملاك وسفراء المخاطر بتحديد المخاطر وبيان أسبابها وتأثيرها بما يتوافق مع منهجية تقييم المخاطر وأهداف الشركة.

RAM 009 - يجب على الجهة التي تتولى إدارة المخاطر أن تقوم بمراجعة واعتماد نتائج تحديد المخاطر بما يتوافق مع منهجية تقييم المخاطر.

RAM 010 - يجب على الجهة التي تتولى إدارة المخاطر إعداد وتطوير إجراءات، ضمن عملية تحديد المخاطر، لضمان قيام إدارة الموارد البشرية بتحديد وتصنيف وتوثيق المهارات اللازمة التي تقوم بإدارة الخدمات والوظائف الهامة.

RAM 011 - يجب على الجهة التي تتولى إدارة المخاطر إعداد وتطوير إجراءات، ضمن عملية تحديد المخاطر، لضمان تحديد أوجه الاعتمادية الهامة داخل سلسلة قيم الاتصالات وتقنية المعلومات في الشركة من خلال تقييم الأثر وتحديد مدى توفر الاستراتيجيات اللازمة لتخفيف الخسارة المحتملة أو الحد من هذه الاعتماديات.



RAM 012 - يجب على الجهة التي تتولى إدارة المخاطر إعداد وتطوير إجراءات، ضمن عملية تحديد المخاطر، لضمان قيام الشركة بتحليل سلسلة الإمداد لقطاع الاتصالات وتقنية المعلومات وتحديد الموردين الرئيسيين للحفاظ على الخدمات الرئيسية.

RAM 013 - يجب على الجهة التي تتولى إدارة المخاطر التأكد من تحديد المخاطر المتعلقة باستمرارية الأعمال على مستوى الشركة فيما يتعلق بموارد ومنتجات وخدمات الاتصالات وتقنية المعلومات.

4-1-2 تحليل المخاطر

عملية تحليل المخاطر المحددة لقياس المخاطر الكامنة، وهو مستوى المخاطر المحدد قبل النظر في الضوابط الحالية.

RAM 014 - يجب على الجهة التي تتولى إدارة المخاطر التأكد من قيام ملاك وسفراء المخاطر بإجراء تحليل للمخاطر وفقًا لمنهجية تقييم المخاطر المعتمدة من أجل:

- أ- قياس المخاطر الكامنة التي تواجهها الشركة لكل خطر محدد، بما في ذلك الاحتمالية والتأثير والتصنيف الصحيح للخطر.
- ب- توثيق وتقييم الضوابط الحالية بالشركة.
- ج- التشاور مع أصحاب المصلحة الرئيسيين لفهم توقعاتهم.

RAM 015 - يجب على الجهة التي تتولى إدارة المخاطر أن تقوم بمراجعة واعتماد تحليل المخاطر بما يتوافق مع منهجية تقييم المخاطر.

4-1-3 تقدير المخاطر

عملية قياس المخاطر المتبقية بعد الأخذ بعين الاعتبار الضوابط الحالية بالشركة.

RAM 016 - يجب على الجهة التي تتولى إدارة المخاطر التأكد من قيام ملاك وسفراء المخاطر بإجراء تقدير للمخاطر وفقًا لمنهجية تقييم المخاطر المعتمدة من أجل:

- أ- تقييم فاعلية وكفاية الضوابط الحالية.
- ب- تقييم المخاطر المتبقية التي تواجهها الشركة لكل خطر محدد.
- ج- تحديد ما إذا كانت المخاطر المتبقية ضمن نطاق حدود تحمل الخطر.
- د- تحديد استراتيجية الاستجابة للمخاطر.

RAM 017 - يجب على الجهة التي تتولى إدارة المخاطر أن تقوم بمراجعة واعتماد تقدير المخاطر بما يتوافق مع منهجية تقييم المخاطر.

4-2 معالجة المخاطر

معالجة المخاطر هي عملية تخفيف حدة المخاطر المتبقية ومعالجتها.

RAM 018 - يجب على الجهة التي تتولى إدارة المخاطر التأكد من قيام ملاك وسفراء المخاطر بإعداد وتطوير خطط معالجة المخاطر وفقًا لاستراتيجية الاستجابة للمخاطر إما بقبول المخاطر المحددة أو معالجتها أو نقلها أو إنهاؤها أو استثمارها.

RAM 019 - يجب على الجهة التي تتولى إدارة المخاطر تقييم خطط معالجة المخاطر المقترحة من قبل ملاك وسفراء المخاطر وتقديم التوجيه فيما يتعلق بهذه الخطط.

RAM 020 - يجب على اللجنة التوجيهية لإدارة المخاطر أن تقوم بمراجعة واعتماد خطط معالجة المخاطر المقترحة، وتحديد الملاك والجهات المسؤولة عن تنفيذها.

RAM 021 - يجب على الجهة التي تتولى إدارة المخاطر التأكد من قيام ملاك المخاطر بتوثيق خطط معالجة طارئة للمخاطر حال وقوعها.

RAM 022 - يجب على الجهة التي تتولى إدارة المخاطر التأكد من وجود خطط لاستمرارية الأعمال على مستوى الشركة لاستمرارية موارد ومنتجات وخدمات الاتصالات وتقنية المعلومات.



5. مراقبة وتقييم البرنامج

هدف المجال: على الشركة مراقبة المخاطر والتقدم المحقق نحو إدارة المخاطر ضمن المستوى المقبول في الشركة.

1-5 المراقبة

تعزز مراقبة المخاطر ثقافة المخاطر داخل الشركة وتسمح بإدارة المخاطر المحددة بشكل استباقي والتكيف مع الظروف المتغيرة.

MON 001 - يجب على اللجنة التوجيهية لإدارة المخاطر مراقبة مؤشرات المخاطر وخطط معالجة المخاطر، والتغيرات في بيئة المخاطر الداخلية والخارجية، والامتثال التشريعي والتنظيمي.

MON 002 - يجب على الجهة التي تتولى إدارة المخاطر مراقبة تنفيذ خطط معالجة المخاطر للتأكد من معالجة المخاطر المحددة بشكل فاعل.

2-5 تقييم البرنامج

على الشركة تقييم فاعلية برنامج إدارة المخاطر لتحديد التحسينات والتطويرات المطلوبة.

MON 003 - يجب على أعلى سلطة في الشركة التأكد من وجود عملية محددة وموضوعية لتقييم برنامج إدارة المخاطر بشكل دوري.

MON 004 - يجب على الجهة التي تتولى إدارة المخاطر توثيق وتحليل وإبلاغ الدروس المستفادة من المخاطر التي حدثت والمتغيرات الداخلية والخارجية.

3-5 ضمان التكاملية

يشير ضمان التكاملية إلى نهج منسق على مستوى الشركة يتضمن مستويات مختلفة من التأكيد لتقليل المخاطر. ويساهم تعدد مستويات التأكيد في تعزيز المساءلة وضمان مراقبة المخاطر ومراجعتها على مستوى الشركة.

MON 005 - يجب على أعلى سلطة في الشركة التأكد من وجود تكامل وتنسيق فعال بين خطوط الدفاع المختلفة.

MON 006 - يجب على الجهة التي تتولى إدارة المخاطر إعداد وتطوير آلية لضمان التعاون بين إدارة المخاطر والمراجعة الداخلية والامتثال ووحدات الرقابة الأخرى لدعم بعضها البعض في تنفيذ مسؤوليات التأكيد المتكامل.

6. الإبلاغ والتواصل

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

REP 001 - يجب على الجهة التي تتولى إدارة المخاطر إعداد وتطوير آلية للإبلاغ والتواصل عن المخاطر في برنامج إدارة المخاطر لأصحاب المصلحة.

REP 002 - يجب على الجهة التي تتولى إدارة المخاطر إعداد مصفوفة صلاحيات تنظم التواصل مع أصحاب المصلحة المعنيين في برنامج إدارة المخاطر.



7. الاستدامة

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

1-7 ثقافة المخاطر

تعزز ثقافة المخاطر الالتزام والتعاون والوعي.

RSU 001 - يجب على أعلى سلطة في الشركة واللجنة التوجيهية تشجيع ودعم برنامج إدارة المخاطر من خلال قنوات التواصل المتاحة.

RSU 002 - يجب على أعضاء الإدارة العليا وملاك وسفراء المخاطر المشاركة والمساهمة بفاعلية في برنامج إدارة المخاطر.

2-7 التدريب والتوعية

يؤدي التدريب والتوعية إلى رفع ثقافة إدارة المخاطر وزيادة نضجها بالشركة.

RSU 003 - يجب على الجهة التي تتولى إدارة المخاطر التنسيق مع الجهة المختصة في الشركة لإعداد وتنفيذ خطة التدريب على إدارة المخاطر بناءً على تقييم سنوي لاحتياجات التدريب.

RSU 004 - يجب على الجهة التي تتولى إدارة المخاطر إعداد وتطوير وتنفيذ برنامج شامل للتوعية بإدارة المخاطر ومراجعتها وتحديثه بشكل دوري.

RSU 005 - يجب على الجهة التي تتولى إدارة المخاطر تقييم فاعلية برامج التدريب والتوعية الخاصة ببرنامج إدارة المخاطر وتحديثها بشكل دوري.

3-7 التنسيق

يعزز التكامل بين برنامجي إدارة المخاطر وإدارة استمرارية الأعمال داخل الشركة من أداء كلا البرنامجين؛ ويعود بالنفع على الشركة.

RSU 006 - يجب على الجهات التي تتولى إدارة المخاطر وإدارة استمرارية الأعمال 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 مجالات إدارة المخاطر وبنود السياسة المرتبطة بها بناءً على الممارسات والمعايير والإرشادات الرائدة، ويشمل ذلك:

- لجنة المنظمات الراعية (COSO) - إطار إدارة المخاطر المؤسسية (2017).
- المنظمة الدولية للمعايير (ISO) المعيار 31000 : 2018 - إدارة المخاطر - الإرشادات.
- معهد إدارة المخاطر IRM.
- تقرير King IV عن حوكمة الشركات.
- هيئة السوق المالية: لائحة حوكمة الشركات في المملكة العربية السعودية.

محرر



الملحق ب: الاختصارات

يقدم (الجدول 2) مرجعاً للاختصارات ومعانيها المستخدمة في هذه السياسة:

الجدول 2: الاختصارات

الاختصار	التعريف
BCRM	إدارة استمرارية الأعمال
CITC	هيئة الاتصالات وتقنية المعلومات
COSO	لجنة رعاية المنظمات (إطار تقييم أنظمة الرقابة الداخلية)
HR	الموارد البشرية
ICT	الاتصالات وتقنية المعلومات
ISO	المنظمة الدولية للمعايير
KRI	مؤشرات المخاطر الرئيسية
MCIT	وزارة الاتصالات وتقنية المعلومات
NISS	الاستراتيجية الوطنية لأمن المعلومات
NRU	وحدة المخاطر الوطنية
NTP	برنامج التحول الوطني
RA	تقييم المخاطر
RM	إدارة المخاطر
RMBCC	مركز إدارة المخاطر واستمرارية الأعمال



الملحق ج: المصطلحات والتعريفات

يقدم (الجدول 3) مرجعاً للمصطلحات والتعريفات المستخدمة في هذه السياسة:

الجدول 3: المصطلحات والتعريفات

المصطلح	الوصف
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 الشركة سواء كانت صلاحيات مالية أو إدارية أو تشغيلية. كما يبين نوع الصلاحية الممنوحة سواء كانت أعداد أو مراجعة أو اعتماد.
إدارة استمرارية الأعمال والقدرة على الصمود (Business Continuity and Resilience Management)	قدرة الشركة أو الموظفين أو النظام أو شبكة الاتصالات أو النشاط أو العملية على استيعاب أثر انقطاع أو خسارة الأعمال والاستمرار في تقديم مستوى مقبول للخدمة.
ضمان التكاملية (Combined Assurance)	نهج منسق (متكامل) يتم تطبيقه في الشركة للتأكد من أن المخاطر الرئيسية تدار بشكل مناسب داخل الشركة.
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 الشركة.
المجالات (Domains)	المجالات الموجودة في سياسة إدارة مخاطر الشركات المرخصة في قطاع الاتصالات وتقنية المعلومات والتي تساهم في النهج الشامل والمنظم لإدارة المخاطر.
إدارة المخاطر المؤسسية (Enterprise Risk Management)	نهج يتم تطبيقه على مستوى الشركة لإدارة جميع المخاطر التي تتعرض لها الشركة.
وظيفياً (Functionally)	الأنشطة المرتبطة بتنفيذ المهام الوظيفية ضمن برنامج إدارة المخاطر وتشمل المسؤولية النهائية للحصول على الموافقات النهائية لمخرجات برنامج إدارة المخاطر من اللجنة التوجيهية.
أعلى سلطة (Highest Authority)	تعني الجهة ذات الصلاحية والحق في استخدام الموارد وتخصيصها بكفاءة، واتخاذ القرارات وإعطاء الأوامر لتحقيق الأهداف التنظيمية.
الشركات المرخصة في قطاع الاتصالات وتقنية المعلومات (ICT Licensed Organizations)	الشركات الحاصلة والحاملة لرخصة سارية في خدمات الاتصالات وتقنية المعلومات، صادرة عن هيئة الاتصالات وتقنية المعلومات.
موارد ومنتجات وخدمات الاتصالات وتقنية المعلومات (ICT Resources, Products and Services)	الموارد والمنتجات والخدمات الخاصة بالاتصالات وتقنية المعلومات، لتمكين الشركة من تحقيق أهدافها ومهامها على النحو المحدد في استراتيجيتها.
الاتصالات وتقنية المعلومات (Information and Communications Technology)	مجموعة متنوعة من الأدوات والموارد التقنية المستخدمة لنقل المعلومات أو تخزينها أو إنشائها أو مشاركتها أو تبادلها.
التأثير (Impact)	تأثير وعواقب المخاطر إذا وقعت.
المخاطر الكامنة (Inherent Risks)	هي المخاطر المتأصلة في الاعمال دون الأخذ بالاعتبار فاعلية الضوابط الحالية.



المصطلح	الوصف
الاعتمادية المتبادلة (Interdependency)	اعتماد شركتين أو أكثر من الشركات العاملة في قطاع الاتصالات وتقنية المعلومات على بعضها البعض لتوفير الخدمات و/أو التقنية.
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 الشركة.
الممارسة الرائدة (Leading Practices)	طريقة أو تقنية تم قبولها بشكل عام عوضاً عن البدائل الأخرى لأنها تحقق نتائج أصبحت 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.
المخاطر التشغيلية (Operational Risks)	المخاطر الهامة التي تؤثر على قدرة الشركة على تنفيذ خطتها الاستراتيجية.
مخاطر العمليات (Processes Risks)	المخاطر المرتبطة بالعمليات اليومية للشركة.
المخاطر المتبقية (Residual Risks)	تشير المخاطر المتبقية إلى مستوى المخاطر المتبقية بعد الأخذ بالاعتبار فاعلية الضوابط الحالية. وبمعنى آخر، التأثير الصافي للمخاطر الكامنة ومستوى فاعلية الضوابط.
الموارد (Resources)	جميع الموظفين، والمهارات، والبنية التحتية للتقنية، والمنتجات، والخدمات، والمباني، والإمدادات، والمعلومات (سواء كانت إلكترونية أم لا) التي يجب أن تتوفر لدى الشركة لاستخدامها، عند الحاجة، من أجل تسيير العمل وتحقيق أهدافها.
المخاطر (Risks)	حدث غير متوقع يمكن أن يؤثر على أهداف الشركة إيجاباً أو سلباً.
المستوى المقبول للمخاطر (Risk Appetite)	تعبير مختصر عن مقدار ونوع المخاطر التي تقبلها الشركة في إطار سعيها لتحقيق أهداف ونتائج أعمالها.
تقييم المخاطر (Risk Assessment)	عملية ممنهجة لتحديد المخاطر وتحليلها وتقييمها ومعالجتها لضمان إدارة المخاطر التي تواجهها الشركة بشكل مناسب لتحقيق أهداف العمل في النهاية.
القدرة القصوى على تحمل المخاطر (Risk Capacity)	الحد الأقصى من المخاطر التي يمكن أن تتحملها الشركة 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.
أحداث المخاطر (Risk Events)	أحداث المخاطر هي احتمالية أن يؤثر حدث غير متوقع سلباً على قدرة الشركات على الاستمرار في ظل الظروف العادية.
الجهة التي تتولى إدارة المخاطر (Risk Management Function)	الجهة المسؤولة عن الإدارة اليومية المستمرة لبرنامج إدارة المخاطر والأنشطة المرتبطة به.
سياسة إدارة المخاطر (Risk Management Policy)	نوايا واتجاهات الشركة، وفقاً لما حددته رسمياً إدارتها العليا فيما يتعلق بإدارة المخاطر.
اللجنة التوجيهية لإدارة المخاطر (Risk Management Steering Committee)	لجنة من صانعي القرارات (مثل قادة الأعمال وخبراء التقنية وإدارة المخاطر المكلفون بإعداد السياسة الاستراتيجية واتخاذ قرارات إدارة المخاطر للشركة، وتوفير الموارد اللازمة لتحقيق جميع أهداف برنامج إدارة المخاطر.
هيكل إدارة المخاطر (Risk Function Tower)	رسم توضيحي للمفاهيم الأساسية المرتبطة بمجالات إدارة المخاطر الموضحة في هذه السياسة.



المصطلح	الوصف
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.
معالجة المخاطر (Risk Mitigation)	يشير إلى الإجراءات المتخذة لتخفيف مستوى المخاطر وصولاً إلى مستوى مقبول. ويشار إليه أحياناً بمعالجة المخاطر.
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 بالشركة لتفعيل تنفيذ سياسة إدارة المخاطر وتحديد جميع متطلبات إدارة المخاطر التي تحتاج الشركة إلى تنفيذها.
الحدود القصوى لتحمل الخطر (Risk Tolerance)	الحد الأقصى المحدد للمخاطر (التعرض) التي تكون الشركة على استعداد لتحمله/قبوله فيما يتعلق بكل خطر تتعرض له.
الإدارة العليا (Senior Management)	أعلى مستوى للمدراء في الشركة، مباشرة تحت هيكل القيادة للشركة (أعلى سلطة).
الاستدامة (Sustainability)	ترسيخ ثقافة المخاطر في الشركة من خلال مبادرات التدريب والتوعية المستمرة.
سلسلة الإمداد (Supply Chain)	سلسلة من العمليات المتضمنة في إنتاج وتوزيع منتج أو خدمة.
المخاطر الاستراتيجية (Strategic Risks)	المخاطر التي تؤثر على استراتيجية عمل الشركة وأهدافها الاستراتيجية أو تنشأ عنها.
سلسلة القيم (Value Chain)	تشمل المساهمين والمطورين ومقدمي الخدمات والمستخدمين النهائيين في البنية التحتية غير النشطة/النشطة.
الوظائف الهامة (Key Positions)	وهي وظائف تساعد على تمكين استمرارية موارد الاتصالات وتقنية المعلومات ومنتجاتها وخدماتها والمساهمة في تحقيق الأهداف التنظيمية، وهي: - الوظائف القيادية - وظائف أمن المعلومات - الوظائف المتعلقة بإدارة الشبكات - الوظائف المتعلقة بإدارة البيانات والتطبيقات



نهاية الوثيقة