الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1054

(2021/04)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن المعلومات والشبكات – إدارة الأمن

أمن المعلومات والأمن السيبراني وحماية الخصوصيات – إدارة أمن المعلومات

التوصية ITU-T X.1054

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.1–X.199
التوصيل البيني للأنظمة المفتوحة	X.200–X.299
التشغيل البيني للشبكات	X.300–X.399
أنظمة معالجة الرسائل	X.400–X.499
الدليل	X.500–X.599
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.600–X.699
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.700–X.799
الأمن	X.800–X.849
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.850–X.899
المعالجة الموزعة المفتوحة	X.900–X.999
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1000–X.1029
أمن الشبكة	X.1030–X.1049
إدارة الأمن	**X.1050–X.1069**
الخصائص البيومترية	X.1080–X.1099
تطبيقات وخدمات آمنة (1)	
أمن البث المتعدد	X.1100–X.1109
أمن الشبكة المحلية	X.1110–X.1119
أمن الخدمات المتنقلة	X.1120–X.1139
أمن الويب (1)	X.1140–X.1149
تطبيقات الأمن (1)	X.1150–X.1159
الأمن بين جهتين نظيرتين	X.1160–X.1169
أمن معرفات الهوية عبر الشبكات	X.1170–X.1179
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1180–X.1199
أمن الفضاء السيبراني	
الأمن السيبراني	X.1200–X.1229
مكافحة الرسائل الاقتحامية	X.1230-X.1249
إدارة الهوية	X.1250–X.1279
تطبيقات وخدمات آمنة (2)	
اتصالات الطوارئ	X.1300–X.1309
أمن شبكات المحاسيس واسعة الانتشار	X.1310–X.1319
أمن شبكة الكهرباء الذكية	X.1330–X.1339
البريد المعتمد	X.1340–X.1349
أمن إنترنت الأشياء (IoT)	X.1350–X.1369
أمن أنظمة النقل الذكية (ITS)	X.1370–X.1399
أمن سجل الحسابات الموزع (DLT)	X.1400–X.1429
أمن التطبيقات (2)	X.1450–X.1459
أمن شبكة الإنترنت (2)	X.1470–X.1489
تبادل معلومات الأمن السيبراني	
نظرة عامة على الأمن السيبراني	X.1500–X.1519
تبادل مواطن الضعف/الحالة	X.1520–X.1539
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1540–X.1549
تبادل السياسات	X.1550–X.1559
طلب المعلومات الحدسية والمعلومات الأخرى	X.1560–X.1569
تعرف الهوية والاكتشاف	X.1570–X.1579
التبادل المضمون	X.1580–X.1589
الدفاع السيبراني	X.1590–X.1599
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1600–X.1601
تصميم أمن الحوسبة السحابية	X.1602–X.1639
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1640–X.1659
تنفيذ أمن الحوسبة السحابية	X.1660–X.1679
أمن أشكال أخرى للحوسبة السحابية	X.1680–X.1699
الاتصالات الكمومية	
المصطلحات	X.1700–X.1701
المولد الكمومي للأعداد العشوائية	X.1702–X.1709
إطار أمن شبكات توزيع المفاتيح الكمومية (QKDN)	X.1710–X.1711
التصميم الأمني للشبكات QKDN	X.1712–X.1719
التقنيات الأمنية للشبكات QKDN	X.1720–X.1729
أمن البيانات	
أمن البيانات الضخمة	X.1750–X.1759
حماية البيانات	X.1770–X.1789
أمن شبكات الاتصالات المتنقلة الدولية–2020	X.1800–X.1819

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

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

أمن المعلومات والأمن السيبراني وحماية الخصوصيات – إدارة أمن المعلومات

ملخص

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

يمثل أمن المعلومات قضية رئيسية بالنسبة إلى المنظمات، يزداد تفاقمها من خلال التقدم السريع في منهجيات وتكنولوجيات الهجوم، وما يقابلها من ضغوط تنظيمية متزايدة.

ويمكن أن يؤدي فشل ضوابط أمن معلومات المنظمة إلى العديد من الآثار السلبية على المنظمة وأطرافها المعنية بما في ذلك على سبيل المثال لا الحصر تقويض الثقة.

وتتمثل إدارة أمن المعلومات في استخدام الموارد لضمان التنفيذ الفعّال لأمن المعلومات، وتوفير ضمان:

- باتباع التوجيهيات المتعلقة بأمن المعلومات؛
- بتلقي مجلس الإدارة تقارير موثوقة وذات صلة بشأن الأنشطة المتعلقة بأمن المعلومات.

وهذا يساعد مجلس الإدارة على اتخاذ القرارات المتعلقة بالأهداف الاستراتيجية للمنظمة من خلال توفير معلومات بشأن أمن المعلومات قد تؤثر على هذه الأهداف. كما يضمن تماشي استراتيجية أمن المعلومات مع الأهداف العامة للكيان.

يحتاج المديرون وغيرهم من العاملين في المنظمات إلى فهم:

- متطلبات الإدارة التي تؤثر على عملهم؛
- كيفية الوفاء بمتطلبات الإدارة التي تتطلب منهم اتخاذ إجراءات.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1054	2012-09-07	17	11.1002/1000/11594
2.0	ITU-T X.1054	2021-04-30	17	11.1002/1000/14248

مصطلحات أساسية

أمن المعلومات، إدارة أمن المعلومات، توجيه أمن المعلومات، نظام إدارة أمن المعلومات (ISMS).

* للنفاذ إلى توصية، ترجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

الاتحاد الدولي للاتصالات وكالة الأمم المتحدة المتخصصة 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 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

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

ملاحظة

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 "يلزم" وصيغ ملزمة أخرى مثل فعل "يجب" 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/حقوق تأليف ونشر البرمجيات 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 قواعد البيانات المناسبة لدى الاتحاد المتاحة من خلال الموقع الإلكتروني لقطاع تقييس الاتصالات عبر الرابط: http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

تمهيد

الاتحاد الدولي للاتصالات (ITU) هو وكالة متخصصة للأمم المتحدة في ميدان الاتصالات. 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).

تشكل المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC) النظام المتخصص بشأن التقييس على الصعيد العالمي. وتشارك الهيئات الوطنية التي هي أعضاء في المنظمة الدولية للتوحيد القياسي (ISO) أو اللجنة الكهرتقنية الدولية (IEC) في وضع توصيات | معايير دولية من خلال اللجان التقنية التي تنشئها المنظمة المعنية لتناول مجالات معينة من النشاط التقني. وتتعاون اللجان التقنية المنبثقة عن المنظمة ISO واللجنة IEC في مجالات ذات اهتمام مشترك. وتشارك في العمل أيضاً منظمات دولية أخرى، حكومية وغير حكومية، تكون على علاقة مع المنظمة ISO واللجنة IEC. أما في مجال أمن المعلومات، والأمن السيبراني وحماية الخصوصية، فقد أنشأت المنظمة الدولية للتوحيد القياسي واللجنة الكهرتقنية الدولية اللجنة التقنية المشتركة رقم 1 (ISO/IEC JTC 1).

ووُضعت هذه التوصية | المعيار الدولي وفقاً للقواعد الواردة في الجزء الثاني من توجيهات المنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية.

وتتمثل المهمة الرئيسية للجنة التقنية المشتركة في إعداد هذه التوصية | المعيار الدولي. ويُعمم مشروع التوصية | المعايير الدولية التي تعتمدها اللجنة التقنية المشتركة على الهيئات الوطنية للتصويت عليها. ويتطلب نشر المعيار كمعيار دولي موافقة 75% على الأقل من الهيئات الوطنية التي تدلي بأصواتها.

ويُسترعى الانتباه إلى إمكانية أن تكون بعض عناصر هذه التوصية | المعيار الدولي خاضعة لحقوق براءات الاختراع. ولا تقع على عاتق الاتحاد الدولي للاتصالات أو المنظمة الدولية للتوحيد القياسي أو اللجنة الكهرتقنية الدولية مسؤولية تحديد أيّ حق من حقوق براءات الاختراع هذه أو جميعها.

وقد أعدت التوصية ITU-T X.1054 | المعيار الدولي ISO/IEC 27014 اللجنة التقنية المشتركة ISO/IEC JTC 1، *تكنولوجيا المعلومات*، اللجنة الفرعية 27، *أمن المعلومات، والأمن السيبراني وحماية الخصوصية*، بالتعاون مع لجنة الدراسات 17 بقطاع تقييس الاتصالات.

المعيار الدولي
توصية قطاع تقييس الاتصالات

أمن المعلومات والأمن السيبراني وحماية الخصوصيات – إدارة أمن المعلومات

1 مجال التطبيق

تقدم هذه التوصية | هذا المعيار الدولي إرشادات بشأن المفاهيم والأهداف والعمليات لإدارة أمن المعلومات التي يمكن من خلالها للمنظمات تقييم العمليات المتعلقة بأمن المعلومات داخل المنظمة وتوجيهها ورصدها وتناقلها.

والجمهور المستهدف لهذه الوثيقة هو:

- مجلس الإدارة والإدارة العليا؛
- المسؤولون عن تقييم نظام إدارة أمن المعلومات (ISMS) وتوجيهه ومراقبته استناداً إلى المعيار ISO/IEC 27001؛
- المسؤولون عن إدارة أمن المعلومات التي تجري خارج نطاق نظام ISMS قائم على المعيار ISO/IEC 27001، ولكن ضمن نطاق الإدارة.

وتُطبق هذه التوصية | المعيار الدولي على المنظمات بأنواعها وأحجامها كافة.

تنطبق جميع الإشارات إلى نظام ISMS في هذه الوثيقة على نظام ISMS قائم على المعيار ISO/IEC 27001.

وتركز هذه التوصية | المعيار الدولي على ثلاثة أنواع من المنظمات ISMS مبينة في الملحق B. ومع ذلك، يمكن لأنواع أخرى من المنظمات أن تستخدمها.

2 المراجع المعيارية

تتضمن التوصيات والمعايير الدولية التالية 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 والمعايير تخضع إلى المراجعة، وتشجَّع الأطراف في اتفاقات تستند إلى هذه التوصية | هذا المعيار الدولي على السعي إلى تطبيق أحدث طبعة للتوصيات والمعايير 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 قطاع تقييس الاتصالات السارية الصلاحية.

– المعيار الدولي ISO/IEC 27000:2013 النافذ، *تكنولوجيا المعلومات – تقنيات الأمن – أنظمة إدارة أمن المعلومات – نظرة عامة ومفردات*.

– المعيار الدولي ISO/IEC 27001 النافذ، *تكنولوجيا المعلومات – تقنيات الأمن – أنظمة إدارة أمن المعلومات – متطلبات*.

3 تعاريف

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

تحتفظ المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC) والاتحاد الدولي للاتصالات (ITU) بقواعد بيانات مصطلحات من أجل استخدامها في مجال التقييس وهي متاحة في العناوين التالية:

- الموسوعة الإلكترونية الخاصة باللجنة الكهرتقنية الدولية، متاحة في العنوان التالي: http://www.electropedia.org/.
- منصة التصفح الإلكترونية الخاصة بالمنظمة الدولية للتوحيد القياسي، متاحة في العنوان التالي: http://www.iso.org/obp.
- مصطلحات وتعاريف الاتحاد، متاحة في العنوان التالي: http://www.itu.int/go/terminology-database.

1.3 الكيان (entity): المنظمة (2.3) والهيئات أو الأطراف الأخرى.

ملاحظة – قد يكون الكيان مجموعة من الشركات، أو شركة واحدة، أو شركة غير ربحية، أو غيرها. ويتمتع الكيان بسلطة إدارية على المنظمة. وقد يكون الكيان مطابقاً للمنظمة، مثلاً في الشركات الصغرى.

2.3 المنظمة (organization): هي ذلك الجزء من الكيان (1.3) الذي يقوم بتشغيل وإدارة نظام إدارة أمن المعلومات.

3.3 مجلس الإدارة (governing body): شخص أو مجموعة من الأشخاص المسؤولين عن أداء الكيان وتوافقه.

ملاحظة – في **المصدر**: المعيار ISO/IEC 27000:2018، 24.3، المعدّل – استُعيض عن مصطلح "منظمة" بمصطلح "كيان".

4.3 الإدارة العليا (top management): شخص أو مجموعة من الأشخاص يديرون منظمة (2.3) ما ويتحكمون فيها على أعلى مستوى.

الملاحظة 1 – المصدر: المعيار ISO/IEC 9001.

الملاحظة 2 – للإدارة العليا سلطة تفويض السلطة وتوفير الموارد داخل المنظمة.

الملاحظة 3 – إذا كان نطاق نظام الإدارة لا يغطي سوى جزء من الكيان، فإن الإدارة تشير إلى أولئك الذين يوجهون هذا الجزء من الكيان ويتحكمون فيه. وفي هذه الحالة، تكون الإدارة العليا مسؤولة أمام مجلس إدارة الكيان.

الملاحظة 4 – تبعاً لحجم المنظمة ومواردها، يمكن أن تكون الإدارة العليا مماثلة لمجلس الإدارة.

الملاحظة 5 – المتعلقة بهذا التعريف – تقدم الإدارة العليا تقارير إلى مجلس الإدارة. [**المصدر**: ISO/IEC 27000:2018, 3.75].

الملاحظة 6 – يوفر المعيار ISO/IEC 37001 أيضاً تعاريف لمجلس الإدارة والإدارة العليا.

4 المختصرات

لأغراض هذه التوصية | المعيار الدولي، تُستعمل المختصرات التالية:

ISMS نظام إدارة أمن المعلومات *(Information Security Management System)*

IT تكنولوجيا المعلومات *(Information Technology)*

5 استخدام وهيكل هذه التوصية | هذا المعيار الدولي

تصف هذه التوصية | هذا المعيار الدولي كيفية عمل إدارة أمن المعلومات ضمن نظام إدارة أمن المعلومات القائم على المعيار ISO/IEC 27001، وكيف يمكن لهذه الأنشطة أن تتصل بأنشطة إدارية أخرى تعمل خارج نطاق نظام إدارة أمن المعلومات. وتحدد أربع عمليات رئيسية هي "التقييم" و"التوجيه" و"الرصد" و"التواصل" يمكن فيها تنظيم نظام إدارة أمن المعلومات داخل المنظمة، وتقترح نُهجاً لإدماج إدارة أمن المعلومات في أنشطة الإدارة التنظيمية في كل عملية من هذه العمليات. وأخيراً يصف الملحق A العلاقات بين الإدارة التنظيمية وإدارة تكنولوجيا المعلومات وإدارة أمن المعلومات.

ويغطي نظام إدارة أمن المعلومات المنظمة بأكملها حسب التعريف (انظر المعيار ISO/IEC 27000). وقد يغطي الكيان بأكمله أو جزءاً منه. وهذا موضح في الشكل 1.B.

6 معايير التنظيم والإدارة

1.6 لمحة عامة

إدارة أمن المعلومات هي الوسيلة التي يوفر بها مجلس إدارة المنظمة التوجيه والرقابة عموماً على الأنشطة التي تؤثر على أمن معلومات المنظمة. ويركز هذا التوجيه وهذه الرقابة على الظروف التي يمكن فيها لأمن المعلومات غير الكافي أن يؤثر سلباً على قدرة المنظمة على تحقيق أهدافها الإجمالية. ومن الشائع أن يحقق مجلس الإدارة أهدافه في مجال التنظيم من خلال ما يلي:

- توفير التوجيه من خلال وضع الاستراتيجيات والسياسات؛

- رصد أداء المنظمة؛
- تقييم المقترحات والخطط التي يضعها المديرون.

وترتبط إدارة أمن المعلومات بضمان تحقيق أهداف المنظمة الموصوفة في الاستراتيجيات والسياسات التي يضعها مجلس الإدارة. ويمكن أن يشمل ذلك التفاعل مع مجلس الإدارة عن طريق ما يلي:

- توفير مقترحات وخطط كي ينظر فيها مجلس الإدارة؛
- تزويد مجلس الإدارة بمعلومات بشأن أداء المنظمة.

وتتطلب الإدارة الفعّالة لأمن المعلومات أن يضطلع أعضاء مجلس الإدارة والمديرون على السواء بدور كل منهم بطريقة متسقة.

2.6 أنشطة الإدارة في نطاق نظام إدارة أمن المعلومات

يحدد المعيار ISO/IEC 27001 متطلبات إنشاء نظام إدارة أمن المعلومات وتنفيذه وصيانته وتحسينه باستمرار ضمن سياق المنظمة. كما يشمل متطلبات تقييم ومعالجة مخاطر أمن المعلومات المصممة خصيصاً لاحتياجات المنظمة.

لا يستخدم المعيار ISO/IEC 27001 مصطلح "إدارة" وإنما يحدد عدداً من المتطلبات التي هي بمثابة أنشطة الإدارة. وتوفر القائمة التالية أمثلة لهذه الأنشطة. وترتبط الإشارات إلى المنظمة والإدارة العليا، كما سبقت الإشارة، بنطاق نظام إدارة أمن المعلومات القائم على المعيار ISO/IEC 27001.

- الفقرة 1.4 من المعيار ISO/IEC 27001:2013 تفيد بأن فهم المنظمة وسياقها يتطلب أن تحدد الإدارة ما تهدف إلى تحقيقه – أهدافها وغاياتها فيما يتعلق بأمن المعلومات. ويجب أن تكون هذه الأهداف والغايات مرتبطة بالأهداف والغايات الإجمالية للكيان وأن تدعمها. ويتعلق ذلك بأهداف الإدارة 1 و3 و4 المذكورة في الفقرة 2.7 من هذه التوصية | المعيار الدولي.
- الفقرة 2.4 من المعيار ISO/IEC 27001:2013 تفيد بأن فهم احتياجات الأطراف المهتمة وتوقعاتها يتطلب أن تحدد المنظمة الأطراف المهتمة ذات الصلة بنظام إدارة أمن المعلومات لديها، ومتطلبات تلك الأطراف المهتمة ذات الصلة بأمن المعلومات. ويتعلق ذلك بهدف الإدارة 4 المذكور في الفقرة 2.7 من هذه التوصية | المعيار الدولي.
- الفقرة 3.4 من المعيار ISO/IEC 27001:2013 تفيد بأن تحديد نطاق نظام إدارة أمن المعلومات يتطلب أن تعرّف المنظمة حدود النظام ISMS وإمكانية تطبيقه لتحديد نطاقه من خلال النظر في القضايا الخارجية والقضايا الداخلية، والمتطلبات والواجهات والتبعيات. ومن المحدد أيضاً أن تقوم المنظمة بإدماج متطلبات وتوقعات الأطراف المهتمة في نظام إدارة أمن المعلومات لديها، وكذلك المسائل الخارجية والداخلية (مثل القوانين واللوائح والعقود). ويتعلق ذلك بهدف الإدارة 1 المذكور في الفقرة 2.7 من هذه التوصية | المعيار الدولي.
- الفقرة 5 من المعيار ISO/IEC 27001:2013 تنص على أن تضع المنظمة السياسات والأهداف وتدمج أمن المعلومات في عملياتها (التي يمكن اعتبارها عمليات الإدارة). وتتطلب من المنظمة توفير الموارد المناسبة المتاحة والإبلاغ عن أهمية إدارة أمن المعلومات. والأهم من ذلك، فهي تنص أيضاً على أن تقوم المنظمة بتوجيه ودعم الأشخاص للمساهمة في فعالية نظام إدارة أمن المعلومات، ودعم الأدوار الإدارية الأخرى ذات الصلة في مجالات مسؤوليتها. وتتضمن الفقرة 5 من المعيار ISO/IEC 27001:2013 إرشادات لوضع السياسات وإسناد أدوار إدارة أمن المعلومات وإعداد التقارير. ويتعلق ذلك بهدفي الإدارة 1 و3 المذكورين في الفقرة 2.7 من هذه التوصية | المعيار الدولي.
- الفقرة 6 من المعيار ISO/IEC 27001:2013 تنظر في تصميم نهج إدارة مخاطر المنظمة، مع الإشارة إلى ضرورة تحديد الإدارة للمخاطر والفرص التي يتعين معالجتها لضمان فعالية نظامها لإدارة معلومات البيانات. وتقدم مفهوم المسؤولين عن مواجهة المخاطر وتضع مسؤولياتهم في سياق أنشطة المنظمة لإدارة المخاطر والموافقة على أنشطة معالجة المخاطر. وتتطلب أيضاً أن تقوم المنظمة بوضع أهداف أمن المعلومات. ويتعلق ذلك بهدف الإدارة 2 المذكور في الفقرة 2.7 من هذه التوصية | المعيار الدولي.

- الفقرة 7 من المعيار ISO/IEC 27001:2013 تنص على أن يكون الأشخاص مؤهلين في مجال تنفيذ التزاماتهم المتعلقة بأمن المعلومات، ويحدد متطلبات الاتصالات التنظيمية. ويتعلق ذلك بهدف الإدارة 5 المذكور في الفقرة 2.7 من هذه التوصية | المعيار الدولي.
- الفقرة 8 من المعيار ISO/IEC 27001:2013 تحدد مسؤولية المنظمة عن تخطيط نظام إدارة أمن المعلومات لديها وتنفيذه ومراقبته، بما في ذلك الترتيبات الخارجية. ويتعلق ذلك بهدفي الإدارة 4 و6 الواردين في الفقرة 2.7 من هذه التوصية | المعيار الدولي.
- الفقرة 9 من المعيار ISO/IEC 27001:2013، تفيد تقييم الأداء بأن يتطلب الرصد والإبلاغ عن جميع الجوانب ذات الصلة لنظام إدارة أمن المعلومات والتدقيق الداخلي واستعراض الإدارة العليا ومجلس الإدارة واتخاذ القرارات بشأن الفعالية التشغيلية لنظام إدارة أمن المعلومات، بما في ذلك أي تغييرات مطلوبة. ويتعلق ذلك بهدف الإدارة 6 المذكور في الفقرة 2.7 من هذه التوصية | المعيار الدولي.
- الفقرة 10 من المعيار ISO/IEC 27001:2013 توصِّف تحديد ومعالجة عدم المطابقة، ومتطلبات تحديد فرص التحسين المستمر، والعمل على تلك الفرص. ويتعلق ذلك بهدف الإدارة 4 المذكور في الفقرة 2.7 من هذه التوصية | المعيار الدولي.

3.6 معايير أخرى ذات صلة

يوفر المعيار ISO/IEC 38500 مبادئ توجيهية لأعضاء الهيئات الإدارية للمنظمات بشأن الاستخدام الفعّال والكفء والمقبول لتكنولوجيا المعلومات داخل مؤسساتهم. كما يوفر إرشادات للقائمين على تقديم المشورة أو الإبلاغ أو المساعدة إلى مجالس الإدارة في مجال إدارة تكنولوجيا المعلومات.

4.6 تسلسل الإدارة داخل المنظمة

تتوافق هذه التسلسلات تماماً مع عمليات الإدارة التنظيمية الموضحة في الفقرة 7. والعنصران الأخيران في القائمة متكافئان من حيث جوانب الإدارة في سياق أمن المعلومات:

- مواءمة أهداف أمن المعلومات مع أهداف العمل؛
- إدارة مخاطر أمن المعلومات وفقاً لأهداف أمن المعلومات؛
- تجنب تضارب المصالح في مجال إدارة أمن المعلومات؛
- منع استخدام تكنولوجيا المعلومات الخاصة بالمنظمة لإلحاق الضرر بمنظمات أخرى.

7 إدارة الكيان وإدارة أمن المعلومات

1.7 لمحة عامة

هناك العديد من مجالات الإدارة داخل الكيان، منها أمن المعلومات وتكنولوجيا المعلومات والصحة والسلامة والجودة والتمويل. وكل مجال من مجالات الإدارة هو أحد مكونات أهداف الإدارة الإجمالية للكيان، وبالتالي ينبغي أن يكون متماشياً مع تخصص الكيان. وتتداخل نطاقات نماذج الإدارة أحياناً. وتصف الفقرتان 2.7 و3.7 الأهداف والعمليات التي تنطوي عليها الإدارة، والتي يمكن أن تنطبق على أي مجال خاضع للإدارة.

ويركز نظام إدارة أمن المعلومات على إدارة المخاطر المتعلقة بالمعلومات. ولا يتناول بشكل مباشر مواضيع مثل الربحية وحيازة الأصول واستخدامها أو تحقيقها أو كفاءة العمليات الأخرى، على الرغم من أنه ينبغي أن يدعم أي أهداف تنظيمية بشأن هذه المواضيع.

2.7 الأهداف

1.2.7 الهدف 1: إرساء أمن معلومات متكامل وشامل على مستوى الكيان 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 مستوى الكيان في إطار مراعاة عملية صنع القرار لأولويات الكيان. وينبغي توثيق عرى تنسيق الأنشطة المتعلقة بالأمن المادي والمنطقي. ومع ذلك، فهذا لا يتطلب مجموعة واحدة من إجراءات الأمن، أو نظاماً واحداً لإدارة أمن المعلومات (ISMS) في إطار الكيان.

وضماناً لأمن المعلومات على مستوى الكيان ككل، ينبغي تحديد المسؤولية والمساءلة عن أمن المعلومات في كامل طائفة الأنشطة التي يضطلع بها الكيان. وهو أمر قد يمتد نطاقه ليتعدى "الحدود" المنظورة للكيان عموماً، ليشمل، على سبيل المثال، المعلومات التي تتولى أطراف خارجية تخزينها أو نقلها.

2.2.7 الهدف 2: اتخاذ القرارات باستخدام نهج قائم على إدارة المخاطر

ينبغي أن تستند إدارة أمن المعلومات إلى التزامات الامتثال، وكذلك إلى القرارات القائمة على إدارة المخاطر الخاصة بالكيان. وبالإضافة إلى الوفاء بالمتطلبات التنظيمية ذات الصلة، لا بد من أن يُبنى تحديد المقدار الكافي من الأمن على المخاطر التي يتحملها الكيان، بما فيها مخاطر خسارة الميزة التنافسية والامتثال والمسؤولية والاضطرابات التشغيلية والإضرار بالسمعة والخسائر المالية.

ويجب أن تتسم إدارة مخاطر أمن المعلومات بالاتساق في إطار الكيان وأن تتضمن اعتبارات الآثار السلبية المالية والتشغيلية والمتعلقة بالسمعة للانتهاكات وعدم الامتثال. وعلاوةً على ذلك، ينبغي دمج إدارة مخاطر أمن المعلومات مع النهج العام لإدارة المخاطر الذي يتبعه الكيان بحيث لا يتم ذلك بشكل منعزل ولا يسبب الارتباك، مثل التقابل مع منهجية الكيان أو تسجيل مخاطر المعلومات الاستراتيجية في سجل المخاطر الخاص بالكيان.

ولا بد من تخصيص الموارد المناسبة لتنفيذ إدارة المخاطر المتعلقة بالمعلومات كجزء من عملية إدارة الأمن.

3.2.7 الهدف 3: تحديد اتجاه الحيازة

ينبغي تقييم أثر مخاطر أمن المعلومات تقييماً وافياً عند الاضطلاع بأنشطة جديدة، منها على سبيل المثال لا الحصر، أي استثمار أو مشتريات أو دمج أو اعتماد تكنولوجيا جديدة، أو ترتيبات الاستعانة بمصادر خارجية أو التعاقد مع موردين خارجيين.

ولتحسين حيازة أمن المعلومات لدعم أهداف الكيان، ينبغي أن يكفل مجلس الإدارة دمج أمن المعلومات في عمليات الكيان القائمة، بما فيها إدارة المشاريع، والمشتريات، والنفقات المالية، والامتثال القانوني والتنظيمي، وإدارة المخاطر الاستراتيجية.

وينبغي للإدارة العليا لنظام إدارة أمن المعلومات أن تضع استراتيجية لأمن المعلومات تستند إلى أهداف الكيان، مع ضمان المواءمة بين متطلبات الكيان ومتطلبات أمن المعلومات التنظيمية، وبالتالي تلبية احتياجات الأطراف المهتمة الحالية والمتغيرة.

4.2.7 الهدف 4: ضمان التوافق مع المتطلبات الداخلية والخارجية

ينبغي لإدارة أمن المعلومات أن تكفل توافق سياسات وممارسات أمن المعلومات مع متطلبات الأطراف المهتمة. ويمكن أن يشمل ذلك التشريعات واللوائح، إلى جانب الشروط التعاقدية والالتزامات الداخلية.

ولمعالجة المسائل المتعلقة بالتوافق والامتثال، يمكن أن تحصل الإدارة العليا على تأكيدات تثبت أن أنشطة أمن المعلومات تستوفي بشكل مرضٍ متطلبات داخلية وخارجية عن طريق التكليف بإجراء عمليات تدقيق أمني مستقلة.

5.2.7 الهدف 5: تعزيز ثقافة إيجابية أمنياً

ينبغي بناء إدارة أمن المعلومات على ثقافة الكيان، ومنها الاحتياجات المستجدة للأطراف المعنية 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 أي هدف من الأهداف المنشودة. لذا فإن التنسيق وتضافر جهود التوجيه بين مختلف الأطراف المهتمة أمر غاية في الأهمية.

وسعياً إلى إقامة ثقافة إيجابية بخصوص أمن المعلومات، فإن على الإدارة العليا أن تطالب بالنهوض بأنشطة الأطراف المهتمة ودعمها وتنسيقها لتحقيق اتجاه متماسك في مجال أمن المعلومات. ويدعم ذلك تنفيذ برامج بشأن التثقيف بالجوانب الأمنية والتدريب عليها والتوعية بها. وينبغي دمج مسؤوليات أمن المعلومات في دور الموظفين والأطراف الأخرى، وينبغي لهم دعم نجاح كل نظام لإدارة أمن المعلومات من خلال تحمل هذه المسؤوليات.

6.2.7 الهدف 6: ضمان استيفاء الأداء الأمني للمتطلبات الحالية والمستقبلية للكيان

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

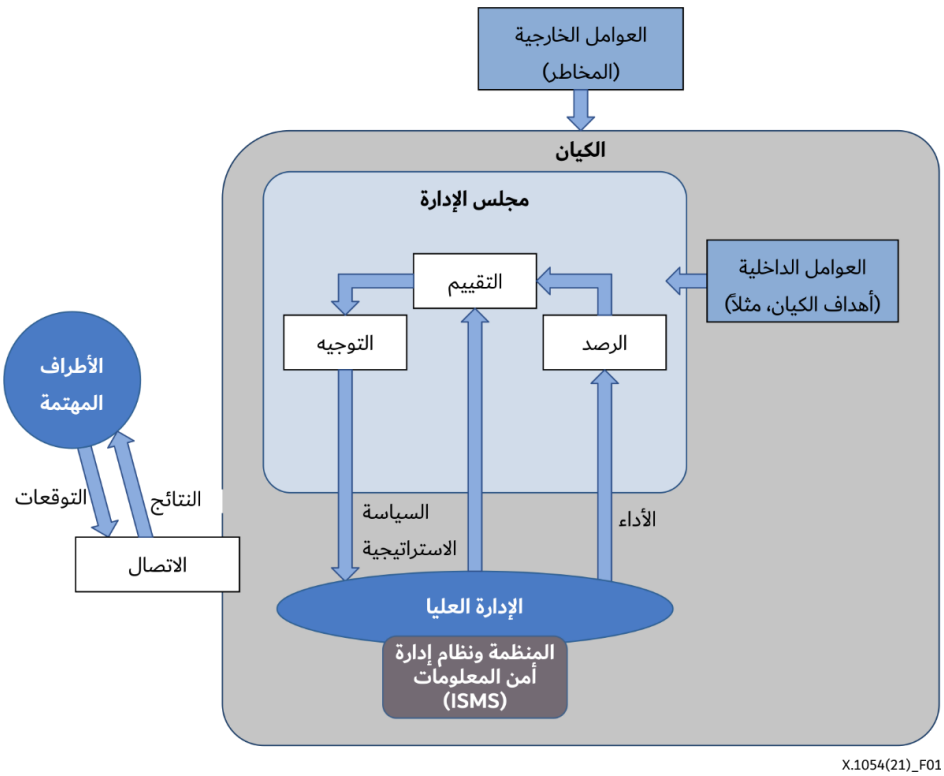
ولمراجعة أداء أمن المعلومات من وجهة نظر الإدارة، ينبغي لمجلس الإدارة أن يُقيّم أداء أمن المعلومات على أساس آثاره على مستوى الكيان، لا على أساس فعالية الضوابط الأمنية وكفاءتها حصراً.

وضمن كل نظام لإدارة أمن المعلومات، ينبغي أن يُتطلب من الإدارة العليا لنظام ISMS أن تنفذ برنامجاً لقياس الأداء من أجل رصد فرص التحسين وتدقيقها وتحديدها. وينبغي أن يربط مجلس الإدارة بين أداء أمن المعلومات وأداء المنظمة والكيان.

3.7 العمليات

1.3.7 عرض عام

يقوم مجلس الإدارة بعمليات "التقييم" و"التوجيه" و"الرصد" و"الاتصال". لأغراض إدارة أمن المعلومات. ويبين الشكل 1 العلاقة بين هذه العمليات.



الشكل 1 – نموذج الإدارة من أجل كيان ينفّذ نظام إدارة أمن معلومات واحد

الملاحظة 1 – تعريف مطلح "المنظمة" الوارد في الفقرة الفرعية [2.3] من هذه الوثيقة، يعني أن الإدارة العليا تشارك دائماً مشاركة فعّالة في تشغيل المنظمة.

الملاحظة 2 – يمكن أن يحتوي الكيان على أكثر من نظام إدارة أمن معلومات واحد، وقد تكون هناك أجزاء من كيان تنطبق عليها الإدارة دون أن تشكل جزءاً من نظام إدارة أمن المعلومات. انظر الفقرة 8 والملحق B.

2.3.7 التقييم

"التقييم" هو عملية إدارة تدرس المحقق حالياً من الأهداف 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 الكيان عملية "التقييم":

- يتعين عليه القيام بما يلي:
  - ضمان أن تراعي المبادرات المخاطر والفرص ذات الصلة؛
  - الاستجابة لقياسات وتقارير أمن المعلومات ونظام إدارة أمن المعلومات من خلال توصيف وتحديد أولويات الأهداف المطلوبة في سياق كل نظام إدارة لأمن المعلومات (ويتضمن ذلك النظر في المتطلبات خارج نطاق نظام إدارة أمن المعلومات)؛
- يتعين على الإدارة العليا لنظام ISMS القيام بما يلي:
  - ضمان أن يُقدم أمن المعلومات الدعم الكافي لبلوغ وصيانة أهداف الكيان؛
  - تقديم مشاريع جديدة بشأن أمن المعلومات ذات تأثير كبير إلى مجلس الإدارة للموافقة عليها.

3.3.7 التوجيه

"التوجيه" هو عملية إدارة تمكّن مجلس الإدارة من إعطاء توجيهات حول أهداف الكيان واستراتيجيته. 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 تنفَّذ عملية "التوجيه":

- ينبغي لمجلس الإدارة القيام بما يلي:
  - تعيين مجمل الاتجاه الاستراتيجي والأهداف للكيان؛
  - تحديد مدى تقبّل الكيان للمخاطر؛
  - الموافقة على استراتيجية أمن المعلومات.
- ويتعين على الإدارة العليا لكل نظام ISMS القيام بما يلي:
  - تخصيص استثمارات وموارد كافية؛
  - مواءمة أهداف أمن المعلومات التنظيمية مع أهداف الكيان؛
  - تخصيص الأدوار والمسؤوليات بشأن أمن المعلومات؛
  - وضع سياسة بشأن أمن المعلومات.

ملاحظة – شهية الإقدام على المخاطر هي مقدار ونوع المخاطر التي ترغب المنظمة في متابعتها أو الاحتفاظ بها.

4.3.7 الرصد

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

ولكي تنفَّذ عملية "الرصد":

- ينبغي لمجلس الإدارة القيام بما يلي:
  - تلقي تقرير عن فعالية تشغيل كل نظام لإدارة أمن المعلومات؛

- تقييم هذه التقارير في سياق أولويات الكيان؛
- إبلاغ الإدارة العليا للنظام ISMS بالأولويات؛

– ويتعين على الإدارة العليا لكل نظام إدارة أمن المعلومات ما يلي:

- تقييم فعالية أنشطة إدارة أمن المعلومات؛
- ضمان توافقها مع المتطلبات الداخلية والخارجية؛
- مراعاة البيئة المتغيرة للكيان، وتغير البيئة القانونية والتنظيمية وتبعاتها المحتملة بشأن المخاطر المتعلقة بالمعلومات؛
- اختيار مقاييس الأداء المناسبة والمطالبة بالإبلاغ في الوقت المناسب من منظور تنظيمي؛
- تزويد مجلس الإدارة بتعليقات على نتائج أداء أمن المعلومات؛
- تنبيه مجلس الإدارة إلى ما يستجد من تطورات تؤثر على المخاطر المتعلقة بالمعلومات وأمن المعلومات.

ولمراجعة أداء أمن المعلومات من وجهة نظر الإدارة، ينبغي للإدارة العليا أن تُقيّم أداء أمن المعلومات على أساس آثاره على المستوى التنظيمي ومستوى الكيان، لا على أساس فعالية الضوابط الأمنية وكفاءتها حصراً. ويمكن تحقيق ذلك بتنفيذ برنامج قياس الأداء لرصد فرص التحسين وتدقيقها وتحديدها، وربط أداء أمن المعلومات بأداء المنظمة والكيان.

5.3.7 الاتصال

"الاتصال" هو عملية إدارة ثنائية الاتجاه يتبادل بموجبها مجلس الإدارة معلومات مع الأطراف المهتمة على نحو يلبي احتياجاتهم الخاصة.

والطريقة التي يمكن استعمالها "للاتصال" هي بيان حالة أمن المعلومات التي توضح للأطراف المهتمة الأنشطة والمسائل المتعلقة بأمن المعلومات.

وأحد أسباب الاتصال هو السماح بمساءلة الكيانات أمام الأطراف المعنية مثل أصحاب الأسهم. وأصبح هذا الأمر أكثر أهمية، وتوفر المنظمات الآن معلومات عما تقوم به من تنفيذ وحفاظ على إدارة أمن المعلومات، إلى جانب فعاليتها في مجال إدارة المخاطر. وبالمثل، في حالة وقوع حادث يتعلق بأمن المعلومات، ينبغي أن تشرح الكيانات تأثير الضوابط وسببها وتغييراتها للتصدي لخطر تكرار الحوادث بالنسبة للأطراف المعنية، وبشكل منفصل بالنسبة إلى الجمهور، حسب الاقتضاء.

ويمكن إجراء الاتصال من خلال مجموعة متنوعة من الطرق. ويمكن أن يشمل أيضاً مجموعة متنوعة من المحتويات. وسيكون له أيضاً مجموعة متنوعة من الجماهير. وينبغي تصميم أي عملية اتصال لتأخذ الجمهور في الاعتبار، وكذلك الرسال التي يُقصد بها أن يفهمها الجمهور. ويتعين بعد ذلك استخدام هذين العاملين لتحديد محتوى الاتصال، وكذلك القنوات المستخدمة لتسليم الاتصال إلى الجمهور المقصود. ويرد مثال عن ذلك في الملحق C.

ولكي ينفذ مجلس الإدارة عملية "الاتصال":

– يتعين عليه القيام بما يلي:

- تقديم تقرير إلى الأطراف المعنية الخارجية عن أن الكيان يطبق مستوى معيناً من أمن المعلومات يتناسب مع طبيعة أنشطته وأولوياته؛
- تعيين وتحديد أولويات الالتزامات التنظيمية وتوقعات الأطراف المعنية ومتطلبات الكيان فيما يتعلق بأمن المعلومات؛
- تقديم المشورة للإدارة العليا للنظام ISMS في أي أمور تستدعي اهتمامها بها واتخاذ قرار بشأنها؛
- تزويد الأطراف المعنية بتعليمات حول الأهداف التفصيلية التي يجب اتخاذها دعماً لأوليات أمن المعلومات.
- تعزيز ثقافة أمن المعلومات الإيجابية؛
- تدريب الموظفين وغيرهم من الأشخاص في نطاق نظام إدارة أمن المعلومات والتواصل معهم بشأن مسؤولياتهم.

8 متطلبات مجلس الإدارة بشأن نظام إدارة أمن المعلومات

1.8 المنظمة ونظام إدارة أمن المعلومات

ينبغي أن يتطلب مجلس الإدارة تصميم نظام واحد أو أكثر لإدارة أمن المعلومات لدعم أهداف الكيان. وقد تكون أهداف كل نظام إدارة أمن المعلومات هي نفس أهداف الكيان الأصلي أو مختلفة عنها، اعتماداً على حجم الكيان بأكمله ونطاقه وهيكله، ولكن يتعين مواءمتها. ويوضح الملحق A العلاقات الممكنة بين إدارة أمن المعلومات وإدارة تكنولوجيا المعلومات.

وينبغي لمجلس الإدارة أن يتطلب أيضاً تصميم كل نظام لإدارة أمن المعلومات بحيث يتسق مع السياسات والعمليات العامة للكيان، بما في ذلك إدارة المخاطر. وقد يكون من المناسب أن يعتمد نظام إدارة أمن المعلومات نفس عملية تقييم المخاطر التي يعتمدها مجلس الإدارة، لتمكين إبلاغ المعلومات المتعلقة بالمخاطر بشكل واضح. وإذا استخدم مجلس الإدارة عملية لتقييم المخاطر لا تتفق مع متطلبات المعيار ISO/IEC 27001، فينبغي للنظام ISMS لدى المنظمة أن يستخدم، إذا رغبت المنظمة في تحقيق التوافق، نهجاً مختلفاً لتقييم المخاطر إزاء النهج الذي يستخدمه الكيان، وأن يتفق على طريقة لإبلاغ المعلومات المتعلقة بالمخاطر إلى مجلس الإدارة بشروط تتماشى مع نهج مجلس الإدارة. ومن ناحية أخرى، يمكن لمجلس الإدارة أن يختار تغيير عملية تقييم المخاطر الحالية للكيان لتتوافق مع متطلبات المعيار ISO/IEC 27001.

ويمكن لمجلس الإدارة أن يفرض استعمال النظام ISMS لإدارة المخاطر الاستراتيجية المتعلقة بفقدان الملكية الفكرية، والأضرار التي تلحق بالسمعة، والخسائر المالية المرتبطة بالضرر الذي يلحق بسرية المعلومات أو سلامتها أو توافرها.

ويمكن للنظام ISMS أن يزود مجلس الإدارة بمعلومات إدارية تتعلق بما يلي:

- المخاطر التي يتعرض لها الكيان؛
- فعالية نظام إدارة أمن المعلومات.

وينبغي أن يقوم مجلس الإدارة بما يلي:

- الموافقة على إنشاء كل نظام لإدارة أمن المعلومات؛
- تحديد نطاق كل نظام لإدارة أمن المعلومات وإصدار الشهادات (قد تختلف هذه النطاقات)؛
- توفير التوجيه لكل نظام لإدارة أمن المعلومات بما في ذلك الأهداف والمتطلبات والأدوار والموارد؛
- اتخاذ قرارات بشأن المستويات المقبولة للمخاطر المتبقية أو العلاجات المناسبة للمخاطر؛
- تزويد كل نظام لإدارة أمن المعلومات بقنوات الاتصال والسلطة اللازمة لاستخدام تلك القنوات لتوصيل المعلومات المناسبة إلى الأطراف المهتمة وجميع الأشخاص في نطاق نظام إدارة أمن المعلومات.

2.8 السيناريوهات (انظر الملحق B)

1.2.8 النوع A: منظمة ISMS هي الكيان بأكمله

في الحالات التي يكون فيها نظام الإدارة الوحيد المعمول به متوافقاً مع المعيار ISO/IEC 27001، يمكن استخدامه لتوفير معلومات عن المخاطر وبالتالي السماح للمنظمة بإدارة المخاطر المتعلقة بالمعلومات. ومع ذلك، ستظل هناك عمليات مختلفة لدعم إدارة تكنولوجيا المعلومات، والإدارة المالية، والإدارة التشغيلية، وغيرها من أنشطة الإدارة.

في الحالة التي تنطبق فيها منظمة ISMS على الكيان بأكمله:

- تظل عمليات الإدارة الموصوفة في الفقرة 3.7 دون تغيير؛
- تضطلع الإدارة العليا بمسؤوليات الإدارة بالإضافة إلى إدارة أمن المعلومات كإدارة الشركات.

يرجَّح أن تكون مواءمة أهدف المنظمة في مجال أمن المعلومات مع الأهداف العامة للكيان واضحة، لأن الإدارة العليا مسؤولة عن تحديد كليهما. وإذا كان دور واحد يتحمل مسؤولية تنظيم وإدارة أمن المعلومات على السواء، ينبغي تقديم المشورة الكافية لضمان فصل المساءلة فصلاً مناسباً عن وضع السياسات وتنفيذها.

2.2.8 النوع B: منظمة ISMS تشكل جزءاً من كيان أكبر

تشكل بعض منظمات ISMS جزءاً من كيان أكبر. وبما أن أنشطة الإدارة تنطبق عادة على كيان قانوني كامل أو شركة أو مؤسسة خيرية، أو هيئة عامة أو كيان آخر، فإن إدارة ذلك الكيان تمتد في هذه الحالة إلى خارج نطاق نظام إدارة أمن المعلومات. ويمكن أن يكون لدى المنظمة عدة أنظمة لإدارة أمن المعلومات داخل حدودها؛ وبالتالي، يمكن لمجلس الإدارة أن يحكم عدة أنظمة لإدارة أمن المعلومات. وتمت كتابة هذه الوثيقة في معظمها لإتاحة هذا النهج.

تظل عمليات الإدارة الأربع الموضحة في الفقرة في 3.7 ذات صلة. ومع ذلك، اعتماداً على العلاقة بين منظمة (منظمات) إدارة نظام أمن المعلومات والكيان الأم، يمكن أن تنطبق إحدى الحالات التالية:

- تعمل كل منظمة ISMS كجزء مستقل من الكيان الأم وبالتالي لديها أهداف أعمال خاصة بها. وفي هذه الحالة، يجب مواءمة أهداف أمن المعلومات لمنظمة ISMS مع أهداف الأعمال الخاصة بها.
- كل منظمة ISMS مسؤولة عن تحقيق واحد أو أكثر من أهداف أعمال كيانها الأم. وفي هذه الحالة، يجب مواءمة أهداف أمن المعلومات لمنظمة ISMS مع أهداف أعمال كيانها الأم.

أُسندت لكل منظمة ISMS مسؤولية إدارة جانب من جوانب مخاطر أمن المعلومات بالنيابة عن الكيان الأم، وفي هذه الحالة، ينبغي للكيان الأم أن يحدد أهداف أمن المعلومات لمنظمة ISMS، مما يضمن التوافق مع أهداف أعمال الكيان الأم.

ستكون هناك أيضاً علاقة بين الإدارة العليا لكل منظمة ISMS ومجلس إدارة الكيان الأم. ويمكن أن يكون فريق (أفرقة) الإدارة العليا ومجلس الإدارة هو نفسه، ويمكن أن يكون أو لا يكون له بعض الأعضاء المشتركين. وينبغي استخدام الشكل 1.B لتحديد الأفراد الذين ينبغي تعيينهم للاضطلاع بأدوار عضو مجلس الإدارة والطرف المعني.

3.2.8 النوع C: منظمة ISMS تضم أجزاءً من عدة كيانات

في هذه الحالة، تدير الإدارة العليا منظمة ISMS وتتحكم فيها كالمعتاد، بل وتشمل عدداً من الكيانات. ويمكن ملاحظة ذلك في الحالة التي يحكم فيها كيان أكبر، مجموعة من الكيانات التي تتشارك في سياق ومتطلبات مشتركة لأمن المعلومات بشأن مجموعة فرعية من أنشطتها، عندما يتم، مثلاً، جمع البيانات الشخصية ومعالجتها وتخزينها واستخدامها لتقديم خدمات. ويمكن لمجالس الإدارة المتعددة أيضاً تشارك نظام ISMS واحد؛ فمثلاً يمكن للمنظمة أن توفر نظام ISMS كخدمة يستعملها العديد من العملاء.

في الحالة التي تضم فيها منظمة ISMS أجزاءً من عدة كيانات:

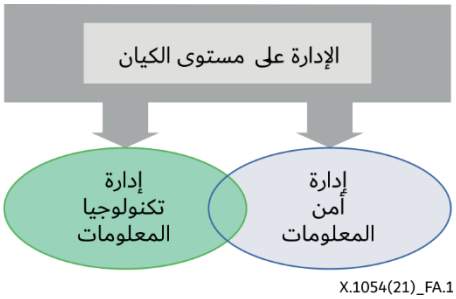
- تظل عمليات الإدارة الموصوفة في الفقرة 3.7 دون تغيير؛
- ينبغي مواءمة أهداف أمن المعلومات لمنظمة ISMS مع أهداف الأعمال المتبادلة التي تربط بين الكيانات الأعضاء.

الملحق A

علاقات الإدارة

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

يبيّن الشكل 1.A العلاقة بين إدارة أمن المعلومات وإدارة تكنولوجيا المعلومات.



الشكل 1.A – 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. ويمكن معالجة مخططي الإدارة كليهما باتباع عمليات الإدارة التالية: التقييم والتوجيه والرصد والاتصال.

الملحق B

أنواع المنظمة ISMS

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

هناك ثلاثة أنواع من العلاقات بين منظمة تدير النظام ISMS، وكيان يطبق النظام ISMS. وتؤثر هذه العلاقات أيضاً على أعضاء الإدارة العليا للنظام ISMS ومجلس إدارة الكيان. وتوضح القائمة أدناه والشكل 1.B هذه الأنواع من العلاقات.

النوع A: الكيان والمنظمة ISMS متماثلان.

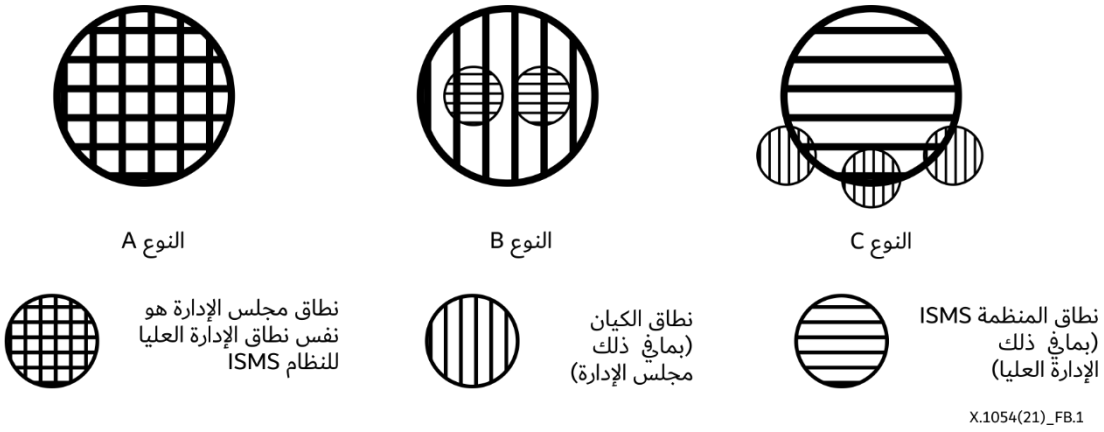
- مجلس الإدارة هو نفس الإدارة العليا للنظام ISMS.

النوع B: يضم الكيان المنظمة ISMS (وقد يكون أكثر من نظام ISMS واحد قيد التشغيل داخل هذا الكيان):

- يجوز أن يكون بعض أعضاء مجلس الإدارة أعضاءً في أي نظام ISMS، ولكن لن تكون العضوية متطابقة.

النوع C: تتشارك عدة كيانات في نظام ISMS واحد:

- إذا كان للكيانات مصلحة مباشرة في النظام ISMS، يمكن أن يكون لمجلس الإدارة لكل كيان عضوية في الإدارة العليا للنظام ISMS؛
- إذا قام طرف ثالث بتوفير النظام ISMS كخدمة، فمن غير المرجح أن تضم عضوية الإدارة العليا للنظام ISMS أعضاءً من مجالس إدارة الكيانات التي تتشارك في النظام ISMS.



الشكل 1.B – العلاقات الممكنة لكيان (كيانات) ونظامه (أنظمته) ISMS

الملحق C

أمثلة الاتصال

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

يُلاحظ أحد الأمثلة على الاتصالات في أسواق الأوراق المالية حيث تلتزم الشركات بالكشف عن مخاطر أمن المعلومات بسبب القوانين أو قواعد الصناعة. وثمة مثال آخر هو التقرير البيئي والاجتماعي والإداري (ESG) كوسيلة للمنظمات لشرح/إبلاغ الأطراف المعنية بجهودها من المنظورات البيئية والاجتماعية والاقتصادية. وتصف بعض التقارير البيئية والاجتماعية والإدارية النُهج المتبعة في حماية بيانات الخصوصية وأنشطة أمن المعلومات وإدارة الأزمات من أجل منع الحوادث الأمنية.

وينبغي أن تراعي أنشطة تصميم الاتصالات أيضاً الآثار غير المقصودة المتمثلة في سوء فهم الجمهور أو استنتاج محتوى إضافي، والاتصالات التي تصل إلى أشخاص غير الجمهور المقصود.

بيبليوغرافيا

[1] Recommendation ITU-T X.1051 (2016) | ISO/IEC 27011:2016, *Information technology – Security techniques – Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations*.

[2] ISF, Standard of Good Practice for Information Security: 2018.

[3] ISO 37001:2016, *Anti-bribery management systems – Requirements with guidance for use*.

[4] ISO/IEC 9001:2015, *Quality management systems – Requirements*.

[5] ISO/IEC 27000:2018, *Information security, cybersecurity and privacy protection – Overview and vocabulary*.

[6] ISO/IEC 27002:2013, *Information security, cybersecurity and privacy protection – Code of practice for information security controls*.

[7] ISO/IEC 38500:2015, *Information technology – Governance of IT for the organization*.

[8] ISO Guide 73:2009

[9] IT Governance Institute (ITGI), *Information Security Governance: Guidance for Information Security Managers: 2008*.

[10] ITGI, *Information Security Governance Guidance for Boards of Directors and Executive Management*, 2nd Edition: 2006.

[11] ITGI, *COBIT Control Practices: Guidance to Achieve Control Objective for Successful IT Governance*, 2nd Edition: 2007.

[12] Ohki E., Harada Y., Kawaguchi S., Shiozaki T., Kgaua T., *Information Security Governance framework, Proceedings of the first ACM workshop on Information security governance*, pp. 1-6, 2009.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي
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	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
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، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2022