المواصفة القياسية الدولية

أيــزو/ اللجنة الدولية الكهروتقنية
٢٧٠٠٦

الترجمة الرسمية
Official translation
Tradition officials

الإصدار الثالث
٢٠١٥-١٠-٠١

تكنولوجيا المعلومات -- تقنيات الأمن – متطلبات جهات التدقيق وإصدار الشهادات لنظم إدارة أمن المعلومات

Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems (E)

Technologies de l'information — Techniques de sécurité — Exigences pour les organismes procédant à l'audit et à la certification dessystèmes de management de la sécurité de l'information(F)

طبعت في الأمانة المركزية ISO في جنيف، سويسرا كترجمة عربية رسمية بالإنابة عن١٠هيئات أعضاء في ISOالتي أعتمدت دقة الترجمة (انظر القائمة في صفحة ii).

الرقم المرجعى
ISO\IEC 27006:2015 (A)
الترجمة الرسمية

جهات التقييس العربية التي اعتمدت المواصفة

■ مؤسسة المواصفات والمقاييس الأردنية	الأردن
■ هيئة الإمارات للمواصفات والمقاييس	الإمارات
■ المعهد الجزائري للتقييس	الجزائر
■ الهيئة السعودية للمواصفات والمقاييس	السعودية
■ الجهاز المركزي للتقييس والسيطرة النوعية	العراق
■ الهيئة العامة للصناعة	الكويت
■ الهيئة السودانية للمواصفات والمقاييس	السودان
■ الهيئة اليمنية للمواصفات والمقاييس وضبط الجودة	اليمن
■ المعهد الوطني للمواصفات والملكية الصناعية	تونس
■ هيئة المواصفات والمقاييس العربية السورية	سوريا
■ المركز الوطني للمواصفات والمعايير القياسية	ليبيا
■ الهيئة المصرية العامة للمواصفات والجودة	مصر

مكتب حقوق ملكية المنظمة الدولية للتقييس
الرمز البريدي: ٥٦ -Ch-1211- جنيف ٢٠
هاتف: ٠٠٤١٢٢٧٤٩٠١١١
فاكس: ٠٠٤١٢٢٧٤٩٠٩٤٧
بريد الكتروني: copyright@iso.org
الموقع الالكتروني: www.iso.org

تم نشر النسخةالعربية في٢٠١٧
تم النشر في سويسرا

المحتويات

تمهيد

الأيزو (المنظمة الدولية للتقييس) هي اتحاد عالمي لجهات التقييس الوطنية (الجهات الأعضاء في الأيزو)،وغالبا مايتم إعداد المواصفات الدولية من خلال اللجان الفنية للأيزو،وإذا كانت الجهة العضو لها اهتمام بموضوع قد شُكِّلت له لجنة فنية، فإن لهذا العضو الحق في أن يكون له ممثّل في تلك اللجنة.ويشارك في العمل كذلك المنظمات الدولية الحكومية منها وغير الحكومية، التي لها تواصل مع الأيزو.وتتعاون الأيزو تعاونا وثيقا مع اللجنة الدولية الكهروتقنية (IEC) في جميع الأمور التي تهم التقييس في المجال الكهرو تقني.

وتصاغ المواصفات الدولية وفقا للوائح الواردة في توجيهات الأيزو/أي إي سي - الجزء الثاني.
المهمة الرئيسية للجان الفنية هو اعداد المواصفات الدولية. ويتم توزيع مشاريع المواصفات الدولية على الهيئات الوطنية للتصويت.ويتطلب اصدار هذه المشاريع كمواصفات دولية موافقة ٧٥% على الأقل من الهيئات الوطنية التي يحق لها التصويت.

ونود لفت الانتباه إلى احتمالية أن تكون بعض عناصر هذه الوثيقة خاضعة لحقوق براءة الاختراع. ولن تتحمل المنظمة الدولية للتقييس (ISO) مسؤولية تحديد أيّ من هذه الحقوق أو جميعها.

وقد تم إعداد مواصفة الأيــزو/ اللجنة الدولية الكهرو تقنية٢٧٠٠٦ بواسطة اللجنة الفنية، الخاصة ب المشتركة ISO / IEC JTC 1 ، تكنولوجيا المعلومات، اللجنة الفرعية SC 27 ، تقنيات الأمن.
تلغى هذه الطبعة الثالثة، الطبعة الثانية (ISO / IEC 27006: 2011) حيث تم تنقيحها من الناحية الفنية،

مقدمة

تضع المواصفة ايزو/ اي إي سي ١٧٠٢١ المعايير للجهات القائمة على تدقيق ومنح الشهادات لنظم الإدارة للمنظمات. فإن كان لهذه المنظمات أن تعتمد كممتثلة للمواصفة ايزو/ اي إي سى ١٧٠٢١ بهدف تدقيق ومنح الشهادة لنظم إدارة أمن المعلومات (ISMS)طبقا للمواصفة ايزو/ اي إى سى ٢٧٠٠١: ٢٠٠٥، فإن هناك متطلبات وإرشادات إضافية ضرورية للمواصفة ايزو/ اي إى سى ١٧٠٢١. وهو ما تقدمه هذه المواصفة الدولية.

يتبع النص في هذه المواصفة الدولية نفس هيكل المواصفة ايزو/ اي إى سى ١٧٠٢١، وقد تم تمييز المتطلبات والإرشادات الإضافية الخاصة بنظم إدارة أمن المعلومات (ISMS)عند تطبيق المواصفة ايزو/ اي إى سى ١٧٠٢١-١، فى منح الشهادات لنظم إدارة أمن المعلومات (ISMS) بالأحرف"IS" " أ م ".

يستخدم التعبير " يجب " فى هذه المواصفة الدولية لبيان تلك الأحكام التي تعكس إلزامية متطلبات المواصفتين ايزو/ اي إى سى ١٧٠٢١وايزو/ اي إى سى ٢٧٠٠١. فيما يستخدم التعبير " ينبغي " ليحمل معنى التوصية والنصح والتفضيل.

والهدف الأولى لهذه المواصفة الدولية هو تمكين جهات الاعتماد من تناغم أكثر فعالية في تطبيقها للمعايير التي تلتزم بها عند تقييم جهات التصديق (منح الشهادات).

خلال هذه المواصفة الدولية يستخدم المصطلحان "نظام الإدارة" و"النظام " بالتبادل. تعريف نظام الإدارة وارد بالمواصفة الدولية ايزو ٩٠٠٠: ٢٠٠٥. ولا ينبغي أن يختلط على الملتقى، "نظام الإدارة" كما هو مستخدم في هذه المواصفة الدولية مع أنواع الأنظمة الأخرى مثل نظام تقنية المعلومات.

تكنولوجيا المعلومات - تقنيات الأمن – متطلبات جهات التدقيق والتصديق (إصدار الشهادات) لنظم إدارة أمن المعلومات

١- المجال

تحدد هذه المواصفة الدولية المتطلبات وتقدم الإرشادات لجهات تقديم التدقيق وإصدار الشهادات لنظم إدارة أمن المعلومات بالإضافة إلى المتطلبات الواردة في المواصفة ايزو/ اي إى سى ١٧٠٢١والمواصفة ايزو/ اي إى سي ٢٧٠٠١. والمقصود هنا في المقام الأول هودعم اعتماد جهات التصديق (منح الشهادات) التي تصدر الشهادات لنظم إدارة أمن المعلوماتISMS.

المتطلبات الواردة في هذه المواصفة الدولية بحاجة إلى إظهارها بدلالة الاقتدارو الاعتمادية، من قبل أي جهة تقوم بمنح شهادات نظم إدارة أمن المعلومات، وتقدم الإرشادات الواردة في هذه المواصفة الدولية تفسيرات إضافية لتلك المتطلبات لأي جهة مانحة للشهادات

ملحوظة: يمكن أن تستخدم هذه المواصفة الدولية كمستند / كوثيقة معايير للاعتماد أو للتقييم من قبل الأقران أو غير ذلك من عمليات التدقيق.

٢- المراجع التكميلية

المستندات التالية، بكاملها أو أجزاء منها، استخدمت كمراجع معيارية لهذه المواصفة، ولا عوض عنهاعند التطبيق . وعند الإشارة لمراجع قديمة (ملغاة)، يعتد فقط بالإصدار الوارد ذكره هنا وفيما عدا ذلك يعتد بالإصدار الأخير من المراجع المشار إليها (مع أخذ أية تعديلات أو تصحيحات في الاعتبار).

ISO/IEC 17021-1:2015, *Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements*

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*
ISO/IEC 27001:2013, *Information technology — Security techniques —*

Information security management systems — Requirements

٣- المصطلحات والتعاريف

لأغراض هذه المواصفة تسري المصطلحات والتعاريف الواردة في المواصفة الدولية ايزو/ اي إى سى ١٧٠٢١ والواردة في المواصفة الدولية ايزو/ اي إى سى ٢٧٠٠٠ إلى جانب المصطلحات التالية:

١/٣ مستندات التصديق

المستندات المبينة أن نظام إدارة أمن المعلومات للمنظمة العميل مطابق لمواصفات نظام إدارة أمن المعلومات المحددة وأي وثائق إضافية مطلوبة طبقا للنظام.

٤- المبادئ

تنطبق المبادئ الواردة في المواصفة ايزو/ اي إيسي ١٧٠٢١-١، في البند ٤

٥ ـ المتطلبات العامة

١/٥ الشئون القانونية والتعاقدية
تنطبق المتطلبات الواردة في المواصفة ايزو/ اي إي سي ١٧٠٢١-١، في البند ١/٥

٢/٥ إدارة الحيادية
تنطبق المتطلبات الواردة في المواصفة ايزو/ اي إي سي ١٧٠٢١-١، في البند ٢/٥، بالإضافة إلى المتطلبات والتوجيهات التالية الخاصة بنظام إدارة أمن المعلومات.

١/٢/٥ أ م ٢/٥ تعارض الاهتمامات (المصالح)
يمكن لجهات منح الشهادات إجراء المهام التالية دون أن تعد من قبيل الاستشارات أوالتعارض المحتمل في الاهتمامات:

أ) الترتيب والمشاركة كمحاضر في دورات تدريبية، شريطة أنه، إذا كانت هذه الدورات ذات علاقة بإدارة أمن المعلومات، أو نظم الإدارة ذات الصلة أوالتدقيق، تقتصر جهات المنح على تقديم المعلومات الأساسية والمشورة المتاحة اتاحة عامة، بمعنى أنه لا يجوز لجهة المنح تقديم المشورة الخاصة بشركة بعينها بما يتعارض مع متطلبات الفقرة (ب) التالية؛

ب) الإتاحة أو النشر عند الطلب للمعلومات التي تصف تفسير جهة إصدارالشهادات لمتطلبات معايير تدقيق منح / إصدار الشهادات (انظر ٦/٣/١/٩)؛

ج) أنشطة ما قبل المراجعة، الهادفة فقط إلى تحديد الاستعداد (الجاهزية) لتدقيق التصديق (إصدار / منح الشهادات)، ومع ذلك، فلا يجوزأن تؤدي مثل هذه الأنشطة إلى تقديم توصيات أو نصائح منشأنها أن تخالف هذا البند ويجب على جهة إصدار الشهادات أن تكون قادرة على تأكيد أن مثل هذه الأنشطة لاتتعارض مع هذه المتطلبات وأنها لن يتماس تخدامه التبريرالانتهاء إلى انتقاص مدة التدقيق الكلية لمنح الشهادات؛

د) إجراء تدقيق الطرف الثاني والطرف الثالث وفقا لمعايير أوتنظيمات أخرى غير تلك التي تعد جزءا من مجال الاعتماد؛

ه) إضافة القيمة خلال عمليات تدقيق التصديق (منح الشهادة) وخلال زيارات المراقبة، على سبيل المثال، عن طريق تحديد فرص التحسين، حيث تصبح واضحة أثناءعملية المراجعة، دون التوصية بحلول بعينها.

يجب أن تكون جهة إصدار الشهادات مستقلة عن الجهة أوالجهات (بما في ذلك الأفراد) التي تقدم التدقيق الداخلي لنظام إدارة أمن المعلومات للمنشأة العميل الخاضعة لتدقيق المنح. وفوق ذلك تكون جهة التصديق مستقلة عن الجهة أو الجهات (بما فيهم من أفراد) التي تقوم بالتدقيق الداخلي لنظم إدارة أمن المعلومات

٣/٥ الالتزامات والتمويل
تنطبق المتطلبات الواردة في المواصفة ايزو/ اي إيسي ١٧٠٢١-١، في البند ٣/٥.

٦ ـ المتطلبات الهيكلية

تنطبق المتطلبات الواردة في المواصفة ايزو/ اي إيسي ١٧٠٢١-١، في البند ٦.

٧ ـ متطلبات الموارد

١/٧ كفاءات الأفراد

تنطبق المتطلبات الواردة في ايزو/ اي إي سي ١٧٠٢١-١في البند ١/٧ وبالإضافةإلى ذلك، تنطبق المتطلبات والتوجيهات التالية:

١/١/٧ أ م ١/١/٧ اعتبارات عامة

١/١/١/٧ متطلبات الكفاءةالعامة/ الأولية

يجب أن تتحقق جهة التصديق من أن لديها المعرفة بالتطورات التقنية والقانونية والتنظيمية ذات العلاقة بنظام إدارة أمن المعلومات للعميل الذي تقوم بتقييمه.
يجب أن تحدد جهة التصديق متطلبات الكفاءة لكل من وظائف / مهام التصديق على النحو المشار إليه في الجدول أ-١ من المواصفة ايزو/ اي إيسي ١٧٠٢١-١. تأخذ جهة التصديق فى اعتبارها المتطلبات الموصفة في ايزو/ اي إيسي ١٧٠٢١-١والفقرات ٢/١/٧ و١/٢/٧ من هذه المواصفة الدولية وذات العلاقة بجوانبنظام أمن المعلومات التقنية على النحو المحدد من قبل جهة التصديق.

ملحوظة: يقدم المرفق أ ملخصا لمتطلبات الكفاءة للأفراد المشاركين فى وظائف التصديق المحددة

٢/١/٧ أ م ٢/١/٧تحديد معايير الكفاءة

١/٢/١/٧ متطلبات الكفاءةلتدقيق نظام إدارة أمن المعلومات

١/٢/١/٧ /١المتطلبات العامة

يجب أن تكون لجهة التصديق معاييرها للتحقق من خلفية الخبرات والتدريب الخاص أو سيرا مختصرة لأفراد فريق التدقيق التي توكد ما يلي كحد أدنى:

أ) المعرفة بأمن المعلومات؛
ب) المعرفة التقنية بالنشاط المطلوب تدقيقه.
ج) المعرفة بنظم الإدارة؛
د) المعرفة بمبادئ التدقيق

ملحوظة: تقدم المواصفة.ISO 19011 مزيدا من المعلومات عنمبادئالتدقيق

ه) المعرفة بمراقبة وقياسات وتحليل وتقييم نظم إدارة أمن المعلومات ISMS

تنطبق هذه المتطلبات من أ) إلى ه) على كافة المدققين الذين يشكلون جزءا من فريق التدقيق باستثناء ب)، حيث يتشاركها أعضاء الفريق.
يجب أن يكون فريق التدقيق على اقتدار يمكنه من تتبع علامات / ظواهر واقعات التأمين فى نظام إدارة أمن المعلومات للمنشأة العميل، عكسيا حتى العناصر المناسبة فى نظام إدارة أمن المعلومات.
يجب أن يتمتع فريق التدقيق بخبرة العمل المناسبة والتطبيق العملي للبنود/ للعناصر المذكورة أعلاه (وهذا لا يعني أن المدقق يحتاج إلى كامل مدى الخبرات في جميع مجالات أمن المعلومات، ولكن يجب أن تتوفر لفريق المراجعة ككل ما يكفي من التقدير والخبرة لتغطية مجال التدقيق لنظام إدارة أمن المعلومات ISMS).

٢/١/٢/١/٧ مصطلحات ومبادئ وممارسات وتقنيات أمن المعلومات

عموما، يجب على أن تكون لدى جميع أفراد فريق التدقيق المعارف التالية:

أ) هياكل التوثيق الخاصة بنظم إدارة أمن المعلومات وتدرجها وعلاقاتها البينية؛
ب) الأدوات والطرق والتقنيات ذات الصلة بنظم إدارة أمن المعلومات وتطبيقاتها؛
ج) تقدير وإدارة المخاطر الخاصة بأمن المعلومات ؛
د) المعلومات المنطبقة على نظم إدارة أمن المعلومات ؛
ه) التقنيات الحالية حيث أمن المعلومات وارد أو جدير بالاعتبار
يجب على كل مدقق أن يفي بالعناصر أ) وج) ود)

٣/١/٢/١/٧ مواصفات نظم إدارة أمن المعلومات ومستنداتها المعيارية

يجب أن يكون المدققون المشاركون في تدقيق نظم إدارة أمن المعلومات بما يلي:
أ) كافة المتطلبات الواردة في المواصفة ايزو/ اي سي ٢٧٠٠١
عموما،يجب أن يكون لدى كل أعضاء فريق التدقيق المعارف التالية:
ب) كافة الضوابط الواردة في المواصفة ايزو/ اي سي ٢٧٠٠٢ (إذا ما حدد أنها أيضا ضرورية منظور مواصفات قطاعية) وكيفية تطبيقها، مصنفة على النحو التالي:
١) سياسات أمن المعلومات
٢) تنظيم أمن المعلومات
٣) أمن الموارد البشرية
٤) إدارة الأصول
٥) ضبط الوصول متضمنا منح الصلاحيات
٦) التشفير
٧) الأمن المادي والبيئي
٨) أمن العمليات بما فيها خدمات تقنيات المعلومات
٩) أمن الاتصالات، بما فيها إدارة أمن الشبكات وتحويل / نقل المعلومات
١٠) اقتناء النظم وتطويرها وصيانتها
١١) علاقات الموردين متضمنة الخدمات ذات المصدر الخارجي
١٢) إدارة واقعات أمن المعلومات،
١٣) جوانب أمن المعلومات فيما يختص بإدارة استمرارية الأعمال
١٤) الامتثال، متضمنا مراجعات أمن المعلومات

٤/١/٢/١/٧ ممارسات إدارة الأعمال

يجب أن تكون لدى المدققين المشاركين في تدقيق نظام إدارة أمن المعلومات
أ) الممارسات الجيدة لأمن معلومات الصناعة وإجراءات أمن المعلومات
ب) سياسة ومتطلبات الأعمال لأمن المعلومات
ج) مفاهيم إدارة أمن المعلومات العامة والممارسات والعلاقات البينية بين السياسات والأهداف والنتائج
د) عمليات الإدارة والمصطلحات ذات العلاقة.
ملحوظة: تتضمن هذه العمليات أيضا دارة الموارد البشرية والاتصالات الداخلية والخارجية وغيرها من عمليات الدعم ذات العلاقة.

٥/١/٢/١/٧ قطاع أعمال العميل

يجب أن تكون لدى المدققين المشاركين في تدقيق نظام إدارة أمن المعلومات المعارف التالية:
أ) المتطلبات القانونية والتنظيمية في مجال بعينه لأمن المعلومات أو نطاق جغرافي بعينه أو تحت مظلة نظام قضائي بعينه.

ملحوظة: لا تقتضي معرفة المتطلبات القانونية والتنظيمية خلفية قانونية مسبقة.

ب) مخاطر أمن المعلومات المرتبطة بهذا القطاع من الأعمال.

ج) المصطلحات والعمليات والتقنيات ذات العلاقة بقطاع أعمال العميل.

د) الممارسات ذات العلاقة بقطاع الأعمال.

قد يكون المعيار أ) مشتركا بين فريق العمل.

٦/١/٢/١/٧ منتجات وعمليات ومنشأة العميل

عموما، يجب أن تكون لدى المدققين المشاركين في تدقيق نظام إدارة أمن المعلومات المعارف التالية:

أ) أثار نوع المنشأة وحجمها وحوكمتها وهيكلها ووظائفها وعلاقاتها على تطوير وتنفيذ نظام إدارة أمن المعلومات وأنشطة التصديق، متضمنة الاستعانة بالخبرات من الخارج.

ب) العمليات المعقدة من المنظور الواسع.

ج) المتطلبات القانونية والتنظيمية المنطبقة على المنتج أو الخدمة.

٢/٢/١/٧ متطلبات الكفاءة لقيادة فريق تدقيق نظام إدارة أمن المعلومات

بالإضافة إلى المتطلبات الواردة في ١/٢/١/٧، يجبفي قادة الفرق بالمتطلبات التالية،التي يجب أن تبدى في الدقيقات التي تجرى تحت إشرافهم وبإرشاداتهم.

أ) معارف ومهارات إدارة عمليات التدقيق للتصديق، وفريق التدقيق.

ب) بيان القدرة على التواصل بفعالية،شفاهية وكتابة.

٣/٢/١/٧ متطلبات الكفاءة لإجراء مراجعة الطلب

١/٣/٢/١/٧ مواصفات نظم إدارة أمن المعلومات ومستنداتها المعيارية

يجب أن يكون لدى الأفراد القائمين بمراجعة الطلبات لتحديد كفاءات فريق التدقيق، لاختيار أعضاء الفريق وتحديد زمن التدقيق، المعارف التالية:

أ) مواصفات نظم إدارة أمن المعلومات ومستنداتها المعيارية ذات العلاقة والمستخدمة في عملية التصديق.

٢/٣/٢/١/٧ قطاع أعمال العميل

يجب أن يكون لدى الأفراد القائمين بمراجعة الطلبات لتحديد كفاءات فريق التدقيق، لاختيار أعضاء الفريق وتحديد زمن التدقيق، المعارف التالية:

أ) المصطلحات والعمليات والتقنيات والمخاطر الأولية ذات العلاقة بقطاع أعمال العميل.

٣/٣/٢/١/٧ منتجات وعمليات ومنشأة العميل

يجب أن يكون لدى الأفراد القائمين بمراجعة الطلبات لتحديد كفاءات فريق التدقيق، لاختيار أعضاء الفريق وتحديد زمن التدقيق، المعارف التالية:

أ) منتجات العميل وعملياته ونوع المنشأة وحجمها وحوكمتها وهيكلها ووظائفها وعلاقاتها على تطوير وتنفيذ نظام إدارة أمن المعلومات وأنشطة التصديق،متضمنة الوظائف الاستعانة بالخبرات من الخارج.

٤/٢/١/٧ متطلبات الكفاءة لمراجعة تقارير التدقيق وصناعة قرارات التصديق

١/ ٤/٢/١/٧ عام

يجب أن يكون لدى الأفراد القائمين بمراجعة تقارير التدقيق وصناعة قرارات التصديق، المعارف التي تمكنهم من تمحيص ملائمة مجال التصديق وكذلك التغييرات على المجال وأثارها على فعالية التدقيق، وعلى سبيل الخصوص الصلاحية المستمرة لتمييز الواجهات والاعتماديات والمخاطر المرتبطة:
إضافة إلى ذلك، يجب أن يكون لدى الأفراد القائمين بمراجعة تقارير التدقيق وصناعة قرارات التصديق، المعارف في:

أ) نظم الإدارة عموما
ب) عمليات وإجراءات التدقيق
ج) مبادئ وممارسات وتقنيات التدقيق

٢/٤/٢/١/٧ مصطلحات ومبادئ وممارسات وتقنيات أمن المعلومات

يجب أن يكون لدى الأفراد القائمين بمراجعة تقارير التدقيق وصناعة قرارات التصديق، المعارف التالية:

أ) البنود الواردة في ٢/١/٢/١/٧ أ) وج) ود)
ب) المتطلبات القانونية والتنظيمية ذات العلاقة بأمن المعلومات.

٣/٤/٢/١/٧ مواصفات نظم إدارة أمن المعلومات ومستنداتها المعيارية

يجب أن يكون لدى الأفراد القائمين بمراجعة الطلبات لتحديد كفاءات فريق التدقيق،لاختيار أعضاء الفريق وتحديد زمن التدقيق، المعارف التالية:

أ) مواصفات نظم إدارة أمن المعلومات ومستنداتها المعيارية ذات العلاقة والمستخدمة في عملية التصديق.

٤/٤/٢/١/٧ قطاع أعمال العميل

يجب أن يكون لدى الأفراد القائمين بمراجعة تقارير التدقيق وصناعة قرارات التصديق، المعارف التالية:

أ) المصطلحات والعمليات والتقنيات والمخاطر الأولية ذات العلاقة بقطاع أعمال العميل.

٥/٤/٢/١/٧ منتجات وعمليات ومنشأة العميل

يجب أن يكون لدى الأفراد القائمين بمراجعة تقارير التدقيق وصناعة قرارات التصديق، المعارف التالية:

أ) منتجات العميل وعملياته ونوع المنشأة وحجمها وحوكمتها وهيكلها ووظائفها وعلاقاتها

٢/٧ العاملون المشاركون في أنشطة منح الشهادات

تنطبق المتطلبات الواردة في المواصفة ايزو/ اي إي سي ١٧٠٢١-١ في البند ٢/٧. وبالإضافة إلى ذلك، تنطبق المتطلبات والتوجيهات التالية

١/٢/٧ أ م ١/٢/٧ بيان معارف وخبرات أفراد جهات التدقيق

يجب أن تبين جهات منح الشهادات معارف وخبرات أفراد جهات التدقيقمن خلال:

أ) مؤهلات معترف بها فيما يختص بنظم إدارة أمن المعلوماتISMS
ب) التسجيل كمدقق – حال كون ذلك منطبقا
ج) الاشتراك في البرامج التدريبية فينظم إدارة أمن المعلومات ISMSوتقديم المستندات الدالة على ذلك عند الطلب

د) الحفاظ على سجلات محدثة للتنمية المهنية
ه) شهود عمليات تدقيق نظم إدارة أمن المعلوماتمن قبل مدقق آخر في نفس المجال

١/١/٢/٧اختيار المدققين

بالإضافة إلى ١/٢/١/٧ يجب أن يوكد معايير اختيار المدققين أن يكون كل منهم:
أ) لديه تعليم أو تدريب مهني على مستوى يكافئ الدرجة الجامعية
ب) خبرة عملية أربع سنوات على الأقل من العمل بوقت كامل في مكان العمل في مجال تكنولوجيا المعلومات،منها سنتان على الأقل في دورأووظيفة تتعلق بأمن المعلومات؛
ج) إكمال خمسة أيام من التدريب بنجاح،يغطى مجالها تدقيقات نظام إدارة أمن المعلومات ISMS وإدارة التدقيق مما يعد مناسبا؛
د) خبرة مكتسبة في كامل عملية تقييم أمن المعلومات قب لتحمل مسؤولية الأداء كمدقق.يجب أن تكون هذه الخبرة مكتسبة من خلال المشاركة في أربعة تدقيقات شهادة على الأقل، فيما لا يقل مجموعه عن عشرين يوما، تتضمن مراجعة الوثائق وتحليل المخاطر،وتقييم التنفيذ وتقارير التدقيق؛
ه) خبرة حالية ذات علاقة مناسبة.
و) الحفاظ على حداثة معارفهم ومهاراتهم في مجال أمن المعلومات والتدقيق، من خلال التطوير المهني المستمر.
يجب أن يمتثل الخبراءالفنيون للمعايير أ)، وب)، وهـ)

٢/١/٢/٧ اختبار المدققين لقيادة الفريق
بالإضافة إلى الشروط الواردة في ٢/١/٢/٧و ١/١/٢/٧،يجب أن تكون معايير اختيار مدقق كقائد للفريق مؤكدة أن يكون المدقق

أ) قد شارك فى كافة المراحل لثلاثة عمليات كاملة على الأقل لتدقيق نظام لإدارة أمن المعلومات.ISMS يجب أن تتضمن المشاركة صياغة المجال الأولية والتخطيط، ومراجعة الوثائق وتقدير المخاطر وتقييم التطبيق وتقديم التقريرالرسمي للتدقيق.

٣/٧ استخدام المدققين الخارجيين الأفراد والخبراء الفنيين الخارجيين

تنطبق المتطلبات الواردة فى ايزو/ اي إى سى ١٧٠٢١- ١البند ٣/٧ وبالإضافة إلى ذلك، تنطبق المتطلبات والتوجيهات التالية الخاصة بنظام إدارة أمن المعلومات .ISMS

١/٣/٧ أ م ٣/٧ استخدام المدققين الخارج يين أوالخبراء الفنيين الخارجيين كجزء من فريق التدقيق
يجب أن يعمل الخبراءالفنيون تحت إشراف مدقق. الحد الأدنى من المتطلبات الواجب توافرها فى الخبراء الفنيين واردة فى الفقرة ٧-٢-١-١.

٤/٧ سجلات الموظفين

تنطبق المتطلبات الواردة فى المواصفة ايزو/ اي إى سى ١٧٠٢١-١ فى البند ٤/٧.

٥/٧ الاستعانة بمصادر خارجية

تنطبق المتطلبات الواردة فى المواصفةايزو/ اي إى سى ١٧٠٢١-١ فى البند ٥/٧.

٨ ـ متطلبات المعلومات

١/٨ المعلومات العامة

تنطبق المتطلبات الواردة فى ايزو/ اي إى سى ١٧٠٢١-١،البند ١/٨.