

أيزو/ اللجنة الدولية الكهروتقنية
٢٧٠٠٦

الموافقة القياسية الدولية

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 des systèmes de management de la sécurité de l'information(F) 2015

<https://standards.iteh.ai/catalog/standards/sist/a2a247e8-6734-4b30-977c-1f681baca265/iso-iec-27006-2015>

طبعت في الأمانة المركزية ISO في جنيف، سويسرا كترجمة عربية رسمية بالإنابة عن ١٠ هيئات أعضاء في ISO التي أعتمدت دقة الترجمة (انظر القائمة في صفحة ii).

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

©ISO 2015



إخلاء مسؤولية (تنويه)

قد يحتوي هذا الملف (PDF) على خطوط مدمجة، وبموجب سياسة الترخيص لـ Adobe فإنه يمكن طباعة هذا الملف أو الإطلاع عليه، على الأَن يتم تعديله ما لم تكن الخطوط المدمجة فيهم خصبة ومحملة في الحاسوب الذي يتم فيه التعديل وتحمُل الأطراف - عند تنزيل هذا الملف - مسؤولية عدم الإخلال بسياسة الترخيص لـ Adobe، في حين أن السكرتارية العامة للأيزو لا تتحمل أي مسؤولية قانونية حيال هذا المجال.

تعد الـ **Adobe** علامة تجارية مسجلة للشركة المتحدة لنظم الـ

يمكن الحصول على جميع التفاصيل الخاصة بالبرامج المستخدمة في إنشاء هذا الملف من المعلومات العامة المتعلقة بملف(PDF)، ولأجل الطباعة فقد حُسنت المتغيرات الداخلية في إنشاء (PDF)، حيث رُوعي أن يكون استخدام هذا الملف ملائماً لأعضاء المنظمة الدولية للتقييس ، وفي حالة حدوث أي مشكلة تتعلق بهذا الملف ، يُرجى إبلاغ السكرتارية العامة على العنوان المسجل أدناه.

جهات التقييس العربية التي اعتمدت المواصفة

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



وثيقة حماية حقوق الطبع والنشر
© ٢٠١٥

جميع الحقوق محفوظة. وما لا يرد خلاف ذلك، لا يجوز إعادة إنتاج أي جزء من هذا الإصدار أو استخدامه بأي شكل أو بأي وسيلة الكترونية أو ميكانيكية بما في ذلك النسخ والأفلام الدقيقة دون إذن خطى إما من المنظمة الدولية للتقييس على العنوان أدناه أو أحد الهيئات الأعضاء في المنظمة الدولية للتقييس في دولة الجهة الطالبة.

مكتب حقوق ملكية المنظمة الدولية للتقييس
الرمز البريدي: ٥٦ - Ch-1211 - جنيف ٢٠

هاتف: ٠٠٤١٢٢٧٤٩٠١١١
فاكس: ٠٠٤١٢٢٧٤٩٠٩٤٧

بريد الكتروني: copyright@iso.org

الموقع الإلكتروني: www.iso.org

تم نشر النسخة العربية في ٢٠١٧

تم النشر في سويسرا

المحتويات

v	تمهيد.....
iv	مقدمة
١	١- المجال
١	٢- المراجع التكميلية
١	٣- المصطلحات والتعاريف
١	٤- المبادئ
٢	٥- المتطلبات العامة
٢	٥/١ الشؤون القانونية والتعاقدية
٢	٥/٢ إدارة الحيادية
٢	٥/٣ ١/٢/٥ تعارض الاهتمامات (المصالح)
٢	٥/٤ الالتزامات والتمويل
٢	٦- المتطلبات الهيكيلية
٣	٧- متطلبات الموارد
٣	٧/١ كفاءات الأفراد
٣	٧/٢ اعتبارات عامة
٣	٧/٣ تحديد معايير الاقتدار
٦	٧/٤ الأفراد المشاركون في نشاطات التصديق
٦	٧/٥ بيان معارف وخبرات المدقق
٧	٧/٦ استخدام المدققين الأفراد من الخارج والخبراء الفنيين من الخارج
٧	٧/٧ استخدام المدققين من الخارج والخبراء الفنيين من الخارج كجزء من فريق التدقيق
٧	٨- سجلات العاملين
٧	٨/١ الاستعانة بالعاملين من خارج المنظمة
٧	٨/٢- ممتلكات المعلومات
٧	٨/٣ المعلومات العامة
٧	٨/٤ مستندات التصديق
٧	٨/٥ ١/٢/٨ وثائق شهادات نظام إدارة أمن المعلومات
٨	٨/٦ الإشارة إلى الشهادة واستخدام العلامات
٨	٨/٧ السرية
٨	٨/٨ ١/٤/٨ الوصول إلى السجلات التنظيمية
٨	٨/٩ ٥/٨ تبادل المعلومات بين جهة إصدار الشهادات وعملائها
٨	٩- متطلبات العمليات
٨	٩/١ متطلبات ما قبل المنح / التصديق
٨	٩/٢ ١/١/٩ تقييم التطبيق
٨	٩/٣ ٢/١/٩ مراجعة التطبيق
٨	٩/٤ ٣/١/٩ برنامج المراجعة
١٠	٩/٥ ٤/١/٩ تحديد زمن التدقيق
١١	٩/٦ ٥/١/٩ العينات في ظل تعدد المواقع
١١	٩/٧ ٦/١/٩ تعدد نظم الإدارة
١١	٩/٨ ٢/٢/٩ تخطيط التدقيق
١١	٩/٩ ١/٢/٩ تحديد أهداف التدقيق ومجاله ومعاييره
١١	٩/١٠ ٢/٢/٩ اختيار فريق التدقيق وتحديد تكاليفات أعضائه
١٢	٩/١١ ٣/٢/٩ خطة التدقيق
١٢	٩/١٢ ٣/٣/٢/٩ التصديق الأولى
١٢	٩/١٣ ١/٣/٩ تدقيق منح الشهادات الأولى
١٣	٩/١٤ ٤/٩ إجراء التدقيق
١٣	٩/١٥ ١/٤/٩ عام

١٣	٢/٤/٩ العناصر الخاصة لتدقيق نظم إدارة أمن المعلومات
١٣	٣/٤/٩ تقرير التدقيق
١٣	٥/٩ قرار التصديق
١٥	١/٥/٩ قرار التصديق
١٥	٦/٩ صيانة التصديق
١٥	١/٦/٩ عام
١٦	٢/٦/٩ تدقيق المراقبة
١٦	٣/٦/٩ اصدار الشهادة
١٦	٤/٦/٩ التدقيقات الخاصة
١٦	٥/٦/٩ تعليق أو سحب أو تقليص مجال الشهادة
١٦	٩/٩ الاستفسار
١٧	٨/٩ الشكاوى
١٧	١/٨/٩ الشكاوى
١٧	٩/٩ سجلات العملاء
١٧	١٠ - متطلبات نظام الإدارة لجهات منح الشهادة
١٧	١/١٠ الخيارات
١٧	١٠/١٠ أتم/١٠ انتطبيق نظم إدارة أمن المعلومات
١٧	١٠/٢/١ الخيارأ: متطلبات نظام الإدارة العامة
١٧	١٠/٣/١ الخيارب: متطلبات نظام الإدارة العامة طبقاً للمواصفة الـIزو ٩٠٠١
١٨	ملحق (أ- استرشادي) المعرف والممارسات المطلوبة لتدقيق نظم إدارة أمن المعلومات والتصديق عليها
٢٠	ملحق (ب- مرجعي) زمن التدقيق
٢٥	ملحق (ج- استرشادي) طرق احتساب زمن التدقيق
٢٩	ملحق (د- استرشادي) إرشادات بمراجعة الموافقة أيزو / أي سي ٢٠١٣/٢٧٠٠١، ٢٠١٢/٢٧٠٠١
٣٧	والملحق (هـ) الضوابط
	المصادر

ISO/IEC 27006:2015

<https://standards.iteh.ai/catalog/standards/sist/a2a247e8-6734-4b30-977c-1f681baca265/iso-iec-27006-2015>

تمهيد

الأيزو (المنظمة الدولية للتقييس) هي اتحاد عالمي لجهات التقييس الوطنية (الجهات الأعضاء في الأيزو)، وغالباً ما يتم إعداد المعايير الدولية من خلال اللجان الفنية للأيزو، وإذا كانت الجهة العضو لها اهتمام بموضوع قد شُكلَّت له لجنة فنية، فإن لهذا العضو الحق في أن يكون له ممثل في تلك اللجنة. ويشارك في العمل كذلك المنظمات الدولية الحكومية منها وغير الحكومية، التي لها تواصل مع الأيزو. وتتعاون الأيزو تعاوناً وثيقاً مع اللجنة الدولية الكهروتقنية (IEC) في جميع الأمور التي تهم التقييس في المجال الكهروتقني.

وتصاغ المعايير الدولية وفقاً للوائح الواردة في توجيهات الأيزو/أي إيه سي - الجزء الثاني. المهمة الرئيسية للجان الفنية هو إعداد المعايير الدولية. ويتم توزيع مشاريع المعايير الدولية على الهيئات الوطنية للتصويت. ويتطلب إصدار هذه المشاريع كمعايير 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 أيٍ من هذه الحقوق أو جماعها.

وقد تم إعداد معايير الأيزو / اللجنة الدولية الكهروتقنية ٢٧٠٠٦ بواسطة اللجنة الفنية، الخاصة بالمشتركة ، تقنيات الأمان SC 27 ، تكنولوجيا المعلومات ، اللجنة الفرعية 1 ISO / IEC JTC 1 ISO / IEC 27006: 2011 حيث تم تنقيحها من الناحية الفنية، تلغى هذه الطبعة الثالثة، الطبعة الثانية (ISO / IEC 27006: 2006).

iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO/IEC 27006:2015](#)

<https://standards.iteh.ai/catalog/standards/sist/a2a247e8-6734-4b30-977c-1f681baca265/iso-iec-27006-2015>

مقدمة

تضع الموصفة ايزو/ اي إس٢١٧٠٢١ المعايير للجهات القائمة على تدقيق ومنح الشهادات لنظم الإدارية للمنظمات. فإن كان لهذه المنظمات أن تعتمد كممثلة للموصفة ايزو/ اي إس٢١٧٠٢١ بهدف تدقيق ومنح الشهادة لنظم إدارة أمن المعلومات (ISMS) طبقاً للموصفة ايزو/ اي إس٢٠٠٥:٢٢٠٠١، فإن هناك متطلبات وإرشادات إضافية ضرورية للموصفة ايزو/ اي إس٢١٧٠٢١. وهو ما تقدمه هذه الموصفة الدولية.

يتبّع النص في هذه الموافقة الدوليّة نفس هيكل الموافقة ايزو / اي إس ٢١٧٠٢١، وقد تم تمييز المتطلبات والإرشادات الإضافية الخاصة بنظم إدارة أمن المعلومات (ISMS) عند تطبيق الموافقة ايزو / اي إس ٢١٧٠٢١، في منح الشهادات لنظم إدارة أمن المعلومات (ISMS) بالأحرف "IS" ، "A" ، "M" .

يستخدم التعبير " يجب " في هذه الموصفة الدولية لبيان تلك الأحكام التي تعكس الإزامية مطلبات الموصفاتين ايزو / اي إى سى ١٧٠٢١ و ايزو / اي إى سى ٢٧٠٠١ . فيما يستخدم التعبير " ينبغي " ليحمل معنى التوصية والنصحة والتفضيل .

والمطلب الأولي لهذه المعاصفة الدولية هو تمكين جهات الاعتماد من تناغم أكثر فعالية في تطبيقها للمعايير التي تتلزم بها عند تقييم جهات التصديق (منش الشهادات).

خلال هذه الموصافة الدولية يستخدم المصطلحان "نظام الإدارة" و"النظام" بالتبادل. تعريف نظام الإدارة وارد في الموصافة الدولية أيزو ٩٠٠٥:٢٠٠٥. ولا ينبغي أن يختلط على الملتقي، "نظام الإدارة" كما هو مستخدم في هذه الموصافة الدولية مع أنواع الأنظمة الأخرى مثل نظام تقنية المعلومات.

تكنولوجي المعلومات - تقنيات الأمان - متطلبات جهات التدقيق والتصديق (إصدار الشهادات) لنظم إدارة أمن المعلومات

١- المجال

تحدد هذه الموصفة الدولية المتطلبات وتقدم الإرشادات لجهات تقديم التدقيق وإصدار الشهادات لنظم إدارة أمن المعلومات بالإضافة إلى المتطلبات الواردة في الموصفة أيزو/اي إيه سي ١٧٠٢١ والموصفة أيزو/اي إيه سي ٢٧٠٠٦. والمقصود هنا في المقام الأول هو دعم اعتماد جهات التصديق (منح الشهادات) التي تصدر الشهادات لنظم إدارة أمن المعلومات ISMS.

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

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

٢- المراجع التكميلية

المستندات التالية، بكاملاها أو أجزاء منها، استخدمت كمراجع معيارية لهذه الموصفة، ولا عرض عنها عند التطبيق . وعند الإشارة لمراجع قيمة (ملغاة)، يعتد فقط بالإصدار الوارد ذكره هنا وفيما عدا ذلك يعتد بالإصدار الأخير من المراجع المشار إليها (معأخذ أي 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*

Information security management systems — Requirements

٣- المصطلحات والتعاريف

لأغراض هذه الموصفة تسرى المصطلحات والتعاريف الواردة في الموصفة الدولية أيزو/اي إيه سي ١٧٠٢١ والواردة في الموصفة الدولية أيزو/اي إيه سي ٢٧٠٠٦ إلى جانب المصطلحات التالية:

٤/١ مستندات التصديق

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

٤- المبادئ

تطبق المبادئ الواردة في الموصفة أيزو/اي إيه سي ١٧٠٢١ ، في البند ٤

٥ - المتطلبات العامة

١/ الشروط القانونية والتعاقدية

تنطبق المتطلبات الواردة في المعاشرة أيزو/أي إيه سي ١-١٧٠٢١، في البند ١/٥.

٢/ إدارة الحيادية

تنطبق المتطلبات الواردة في المعاشرة أيزو/أي إيه سي ١-١٧٠٢١، في البند ٢/٥، بالإضافة إلى المتطلبات والتوجيهات التالية الخاصة بنظام إدارة أمن المعلومات.

١/٢/٥ أ م ٢/ تعارض الاهتمامات (المصلح)

يمكن لجهات منح الشهادات إجراء المهام التالية دون أن تعد من قبيل الاستشارات أو التعارض 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 أو التدقيق، تقتصر جهات المنح على تقديم المعلومات الأساسية والمشورة المتاحة 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 إصدار الشهادات لمتطلبات معايير تدقيق منح / إصدار الشهادات (انظر ١/٣/٩)؛
- (ج) أنشطة ما قبل المراجعة، الهدف منها تحديد الاستعداد (الجاهزية) لتتحقق التصديق (إصدار / منح الشهادات)، ومع ذلك، فلا يجوز أن تؤدي مثل هذه الأنشطة إلى تقديم توصيات أو نصائح من شأنها أن تخالف هذا البند ويجب على جهة إصدار الشهادات أن تكون قادرة على تأكيد أن مثل هذه الأنشطة لا تتعارض مع هذه المتطلبات وأنها لن يتماس تخدامه التبرير الانتهاء إلى انتقاد مدة التدقيق الكلية لمنح الشهادات؛
- (د) إجراء تدقيق الطرف الثاني والطرف الثالث وفقاً لمعايير أو ترتيبات أخرى غير تلك التي تعد جزءاً 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 أثناء عملية المراجعة، دون التوصية بحلول بعينها.

يجب أن تكون جهة إصدار الشهادات مستقلة عن الجهة أو الجهات (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 لنظام إدارة أمن المعلومات.

٣/ الالتزامات والتمويل

تنطبق المتطلبات الواردة في المعاشرة أيزو/أي إيه سي ١-١٧٠٢١، في البند ٣/٥.

٦ - المتطلبات الهيكلاية

تنطبق المتطلبات الواردة في المعاشرة أيزو/أي إيه سي ١-١٧٠٢١، في البند ٦.

٧ - متطلبات الموارد

١/٧ كفاءات الأفراد

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

١/١/٧ اعتبارات عامة

١/١/١/٧ متطلبات الكفاءة العامة/ 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 ١-١ من المعاشرة ايزو/ اي اي سي ١٧٠٢١-١. تأخذ جهة التصديق في اعتبارها المتطلبات الموصفة في ايزو/ اي اي سي ١٧٠٢١-١ والفراء ٢/١/٧ و ١/٢/٧ من هذه المعاشرة الدولية ذات العلاقة بجوانب نظام أمن المعلومات التقنية على النحو المحدد من قبل جهة التصديق.

ملحوظة: يقدم المرفق أ ملخصاً لمتطلبات الكفاءة للأفراد المشاركون في وظائف التصديق المحددة

iTeh STANDARD PREVIEW

٢/١/٧ تحديد معايير الكفاءة

١/٢/١/٧ متطلبات الكفاءة لتدقيق نظام إدارة أمن المعلومات

١/١/٢/١/٧ المتطلبات العامة

<https://standards.iteh.ai/catalog/standards/sist/a2a247e8-6734-4b30-977c-3766f5568115>

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

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

ملحوظة: تقدم المعاشرة ISO 19011 مزيداً من المعلومات عن مبادئ التدقيق

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

تنطبق هذه المتطلبات من (أ) إلى (ه) على كافة المدققين الذين يشكلون جزءاً من فريق التدقيق باستثناء (ب)، حيث يتشاركها أعضاء الفريق.

يجب أن يكون فريق التدقيق على اقتدار يمكنه من تتبع علامات / ظواهر واقعات التأمين في نظام إدارة أمن المعلومات للمنشأة العميل، عكسياً حتى العناصر المناسبة في 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 كل ما يكفي من التقدير والخبرة لتغطية مجال التدقيق لنظام إدارة أمن المعلومات (ISMS).

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

عموماً، يجب على أن تكون لدى جميع أفراد فريق التدقيق المعرفات التالية:

- (أ) هيكل التوثيق الخاصة بنظم إدارة أمن المعلومات وترجها و علاقتها البنية؛
ب) الأدوات والطرق والتقييمات ذات الصلة بنظم إدارة أمن المعلومات وتطبيقاتها؛
ج) تدبير 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 موافقات نظم إدارة أمن المعلومات ومستنداتها المعيارية

يجب أن يكون المدققون المشاركون في تدقيق نظم إدارة أمن المعلومات بما يلي:

- أ) كافة المتطلبات الواردة في المعاشرة ايزو / اي سي ٢٧٠٠١ عموما، يجب أن يكون لدى كل أعضاء فريق التدقيق المعرف التالي:
ب) كافة الضوابط الواردة في المعاشرة 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 الصالحيات
(٦) التشغيل
(٧) الأمان المادي والبيئي
(٨) أمن العمليات بما فيها خدمات تقنيات المعلومات
(٩) أمن الاتصالات، بما فيها إدارة أمن الشبكات وتحويل / نقل المعلومات
(١٠) اقتداء 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 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 البنية 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 قطاع أعمال العميل

يجب أن تكون لدى المدققين المشاركين في تدقيق نظام إدارة أمن المعلومات المعرف التالي:

- أ) المتطلبات القانونية والتنظيمية في مجال عينه لأمن المعلومات أو نطاق جغرافي عينه أو تحت مظلة نظام قضائي عينه.

- ملحوظة: لا تقتضي معرفة المتطلبات القانونية والتنظيمية خلية قانونية مسبقة.
- ب) مخاطر أمن المعلومات المرتبطة بهذا القطاع من الأعمال.
 - ج) المصطلحات والعمليات والتقييمات ذات العلاقة بقطاع أعمال العميل.
 - د) الممارسات ذات العلاقة بقطاع الأعمال.
- قد يكون المعيار (أ) مشتركاً بين فريق العمل.

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

- عموماً، يجب أن تكون لدى المدققين المشاركون في تدقيق نظام إدارة أمن المعلومات المعرف التالي:
- أ) أثر نوع المنشأة وحجمها وحوكمنتها وهيكليتها 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، يجب أن تبدي فريق التدقيق التي تجري تحت إشرافهم وبارشاداتهم.
- أ) معارف ومهارات إدارة عمليات التدقيق للتصديق، وفريق التدقيق.
 - ب) بيان القدرة على التواصل بفعالية، شفافية وكتابة.

iTeh STANDARDS REVIEW WORKS

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

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

https://standards.iteh.ai/catalog/standards/sist/a2a247e8-6734-4b30-977c-
يجب أن يكون لدى الأفراد القائمين بمراجعة الطلبات لتحديد كفاءات فريق التدقيق، لاختيار أعضاء الفريق
وتحديد زمن التدقيق، المعرف التالي:

- أ) مواصفات نظم إدارة أمن المعلومات ومستنداتها المعيارية ذات العلاقة المستخدمة 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، المعرف التالي:

- أ) المصطلحات والعمليات والتقييمات 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، المعرف التالي:

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

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

٤/٢/١/١ عام

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

- (أ) نظم الإدارة عموماً
- (ب) عمليات وإجراءات التدقيق
- (ج) مبادئ وممارسات وتقنيات التدقيق

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

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

- (أ) البنود الواردة في ٢/١/٢/١ (أ) وج (د)
- (ب) المتطلبات القانونية والتنظيمية ذات العلاقة بأمن المعلومات.

٣/٤/٢/١/٣ 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، المعرف التالية:

- (أ) مواصفات نظم إدارة أمن المعلومات ومستنداتها المعيارية ذات العلاقة المستخدمة في عملية التصديق.

[ISO/IEC 27006:2015](#)

٤/٤/٢/١/٤ قطاع أعمال العميل

<https://standards.iteh.ai/catalog/standards/sist/a2a247e3f1f681baca265/iso-iec-27006-2015>

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

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

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

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

- (أ) منتجات العميل وعملياته ونوع المنشأة وحجمها وحوكمتها وهيكليتها ووظائفها وعلاقتها

٧/٢ العاملون المشاركون في أنشطة من الشهادات

تنطبق المتطلبات الواردة في المعايير ISO/IEC 27006-1-17021 في البند ٢/٧. وبالإضافة إلى ذلك، تتطبق المتطلبات والتوجيهات التالية

٧/٢/١ م/١ ببيان معارف وخبرات أفراد جهات التدقيق

يجب أن تبين جهات من الشهادات معارف وخبرات أفراد جهات التدقيق من خلال:

- (أ) مؤهلات معترف بها فيما يختص بنظم إدارة أمن المعلومات ISMS
- (ب) التسجيل كمدقق - حال كون ذلك منطبقاً
- (ج) الاشتراك في البرامج التدريبيةفيننظم إدارة أمن المعلومات ISMS وتقدم المستندات الدالة على ذلك عند الطلب

- د) الحفاظ على سجلات محدثة للتنمية المهنية
٥) شهود عمليات تدقيق نظم إدارة أمن المعلومات من قبل مدقق آخر في نفس المجال

٧/١/١ اختيار المدققين

- بالإضافة إلى ١/٢/١ يجب أن يؤكد 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 دور أو وظيفة تتعلق بأمن المعلومات؛
 - ج) إكمال خمسة أيام من التدريب بنجاح، يعطى مجالها تدقيق نظام إدارة أمن المعلومات ISMS وإدارة التدقيق مما يعد مناسباً؛
 - 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 تدقيق شهادة على الأقل، فيما لا يقل مجموعه عن عشرين يوماً، تتضمن مراجعة الوثائق وتحليل المخاطر، وتقييم التنفيذ وتقارير التدقيق؛
 - هـ) خبرة حالية ذات علاقة مناسبة.
 - و) الحفاظ على حداثة معارفهم ومهاراتهم في مجال أمن المعلومات والتدقيق، من خلال التطوير المهني المستمر.
- يجب أن يمثل الخبراء الفنيون للمعايير أ، وب)، وهـ)

٧/٢ اختبار المدققين لقيادة الفريق

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

- (standards.iteh.ai) أ) قد شارك في 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 التقرير الرسمي للتدقيق <https://standards.iteh.ai/catalog/standards/iso-iec-27006-2015> 1f681baca265/iso-iec-27006-2015

٣/٧ استخدام المدققين الخارجيين الأفراد والخبراء الفنيين الخارجيين

تطبق المتطلبات الواردة في أيزو / اي إس ١٧٠٢١ - ١٧٠٢١ ٣/٧ وبالإضافة إلى ذلك، تطبق المتطلبات والتوجيهات التالية الخاصة بنظام إدارة أمن المعلومات ISMS.

- ٧/٣/٣ استخدام المدققين الخارجيين أو الخبراء الفنيين الخارجيين كجزء من فريق التدقيق
يجب أن يعمل الخبراء الفنيون تحت إشراف مدقق. الحد الأدنى من المتطلبات الواجب توافرها في الخبراء الفنيين واردة في الفقرة ١-٢-٧.

٤/٧ سجلات الموظفين

تطبق المتطلبات الواردة في المواصفة ايزو / اي إس ١٧٠٢١ ١-١٧٠٢١ في البند ٤/٧.

٥/٧ الاستعانة بمصادر خارجية

تطبق المتطلبات الواردة في المواصفة ايزو / اي إس ١٧٠٢١ ١-١٧٠٢١ في البند ٥/٧.

٨ - متطلبات المعلومات

١/٨ المعلومات العامة

تطبق المتطلبات الواردة في ايزو / اي إس ١٧٠٢١ ١-١٧٠٢١، البند ١/٨.