الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

ITU-T X.1054

(2012/09)

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن المعلومات والشبكات – إدارة الأمن

تكنولوجيا المعلومات – تقنيات الأمن – إدارة أمن المعلومات

التوصيـــة ITU-T X.1054

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.199–X.1
التوصيل البيني للأنظمة المفتوحة	X.299–X.200
التشغيل البيني للشبكات	X.399–X.300
أنظمة معالجة الرسائل	X.499–X.400
الدليـــل	X.599–X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.699–X.600
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.799–X.700
الأمن	X.849–X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.899–X.850
المعالجة الموزعة المفتوحة	X.999–X.900
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1029–X.1000
أمن الشبكة	X.1049–X.1030
إدارة الأمن	**X.1069–X.1050**
الخصائص البيومترية	X.1099–X.1080
تطبيقات وخدمات آمنة	
أمن البث المتعدد	X.1109–X.1100
أمن الشبكة المحلية	X.1119–X.1110
أمن الخدمات المتنقلة	X.1139–X.1120
أمن الويب	X.1149–X.1140
بروتوكولات الأمن	X.1159–X.1150
الأمن بين جهتين نظيرتين	X.1169–X.1160
أمن معرفات الهوية عبر الشبكات	X.1179–X.1170
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1199–X.1180
أمن الفضاء السيبراني	
الأمن السيبراني	X.1229–X.1200
مكافحة الرسائل الاقتحامية	X.1249–X.1230
إدارة الهوية	X.1279–X.1250
تطبيقات وخدمات آمنة	
اتصالات الطوارئ	X.1309-X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1339–X.1310
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1519–X.1500
تبادل مواطن الضعف/الحالة	X.1539–X.1520
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1549–X.1540
تبادل السياسات	X.1559–X.1550
طلب المعلومات الحدسية والمعلومات الأخرى	X.1569–X.1560
تعرف الهوية والاكتشاف	X.1579–X.1570
التبادل المضمون	X.1589–X.1580

لمزيد من التفاصيل، يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

المعيار الدولي ISO/IEC 27014
التوصيـــة ITU-T X.1054

تكنولوجيا المعلومات – تقنيات الأمن – إدارة أمن المعلومات

ملخص

تقدم التوصية ITU-T X.1054 | المعيار الدولي ISO/IEC 27014 إرشادات بشأن إدارة أمن المعلومات.

وقد أصبحت مسألة أمن المعلومات من المسائل الرئيسية بالنسبة إلى المنظمات. ولا يقتصر الأمر على زيادة في المتطلبات التنظيمية بل يمكن لفشل التدابير الأمنية المتعلقة بمعلومات المنظمة أن يؤثر مباشرة على سمعة المنظمة أيضاً.

ولذلك، فإن مجلس الإدارة مطالب على نحو متزايد، كجزء من مسؤوليات الإدارة التي تقع على عاتقه، بالإشراف على أمن المعلومات لضمان تحقيق أهداف المنظمة.

وبالإضافة إلى ذلك، تقيم إدارة أمن المعلومات صلة قوية بين مجلس إدارة المنظمة والإدارة التنفيذية والمسؤولين عن تنفيذ نظام إدارة أمن المعلومات وتشغيله.

وتوفر الولاية الضرورية لقيادة مبادرات أمن المعلومات في المنظمة برمتها.

وعلاوة على ذلك، فإن إدارة أمن المعلومات بطريقة فعالة تكفل تلقي مجلس الإدارة التقرير ذي الصلة – ضمن سياق الأعمال – حول الأنشطة المتعلقة بأمن المعلومات. ويمكّن ذلك من اتخاذ قرارات ذات صلة وفي الوقت المناسب حول مسائل أمن المعلومات لدعم الأهداف الاستراتيجية للمنظمة.

التسلسل التاريخي

الصيغة	التوصية	تاريخ الموافقة	لجنة الدراسات
1.0	ITU-T X.1054	2012/09/07	17

تمهيـــد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA)، التي تجتمع مرة كل أربع سنوات، المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار رقم 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظـــة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً) ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

المعيـــار الـــدولي

توصية قطاع تقييس الاتصالات

تكنولوجيا المعلومات – تقنيات الأمن – إدارة أمن المعلومات

1 مجال التطبيق

تقدم هذه التوصية | المعيار الدولي مفاهيم وإرشادات بشأن مبادئ وعمليات إدارة أمن المعلومات تمكيناً للمنظمات من تقييم هذه الإدارة وتوجيهها ورصدها.

ويُطبّق هذا التوصية | المعيار الدولي على المنظمات بأنواعها وأحجامها كافة.

2 المراجع المعيارية

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية | المعيار الدولي. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع إلى المراجعة، نحث جميع المستعملين لهذه التوصية على السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الواردة أدناه. ويحتفظ أعضاء اللجنة الكهرتقنية الدولية والمنظمة الدولية للتوحيد القياسي بسجلات بالمعايير الدولية سارية الصلاحية. ويحتفظ مكتب تقييس الاتصالات في الاتحاد الدولي للاتصالات بقائمة بتوصيات القطاع السارية الصلاحية.

– المعيار الدولي ISO/IEC 27000:2009، *تكنولوجيا المعلومات – تقنيات الأمن – أنظمة إدارة أمن المعلومات – نظرة عامة ومصطلحات*.

3 تعاريف

لأغراض هذه التوصية | المعيار الدولي، تنطبق المصطلحات والتعاريف الواردة في المعيار الدولي ISO/IEC 27000 والتعاريف التالية:

1.3 الإدارة التنفيذية: عبارة عن شخص أو مجموعة من الأفراد المكلفين من مجلس الإدارة بمسؤولية تنفيذ استراتيجيات وسياسات رامية إلى تحقيق أهداف المنظمة.

الملاحظـــة 1 – الإدارة التنفيذية جزء من الإدارة العليا: ولتوضيح الأدوار، يفرق هذا المعيار بين مجموعتين ضمن الإدارة العليا: مجلس الإدارة والإدارة التنفيذية.

الملاحظـــة 2 – قد تشمل الإدارة التنفيذية كبار الموظفين التنفيذيين وكبار الموظفين الماليين (CFO) وكبار الموظفين التشغيليين (COO) وكبار الموظفين الإعلاميين (CIO)، وكبار موظفي أمن المعلومات (CISO) وما شابه.

2.3 مجلس الإدارة: عبارة عن شخص أو مجموعة من الأفراد المسؤولين عن أداء المنظمة وامتثالها.

ملاحظـــة – يعتبر مجلس الإدارة جزءاً من الإدارة العليا: ولتوضيح الأدوار، يفرق هذا المعيار بين مجموعتين ضمن الإدارة العليا: مجلس الإدارة والإدارة التنفيذية.

3.3 إدارة أمن المعلومات: نظام يتم من خلاله توجيه الأنشطة المتصلة بأمن المعلومات والإشراف على هذه الأنشطة في المنظمة.

4.3 صاحب المصلحة: أي شخص أو منظمة يمكن أن يؤثر في نشاط تضطلع به المنظمة، أو يتأثر بهذا النشاط، أو يعتبر نفسه متأثراً به.

ملاحظـــة – صانع القرار يمكن أن يكون من بين أصحاب المصلحة.

4 المفاهيم

1.4 معلومات عامة

يلزم أن توفّق إدارة أمن المعلومات بين أهداف واستراتيجيات كل من أمن المعلومات وقطاع الأعمال، وأن تشترط الامتثال للتشريعات واللوائح والعقود، وينبغي أن تُقيّم وتُحلّل وتُنفّذ باتباع نهج لإدارة المخاطر، بدعم من نظام للرقابة الداخلية.

ويتكفل مجلس الإدارة في نهاية المطاف بالمسؤولية عن قرارات المنظمة وأدائها، وينصب اهتمامه في مجال أمن المعلومات على ضمان نجاعة النهج الذي تتبعه المنظمة في تحقيق أمن المعلومات وفعالية هذا النهج ومقبوليته، مع إيلاء المراعاة الواجبة لتوقعات العديد من أصحاب المصلحة الذين تختلف قيمهم واحتياجاتهم.

2.4 الأهداف

فيما يلي الأهداف التي تصبو إدارة أمن المعلومات إلى بلوغها:

- مواءمة استراتيجيات أمن المعلومات مع استراتيجيات قطاع الأعمال وأهدافها (مواءمة استراتيجية)،
- تحقيق فوائد لمجلس الإدارة وأصحاب المصلحة (تحقيق الفوائد)،
- ضمان معالجة المخاطر المحيقة بأمن المعلومات معالجة وافية (المساءلة).

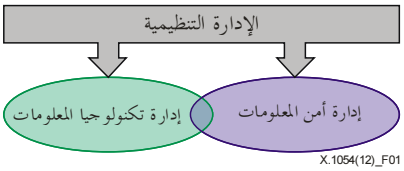
3.4 النتائج المرجوة

فيما يلي النتائج المرجو تحقيقها من التنفيذ الفعال لإدارة أمن المعلومات:

- تكوين مجلس الإدارة لرؤية عن حالة أمن المعلومات،
- اتباع نهج مرن في اتخاذ القرارات المتعلقة بما يحيق بالمعلومات من مخاطر،
- توظيف استثمارات كفؤة وفعالة في مجال أمن المعلومات،
- الامتثال للمتطلبات الخارجية (القانونية والتنظيمية والتعاقدية).

4.4 العلاقة بين الإدارات

هناك العديد من نماذج الإدارة الأخرى المطبقة داخل المنظمة، من قبيل إدارة تكنولوجيا المعلومات والإدارة التنظيمية. ويشكّل كل واحد من نماذج الإدارة هذه جزءاً لا يتجزأ من إدارة المنظمة، التي تشدد على أهمية مواءمة أهدافها مع أهداف قطاع الأعمال. وعادة ما يستفيد مجلس الإدارة من بلورة رؤية شاملة ومتكاملة للنموذج الذي يطبقه في مجال الإدارة، والذي ينبغي أن تشكّل إدارة أمن المعلومات جزءاً منه. وتتداخل أحياناً مجالات تطبيق نماذج الإدارة، إذ يبيّن مثلاً الشكل 1 أدناه العلاقة بين إدارة أمن المعلومات وإدارة تكنولوجيا المعلومات.



الشكل 1 – العلاقة بين إدارة أمن المعلومات وإدارة تكنولوجيا المعلومات

ومع أن المجال الشامل لتطبيق إدارة تكنولوجيا المعلومات يهدف إلى توفير الموارد اللازمة للحصول على المعلومات ومعالجتها وتخزينها ونشرها، فإن مجال تطبيق إدارة أمن المعلومات يرمي كذلك إلى تأمين سرية هذه المعلومات وسلامتها وتوافرها. ويلزم معالجة مخططي الإدارة كليهما باتباع عمليات الإدارة التالية: التقييم والإدارة والرصد (EDM). بيد أن إدارة أمن المعلومات تتطلب العملية الداخلية الإضافية "الاتصال".

وتبيّن الفقرة 5 أدناه المهام التي يلزم أن ينهض بها مجلس الإدارة في مجال إرساء إدارة أمن المعلومات، وهي مهام ذات صلة أيضاً بمتطلبات الإدارة المحددة في المعيار الدولي ISO/IEC 27001، وكذلك بسائر المعايير الأخرى المنخرطة ضمن مجموعة نظام إدارة أمن المعلومات (ISMS) المشار إليها في البيبليوغرافيا.

5 المبادئ والعمليات

1.5 نظرة عامة

تبيّن هذه الفقرة المبادئ والعمليات التي تشكّل معاً إدارة أمن المعلومات. ومبادئ إدارة أمن المعلومات هي عبارة عن قواعد مقبولة بشأن اتخاذ إجراءات أو أعمال إدارية تقوم مقام دليل لتنفيذ الإدارة. أما عمليات إدارة أمن المعلومات فهي تبيّن مجموعة من المهام التي تمكّن من إدارة أمن المعلومات والعلاقات التي تربطها، كما تثبت وجود علاقة بين إدارة أمن المعلومات وتدبير شؤون هذا الأمن. وهذان العنصران توضحهما الفقرات الفرعية التالية.

2.5 المبادئ

تلبية احتياجات أصحاب المصلحة وتحقيق فوائد لهم جزء لا يتجزأ من تكليل أمن المعلومات بالنجاح على المدى الطويل. وتحقيقاً لأهداف الإدارة المتمثلة في توثيق مواءمة أمن المعلومات مع أهداف قطاع الأعمال وتحقيق فوائد لأصحاب المصلحة، تحدد هذه الفقرة الفرعية ستة مبادئ ذات منحى إجرائي.

وترسي المبادئ أساساً متيناً لتنفيذ أنشطة إدارة أمن المعلومات. ويشير بيان كل مبدأ إلى ما سيحدث من أمور، ولكن من دون بيان كيفية تطبيق المبادئ أو وقت تطبيقها أو من يتولى تطبيقها، لأن هذه الجوانب تتوقف على طبيعة المنظمة التي تطبقها. وينبغي أن يشترط مجلس الإدارة تطبيق هذه المبادئ، وأن يعيّن شخصاً يتحلى بالقدر اللازم من المسؤولية والمساءلة والسلطة لتطبيقها.

المبدأ 1: إرساء أمن المعلومات على نطاق المنظمة ككل

ينبغي أن تكفل إدارة أمن المعلومات شمولية وتكامل ما يُضطلع به من أنشطة في مجال أمن المعلومات. ولا بد من التعامل مع أمن المعلومات على المستوى التنظيمي في إطار مراعاة عملية صنع القرار لوجهات النظر المتعلقة بالأعمال، وأمن المعلومات، وكافة الجوانب الأخرى ذات الصلة. وينبغي توثيق عرى تنسيق الأنشطة المتعلقة بالأمن المادي والمنطقي.

وإرساء للأمن على نطاق المنظمة ككل، ينبغي تحديد المسؤولية والمساءلة عن أمن المعلومات في كامل طائفة الأنشطة التي تضطلع بها المنظمة، وهو أمر عادة ما يمتد نطاقه ليتعدى "الحدود" المنظورة للمنظمة عموماً، ومثال ذلك المعلومات التي تتولى أطراف خارجية تخزينها أو نقلها على حد سواء.

المبدأ 2: اعتماد نهج قائم على إدارة المخاطر

ينبغي أن تستند إدارة أمن المعلومات إلى قرارات قائمة على إدارة المخاطر. ولا بد من أن يُبنى تحديد المقدار الكافي من الأمن على المخاطر التي تتحملها المنظمة، بما فيها مخاطر خسارة الميزة التنافسية والامتثال والمسؤولية والاضطرابات التشغيلية والإضرار بالسمعة والخسائر المالية.

وينبغي أن يكون اعتماد النهج المناسب لإدارة المخاطر متسقاً ومكملاً للنهج الشامل الذي تتبعه المنظمة في إدارة المخاطر. وينبغي تحديد المستويات المقبولة من أمن المعلومات استناداً إلى مستوى الخطورة الذي تكون المنظمة على استعداد لتحمله، بما فيها مخاطر خسارة الميزة التنافسية والامتثال والمسؤولية والاضطرابات التشغيلية والإضرار بالسمعة والخسائر المالية. ولا بد أن يخصص مجلس الإدارة الموارد اللازمة لتنفيذ أساليب إدارة المخاطر المتعلقة بالمعلومات.

المبدأ 3: تحديد وجهة القرارات الاستثمارية

ينبغي أن تقوم إدارة أمن المعلومات بوضع استراتيجية استثمارية في مجال أمن المعلومات مبنية على نتائج الأعمال المنجزة، تؤدي إلى مواءمة متطلبات قطاع الأعمال مع متطلبات أمن المعلومات على الأمدين القصير والطويل تلبية لاحتياجات أصحاب المصلحة الحالية والمتوقعة.

وتحقيقاً للحد الأمثل من استثمارات أمن المعلومات التي تدعم بلوغ أهداف المنظمة، ينبغي أن يكفل مجلس الإدارة دمج أمن المعلومات في عمليات التنظيم القائمة فيما يتعلق بالنفقات الرأسمالية والتشغيلية، وذلك لأغراض الامتثال على الصعيدين القانوني والتنظيمي والإبلاغ عن المخاطر.

المبدأ 4: ضمان التوافق مع المتطلبات الداخلية والخارجية

ينبغي لإدارة أمن المعلومات أن تكفل توافق سياسات وممارسات أمن المعلومات مع التشريعات واللوائح الإلزامية ذات الصلة، إلى جانب الشروط التجارية أو التعاقدية المتعهد بها والمتطلبات الداخلية والخارجية الأخرى.

ولمعالجة المسائل المتعلقة بالتوافق والامتثال، ينبغي لمجلس الإدارة أن يحصل على تأكيدات تثبت أن أنشطة أمن المعلومات تستوفي بشكل مرض متطلبات داخلية وخارجية عن طريق التكليف بإجراء عمليات تدقيق أمني مستقلة.

المبدأ 5: تدعيم بيئة إيجابية أمنياً

ينبغي بناء إدارة أمن المعلومات على سلوكيات إنسانية، ومنها الاحتياجات المستجدة لأصحاب المصلحة كافة، لأن السلوك الإنساني أحد العناصر الأساسية لدعم المستوى المناسب من أمن المعلومات. وإن لم تُنسّق الأهداف والأدوار والمسؤوليات والموارد في هذا المضمار بشكل كافٍ، فإنها قد تتعارض مع بعضها البعض وتسفر عن عجز في تحقيق أهداف قطاع الأعمال. لذا فإن التنسيق وتضافر جهود التوجيه بين مختلف أصحاب المصلحة أمر غاية في الأهمية.

وسعياً إلى إقامة ثقافة إيجابية بخصوص أمن المعلومات، فإن على مجلس الإدارة أن يطالب بالنهوض بأنشطة أصحاب المصلحة ودعمها وتنسيقها لتحقيق اتجاه متماسك في مجال أمن المعلومات. ويدعم ذلك تنفيذ برامج بشأن التثقيف بالجوانب الأمنية والتدريب عليها والتوعية بها.

المبدأ 6: مراجعة الأداء على أساس نتائج الأعمال

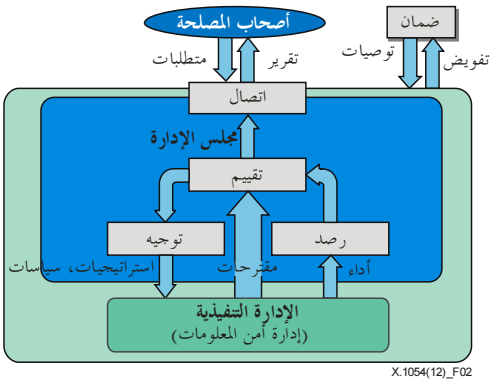
ينبغي لإدارة أمن المعلومات أن تكفل مواءمة النهج المتبع في حماية المعلومات مع الغرض المتمثل في دعم المنظمة لتحقيق المستويات المتفق عليها من أمن المعلومات. ولا بد من إبقاء الأداء الأمني بالمستويات اللازمة لتلبية المتطلبات الحالية والمستقبلية للأعمال.

ولمراجعة أداء أمن المعلومات من وجهة نظر الإدارة، ينبغي لمجلس الإدارة أن يُقيّم أداء أمن المعلومات على أساس آثاره على الأعمال، لا على أساس فعالية الضوابط الأمنية وكفاءتها حصراً. ويمكن تحقيق ذلك بإجراء مراجعات إلزامية لبرنامج لقياس الأداء معني بالرصد والتدقيق والتحسين لإقامة صلة بالتالي بين أداء أمن المعلومات وأداء الأعمال.

3.5 العمليات

1.3.5 نظرة عامة

يستعين مجلس الإدارة والإدارة التنفيذية بعمليات "التقييم" و"التوجيه" و"الرصد" و"الاتصال" لأغراض إدارة أمن المعلومات. وبالإضافة إلى ذلك، يُدلى في إطار عملية "الضمان" برأي مستقل وموضوعي حول إدارة أمن المعلومات والمستوى المحقق منه. ويبين الشكل 2 أدناه العلاقة بين هذه العمليات.



الشكل 2 – تنفيذ نموذج إدارة لأمن المعلومات

2.3.5 التقييم

"التقييم" هو عملية إدارة تدرس المحقق حالياً من الأهداف الأمنية وما يُتوقع تحقيقه منها على أساس العمليات الحالية والتغييرات المزمع إدخالها، وتحدد المواضع التي يلزم فيها إجراء أي تعديلات لتحسين بلوغ الأهداف الاستراتيجية في المستقبل.

ولكي ينفذ مجلس الإدارة عملية "التقييم"، ينبغي له أن يقوم بما يلي:

- ضمان أن تراعي مبادرات الأعمال المسائل المتعلقة بأمن المعلومات،
- الاستجابة لنتائج أداء أمن المعلومات، وتحديد الأولويات والشروع في اتخاذ ما يلزم من إجراءات.

ولكي تُنفذ الإدارة التنفيذية عملية "التقييم"، ينبغي لها أن تقوم بما يلي:

- ضمان أن يُقدم أمن المعلومات الدعم الكافي لبلوغ وصيانة أهداف الأعمال،
- تقديم مشاريع جديدة بشأن أمن المعلومات تحقق نتائج مهمة للمنظمة إلى مجلس الإدارة.

3.3.5 التوجيه

"التوجيه" هو عملية إدارة تمكّن مجلس الإدارة من إعطاء توجيهات حول أهداف أمن المعلومات والاستراتيجية التي يلزم تنفيذها بشأنه. ويمكن أن ينطوي التوجيه على إدخال تغييرات في مستويات توفير الموارد وتخصيصها وتحديد أولويات الأنشطة ومنح موافقات على السياسات وقبول مخاطر المواد ووضع خطط لإدارة المخاطر.

ولكي ينفذ مجلس الإدارة عملية "التوجيه"، ينبغي له أن يقوم بما يلي:

- تحديد مستوى المخاطر التي تتحملها المنظمة،
- الموافقة على استراتيجيات وسياسات أمن المعلومات،
- تخصيص استثمارات وموارد كافية.

ولكي تنفذ الإدارة التنفيذية عملية "التوجيه"، ينبغي لها أن تقوم بما يلي:

- وضع وتنفيذ استراتيجيات وسياسات بشأن أمن المعلومات،
- مواءمة أهداف أمن المعلومات مع أهداف قطاع الأعمال،
- الترويج لإقامة ثقافة إيجابية في مجال أمن المعلومات.

4.3.5 الرصد

"الرصد" هو عملية إدارة تمكّن مجلس الإدارة من تقييم مستوى تحقيق الأهداف الاستراتيجية.

ولكي ينفذ مجلس الإدارة عملية "الرصد"، ينبغي له أن يقوم بما يلي:

- تقييم فعالية أنشطة إدارة أمن المعلومات،
- ضمان توافقها مع المتطلبات الداخلية والخارجية،
- مراعاة البيئة المتغيرة للأعمال وتغير البيئة القانونية والتنظيمية وتبعاتها المحتملة بشأن المخاطر المتعلقة بالمعلومات.

ولكي تنفذ الإدارة التنفيذية عملية "الرصد"، ينبغي لها أن تقوم بما يلي:

- اختيار مقاييس أداء مناسبة من وجهة نظر الأعمال،
- تزويد مجلس الإدارة بتعليقات على نتائج أداء أمن المعلومات، بوسائل منها تطبيق الإجراءات التي حددها المجلس سابقاً وتأثيرها على المنظمة،
- تنبيه مجلس الإدارة إلى ما يستجد من تطورات تؤثر على المخاطر المتعلقة بالمعلومات وأمن المعلومات.

5.3.5 الاتصال

"الاتصال" هو عملية إدارة ثنائية الاتجاه يتبادل بموجبها مجلس الإدارة معلومات مع أصحاب المصلحة عن أمن المعلومات على نحو يلبي احتياجاتهم الخاصة.

ومن أساليب "الاتصال" بيان حالة أمن المعلومات التي توضح لأصحاب المصلحة الأنشطة والمسائل المتعلقة بأمن المعلومات، وترد أمثلة عليها في الملحقين ألف وباء.

ولكي ينفذ مجلس الإدارة عملية "الاتصال"، ينبغي له أن يقوم بما يلي:

- تقديم تقرير إلى أصحاب المصلحة الخارجيين عن أن المنظمة تطبق مستوى معينا من أمن المعلومات يتناسب مع طبيعة أعمالها.
- إخطار الإدارة التنفيذية بنتائج أي مراجعات خارجية تحدد مسائل تتعلق بأمن المعلومات، وطلب اتخاذ إجراءات تصحيحية،
- تمييز المعلومات المتعلقة بالالتزامات التنظيمية وتوقعات أصحاب المصلحة واحتياجات الأعمال، بالنسبة لأمن المعلومات.

ولكي تنفذ الإدارة التنفيذية عملية "الاتصال"، ينبغي لها أن تقوم بما يلي:

- إسداء المشورة إلى مجلس الإدارة بشأن أي مسائل تستدعي اهتمامه بها واتخاذ قرار بشأنها إن أمكن،
- تزويد أصحاب المصلحة المعنيين بتعليمات حول الإجراءات التفصيلية التي يجب اتخاذها دعماً لتوجيهات مجلس الإدارة وقراراته.

6.3.5 الضمان

"الضمان" عملية إدارة يكلّف بموجبها مجلس الإدارة بإجراء عمليات مستقلة وموضوعية في مجال التدقيق أو المراجعة أو منح الشهادات. وتحدد هذه العمليات الأهداف والإجراءات المتصلة بتنفيذ أنشطة الإدارة وعملياتها، وتتحقق من تلك الأهداف والإجراءات من أجل بلوغ المستوى المنشود من أمن المعلومات.

ولكي ينفذ مجلس الإدارة عملية "الضمان"، ينبغي له أن يقوم بما يلي:

- التكليف بإبداء آراء مستقلة وموضوعية حول السبل الكفيلة بامتثال المجلس لمتطلبات المساءلة عن تحقيق المستوى المنشود من أمن المعلومات.

ولكي تنفذ الإدارة التنفيذية عملية "الضمان"، ينبغي لها أن تقوم بما يلي:

- دعم العمليات التي يكلّف بإجرائها مجلس الإدارة في مجال التدقيق أو المراجعة أو منح الشهادات.

الملحق ألف

مثال على حالة أمن المعلومات

(لا يشكّل هذا الملحق جزءاً أساسياً من هذه التوصية | المعيار الدولي)

قد تتولى المنظمة إعداد حالة لأمن المعلومات وتُطلِع الزبائن وأصحاب المصلحة عليها بوصفها أداة للإبلاغ عن أمن المعلومات.

وينبغي أن تختار المنظمة نسق ومحتويات حالة أمن المعلومات وتبت في هذا النسق والمحتويات. والملحق ألف هو مثال يستخدم بياناً لتدقيق أمن المعلومات لأغراض الإعلان عن الرضا.

الجدول ألف – حالة أمن المعلومات

الإدارة مقتنعة بأن ضوابط وإجراءات أمن المعلومات المبنية على المعايير الواردة في **xyz** (من قبيل السلسلة 27000، COBIT) والمتعلقة بإجراءات المنظمة وأنظمتها التشغيلية المستكملة بضوابط إدارية رفيعة المستوى، هي ضوابط وإجراءات مطبقة بمستوى لائق من الفعالية في الفترة الممتدة من **mmm** وحتى **nnn** لأغراض توفير ضمانات معقولة تفيد بأن الأهداف المحددة بشأن ضوابط أمن المعلومات من حيث الحفاظ على سريتها وسلامتها وتوافرها، قد تحققت. وقدمت الإدارة مدققين خارجيين لأمن المعلومات مثّلتهم بالحروف **ABC** مع رسالة تمثيل لهذا الغرض. وقد عيّن مجلس المدراء المدققين ABC لدراسة موضوع تأكيد الإدارة لضوابط أمن المعلومات. وأجرى المدققون دراستهم وفقاً للمعايير الراسخة، وشملت الدراسة تقييماً لفعالية وضع وتطبيق ضوابط أمن المعلومات وإجراءاته من خلال اختبار العينات. وفي هذا الصدد، أدلى المدققون **ABC** برأي للإدارة يفيد بأن نتائج اختباراتهم تشير إلى أن الضوابط الموضوعة بشأن النواحي المادية تتسم بطابع الفعالية بناءً على المعايير الإدارية المحددة في **xyz** (من قبيل السلسلة 27000، CobiT)، باستثناء بعض الحالات. وجرت مناقشة رسالة الإدارة المتعلقة بالتأكيد الكامل وكذلك تقرير التدقيق الخارجي بما فيه من حالات مستثناة فيما يتعلق بضوابط أمن المعلومات مع لجنة المراجعة وعرضها على كافة أعضاء مجلس المدراء. وتقدم نسخ منهما إلى أصحاب المصلحة بناءً على طلبهم.

ملاحظـــة – المقادير "nnn"، و"mmm"، و"xyz"، و"ABC" هي عبارة عن رموز بديلة، وينبغي أن ترد التواريخ والأسماء المحددة في بيانات فعلية.

الملحق باء

مثال على حالة لأمن المعلومات بمحتويات مبيّنة بالتفصيل

(لا يشكّل هذا الملحق جزءاً أساسياً من هذه التوصية | المعيار الدولي)

هذا الملحق هو عبارة عن مثال على حالة لأمن المعلومات بمحتويات مبيّنة بالتفصيل، وهو مفيد بشكل خاص للمنظمات التي تتوخى تعزيز سمعتها من خلال توثيق عرى أمنها، مثل الشركات التجارية في مجال تكنولوجيا المعلومات والاتصالات. ومستوى شفافية النهج الذي تتبعه المنظمة في إدارة المخاطر المحيقة بأمن معلوماتها والكشف عنها كما ينبغي من الأنشطة الفعالة أيضاً في مجال تعزيز الثقة، ويمكن بفضلها أن يشترك أصحاب المصلحة في رفع مستوى الوعي بالمسألة.

الجدول باء – حالة لأمن المعلومات بمحتويات مبيّنة بالتفصيل

المقدمة

- **مجال التطبيق** (الاستراتيجيات، والسياسات، والمعايير)، **محيط التطبيق** (وحدات جغرافية/تنظيمية)، **الفترة المشمولة بالتطبيق** (شهر/ثلاثة أشهر/ستة أشهر/سنة)

الحالة العامة

- **مرضية/ليست مرضية بعد/غير مرضية**

التحديثات (حسب الاقتضاء والأهمية)

- التقدم المحرز في تطبيق استراتيجية أمن المعلومات
  عناصر مستكملة/قيد البحث/يُزمع استكمالها
- التغييرات المدخلة على نظام إدارة أمن المعلومات
  تنقيح سياسات نظام إدارة أمن المعلومات (ISMS)، والهيكل التنظيمي لتطبيق نظام ISMS (بما يشمل تحديد المسؤوليات)
- التقدم المحرز في مجال إصدار الشهادات
  (إعادة) إصدار شهادات النظام ISMS، وإجراء عمليات تدقيق مصدّقة لأمن المعلومات
- الميزنة/التوظيف/التدريب
  الوضع المالي، ومدى كفاية عدد الموظفين، ومؤهلات تحقيق أمن المعلومات
- أنشطة أخرى تتعلق بأمن المعلومات
  إشراك الإدارة في استدامة الأعمال وحملات التوعية والمساعدة الداخلية/الخارجية في مجال التدقيق

القضايا الهامة (إن وجدت)

- نتائج عمليات مراجعة أمن المعلومات
  التوصيات، وردود الإدارة، وخطط العمل، والمواعيد المستهدفة
- التقدم المحرز بشأن إعداد تقارير رئيسية عن عمليات التدقيق الداخلية/الخارجية
  التوصيات، وردود الإدارة، وخطط العمل، والمواعيد المستهدفة
- حوادث أمن المعلومات
  تقدير النتائج، وخطط العمل، والمواعيد المستهدفة
- (عدم) الامتثال للتشريعات واللوائح ذات الصلة
  تقدير النتائج، وخطط العمل، والمواعيد المستهدفة

القرار (القرارات) اللازمة (إن وجدت)

- الموارد الإضافية
  تمكين أمن المعلومات من دعم مبادرة (مبادرات) قطاع الأعمال

بيبليوغرافيـــا

[1] Recommendation ITU-T X.1051 (2008) | ISO/IEC 27011:2008, *Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*.

[2] ISO/IEC 27001:2005, *Information technology – Security techniques – Requirements of information security management systems*.

[3] ISO/IEC 27002:2005, *Information technology – Security techniques – Code of practice for information security management*.

[4] ISO/IEC 27005:2011, *Information technology – Security techniques – Information security risk management*.

[5] ISO/IEC 38500:2008, *Corporate Governance of Information technology*.

[6] ITGI, *Information Security Governance framework: 2009*.

[7] ISF, *Standard of Good Practice for Information Security: 2011*.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	المبادئ العامة للتعريفة
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	إنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات (TMN) وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	المطاريف وطرائق التقييم الذاتية والموضوعية
السلسلة Q	التبديل والتشوير
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التلماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2013