

المواصفة القياسية الدولية

أيزو/ 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 des systèmes de management de la sécurité de l'information (F)*

<https://standards.iteh.ai/>

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

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

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

©ISO 2015



### إخلاء مسؤولية (تنويه)

قد يحتوي هذا الملف (PDF) على خطوط مُدمجة، وبموجب سياسة الترخيص لـ Adobe فإنه يمكن طباعة هذا الملف أو الاطلاع عليه، على ألا يتم تعديله ما لم تكن الخطوط المُدمجة فيهمرخصة ومُحملة في الحاسوب الذي يتم فيه التعديل. وتحمل الأطراف - عند تنزيل هذا الملف - مسؤولية عدم الإخلال بسياسة الترخيص لـ Adobe، في حين أن السكرتارية العامة للأيزو ولا تتحمل أي مسؤولية قانونية حيال هذا المجال.

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

يمكن الحصول على جميع التفاصيل الخاصة بالبرامج المستخدمة في إنشاء هذا الملف من المعلومات العامة المتعلقة بملف (PDF)، ولأجل الطباعة فقد حُسنت المتغيرات الداخلة 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

- مؤسسة المواصفات والمقاييس الأردنية
- هيئة الإمارات للمواصفات والمقاييس
- المعهد الجزائري للتقييس
- الهيئة السعودية للمواصفات والمقاييس
- الجهاز المركزي للتقييس والسيطرة النوعية
- الهيئة العامة للصناعة
- الهيئة السودانية للمواصفات والمقاييس
- الهيئة اليمنية للمواصفات والمقاييس وضبط الجودة
- المعهد الوطني للمواصفات والملكية الصناعية
- هيئة المواصفات والمقاييس العربية السورية
- المركز الوطني للمواصفات والمعايير القياسية
- الهيئة المصرية العامة للمواصفات والجودة



وثيقة حماية حقوق الطبع والنشر

أيزو ٢٠١٥ ©

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

مكتب حقوق ملكية المنظمة الدولية للتقييس

الرمز البريدي: ٥٦-1211-Ch- جنيف ٢٠

هاتف: ٠٠٤١٢٢٧٤٩٠١١١

فاكس: ٠٠٤١٢٢٧٤٩٠٩٤٧

بريد إلكتروني: copyright@iso.org

الموقع الإلكتروني: www.iso.org

تم نشر النسخة العربية في ٢٠١٧

تم النشر في سويسرا

## المحتويات

v	تمهيد
iv	مقدمة ..
1	1- المجال
1	2- المراجع التكميلية
1	3- المصطلحات والتعاريف
1	4- المبادئ
2	5- المتطلبات العامة
2	1/5 الشؤون القانونية والتعاقدية
2	2/5 إدارة الحيادية
2	1/2/5 أم 2/5 تعارض الاهتمامات (المصالح)
2	3/5 الالتزامات والتمويل
2	6- المتطلبات الهيكلية
3	7- متطلبات الموارد
3	1/7 كفاءات الأفراد
3	1/1/7 اعتبارات عامة
3	2/1/7 تحديد معايير الاقتدار
6	2/7 الأفراد المشاركون في نشاطات التصديق
6	1/2/7 بيان معارف وخبرات المدقق
7	3/7 استخدام المدققين الأفراد من الخارج والخبراء الفنيين من الخارج
7	1/3/7 استخدام المدققين من الخارج والخبراء الفنيين من الخارج كجزء من فريق التدقيق
7	4/7 سجلات العاملين
7	5/7 الاستعانة بالعاملين من خارج المنظمة
7	8- متطلبات المعلومات
7	1/8 المعلومات العامة
7	2/8 مستندات التصديق
7	1/2/8 وثائق شهادات نظام إدارة أمن المعلومات
8	3/8 الإشارة إلى الشهادة واستخدام العلامات
8	4/8 السرية
8	1/4/8 الوصول إلى السجلات التنظيمية
8	5/8 تبادل المعلومات بين جهة إصدار الشهادات وعملائها
8	9- متطلبات العمليات
8	1/9 متطلبات ما قبل المنح / التصديق
8	1/1/9 تقديم التطبيق
8	2/1/9 مراجعة التطبيق
8	3/1/9 برنامج المراجعة
10	4/1/9 تحديد زمن التدقيق
11	5/1/9 العينات في ظل تعدد المواقع
11	6/1/9 تعدد نظم الإدارة
11	2/9 تخطيط التدقيقات
11	1/2/9 تحديد أهداف التدقيق ومجاله ومعايير
11	2/2/9 اختيار فريق التدقيق وتحديد تكاليفات أعضائه
12	3/2/9 خطة التدقيق
12	3/9 التصديق الأولى
12	1/3/9 تدقيق منح الشهادات الأولى
13	4/9 إجراء التدقيقات
13	1/4/9 عام

١٣	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	١٧/٩ 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	١/١٠ أم ١/١٠ تطبيق نظام إدارة أمن المعلومات
١٧	٢/١٠ الخيار أ: متطلبات نظام الإدارة العامة
١٧	٣/١٠ الخيار ب: متطلبات نظام الإدارة العامة طبقا للمواصفة الايزو ٩٠٠١
١٨	ملحق (أ- استرشادي) المعارف والمعارات المطلوبة لتدقيق نظم إدارة أمن المعلومات والتصديق عليها
٢٠	ملحق (ب - مرجعي) زمن التدقيق
٢٥	ملحق (ج - استرشادي) طرق احتساب زمن التدقيق
	ملحق (د - استرشادي) إرشادات بمراجعة المواصفة ايزو / أي سي ٢٧٠٠٦/٢٠١٥
٢٩	والملحق (هـ) الضوابط
٣٧	المصادر

## Document Preview

ISO/IEC 27006:2015

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

## تمهيد

الأيزو (المنظمة الدولية للتقييس) هي اتحاد عالمي لجهات التقييس الوطنية (الجهات الأعضاء في الأيزو)، وغالبا ما يتم إعداد المواصفات الدولية من خلال اللجان الفنية للأيزو، وإذا كانت الجهة العضو لها اهتمام بموضوع قد شكّلت 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 وتعاوننا 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 أي من هذه الحقوق أو جميعها.

وقد تم إعداد مواصفة الأيزو/ اللجنة الدولية الكهرو تقنية ٢٧٠٠٦ بواسطة اللجنة الفنية، الخاصة ب المشتركة ، تقنيات الأمن SC 27 ، تكنولوجيا المعلومات، اللجنة الفرعية ISO / IEC JTC 1 تلغى هذه الطبعة الثالثة، الطبعة الثانية (ISO / IEC 27006: 2011) حيث تم تنقيحها من الناحية الفنية،

# iTeh Standards (<https://standards.iteh.ai>) Document Preview

[ISO/IEC 27006:2015](https://standards.iteh.ai/catalog/standards/iso/a2a247e8-6734-4b30-977c-1f681baca265/iso-iec-27006-2015)

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

## مقدمة

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

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

يستخدم التعبير " يجب " في هذه المواصفة الدولية لبيان تلك الأحكام التي تعكس إلزامية متطلبات الموصفتين ايزو/ أي إي سي ١٧٠٢١ و ايزو/ أي إي سي 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.

(<https://standards.iteh.ai/>)  
Document Preview

[ISO/IEC 27006:2015](https://standards.iteh.ai/catalog/standards/iso/a2a247e8-6734-4b30-977c-1f681baca265/iso-iec-27006-2015)

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

# 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/ أي إي سي ١٧٠٢١ والمواصفة ايزو/ أي إي سي ٢٧٠٠١. والمقصود هنا في المقام الأول هودعم اعتماد جهات التصديق (منح الشهادات) التي تصدر الشهادات لنظم إدارة أمن المعلومات ISMS.

المتطلبات الواردة في هذه المواصفة الدولية بحاجة إلى إظهارها بدلالة الاقتدار والاعتمادية، 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 عنها عند 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/ أي إي سي ١٧٠٢١ والواردة في المواصفة الدولية ايزو/ أي إي سي 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 طبقاً للنظام.

## ٤- المبادئ

تنطبق المبادئ الواردة في المواصفة ايزو/ أي إي سي ١٧٠٢١-١، في البند ٤

## ٥ - المتطلبات العامة

### ١/٥ الشئون القانونية والتعاقدية

تنطبق المتطلبات الواردة في المواصفة ايزو/ أي إي سي ١٧٠٢١-١، في البند ١/٥

### ٢/٥ إدارة الحيادية

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

### ١/٢/٥ أم ٢/٥ تعارض الاهتمامات (المصالح)

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 ٦/٣/١/٩)؛
- (ج) أنشطة ما قبل المراجعة، الهادفة فقط إلى تحديد الاستعداد (الجاهزية) لتدقيق التصديق (إصدار / منح الشهادات)، ومع ذلك، فلا يجوز أن تؤدي مثل هذه الأنشطة إلى تقديم توصيات أو نصائح منشأها 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 الانتهاج إلى انتفاص مدة التدقيق الكلية لمنح الشهادات؛
- (د) إجراء تدقيق الطرف الثاني والطرف الثالث وفقا لمعايير أو تنظيمات أخرى غير تلك التي تعد جزءا من مجال الاعتماد؛
- (هـ) إضافة القيمة خلال عمليات تدقيق التصديق (منح الشهادة) وخلال زيارات المراقبة، على سبيل المثال، <https://sta.iso/27006-2015> 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 لنظم إدارة أمن المعلومات

### ٣/٥ الالتزامات والتمويل

تنطبق المتطلبات الواردة في المواصفة ايزو/ أي إي سي ١٧٠٢١-١، في البند ٣/٥.

## ٦ - المتطلبات الهيكلية

تنطبق المتطلبات الواردة في المواصفة ايزو/ أي إي سي ١٧٠٢١-١، في البند ٦.

**٧ - متطلبات الموارد****١/٧ كفاءات الأفراد**

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

**١/١/٧ أم ١/١/٧ اعتبارات عامة****١/١/٧/١ متطلبات الكفاءة العامة/الأولية**

يجب أن تتحقق جهة التصديق من أن لديها المعرفة بالتطورات التقنية والقانونية والتنظيمية ذات العلاقة بنظام إدارة أمن المعلومات للتعامل 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 إي سي ١٧٠٢١-١. تأخذ جهة التصديق في اعتبارها المتطلبات الموصوفة في ايزو/ اي إي سي ١٧٠٢١-١ والفقرات ٢/١/٧ و ١/٢/٧ من هذه المواصفة الدولية وذات العلاقة بجوانب نظام أمن المعلومات التقنية على النحو المحدد من قبل جهة التصديق.

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

**٢/١/٧ أم ٢/١/٧ تحديد معايير الكفاءة****١/٢/١/٧ متطلبات الكفاءة لتدقيق نظام إدارة أمن المعلومات****١/٢/١/٧ المتطلبات العامة**

يجب أن تكون لجهة التصديق معاييرها للتحقق من خلفية الخبرات والتدريب الخاص أو سيرا مختصرة لأفراد فريق التدقيق التي تؤكد 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 عن مبادئ التدقيق

**(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 في نظام إدارة أمن المعلومات للمنشأة العميل، عكسيا 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 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 وعلاقتها البيئية؛
  - 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 ؛
  - هـ) التقنيات الحالية حيث أمن المعلومات وارد أو جدير بالاعتبار
- يجب على كل مدقق أن يفي بالعناصر أ) و ج) و د)

#### 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 عموماً، يجب أن يكون لدى كل أعضاء فريق التدقيق المعارف التالية:
- ب) كافة الضوابط الواردة في المواصفة ايزو/ اي سي ٢٧٠٠٢ (إذا ما حدد أنها أيضاً 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 متضمناً 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، -6734-4b30-6-27006-2015 (https://standards.iteh.ai/catalog/standards/iso/a2a247e8-6734-4b30-6-27006-2015)
- ١٣) جوانب أمن المعلومات فيما يختص بإدارة استمرارية الأعمال
- ١٤) الامتثال، متضمناً 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 البيئية بين السياسات والأهداف والنتائج
  - د) عمليات الإدارة والمصطلحات ذات العلاقة.
- ملحوظة: تتضمن هذه العمليات أيضاً إدارة 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) آثار نوع المنشأة وحجمها وحوكمتها وهيكلها ووظائفها وعلاقتها 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 على قادة الفرق بالمتطلبات التالية، التي يجب أن تبنى في الدقيقات التي تجرى تحت إشرافهم وبارشاداتهم.
- (أ) معارف ومهارات إدارة عمليات التدقيق للتصديق، وفريق التدقيق.
- (ب) بيان القدرة على التواصل بفعالية، شفافية 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: 06-2015 <https://standards.iteh.ai/catalog/standards/iso/a2a247e8-6734-4b30-9>
- (أ) مواصفات نظم إدارة أمن المعلومات ومستنداتها المعيارية ذات العلاقة والمستخدم 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 وعلاقتها 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 عموماً
- 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) و(ج) و(د)
- 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 والمستخدم 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/ أي إي سي ١٧٠٢١-١ في البند ٢/٧. وبالإضافة إلى ذلك، تنطبق المتطلبات والتوجيهات التالية

## ١/٢/٧ أم ١/٢/٧ بيان معارف وخبرات أفراد جهات التدقيق

يجب أن تبين جهات منح 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 التدريبية فينظم إدارة أمن المعلومات ISMS وتقديم المستندات الدالة على ذلك عند الطلب