المواصفة القياسية الدولية

أيــزو/ أي إي سي ٢٧٠٠٣

الترجمة الرسمية
Official translation
Traduction officielle

تكنولوجيا المعلومات –تقنيات التأمين – دليل ارشادي عن تطبيق نظام تامين تكنولوجيا المعلومات

Information technology — Security techniques — Information security management system implementation guidance (E)

Technologies de l'information — Techniques de sécurité — Lignes directrices pour la mise en œuvre du système de management de la sécurité de l'information (F)

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

الرقم المرجعي
ISO 27003/2010 (A)
الترجمة الرسمية

جهات التقييس العربية التي أعتمدت 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 الوطنى للمواصفات والملكية الصناعية	تونس
■ هيئة المواصفات والمقاييس العربية السورية	سوريا
■ المركز الوطنى 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 نشرالنسخة العربية في ٢٠١٦
تم النشر في سويسرا

المحتويات **الصفحة**

تمهيد

تشكل المنظمة الدولية للتقييس (ISO) واللجنة الدولية الكهروتقنية (IEC) نظام متخصص للتوحيد القياسي في جميع أنحاء العالم.وتشارك الهيئات الوطنية الأعضاء في المنظمتين ISOأو IEC في عملية اعدادالمواصفات الدولية من خلال اللجان الفنية التي تنشأها المنظمة المعنية للتعامل مع مجالات معينة من النشاط الفني .وتتعاون اللجان الفنية التابعة لكل منISO و IEC في المجالات ذات الاهتمام المشترك.كما يشارك في العمل المنظمات الدولية الحكومية منهاوغيرالحكومية، ذات الصلة بمنظمتي .IEC , ISO. في مجال تكنولوجيا المعلومات فقد قامت منظمتي IEC , ISOبإنشاء لجنةفنية مشتركة .ISO\IEC JTC1.

وقد صيغت المواصفات الدولية وفقا للوائح الواردة في التوجيهات الصادرة عن كلا منIEC / ISO، الجزء الثاني.

المهمة الأساسية للجنة الفنية المشتركة هي اعداد المواصفات الدولية. مشاريع المواصفات الدولية المتبناه بواسطة اللجنة الفنية المشتركة يتم توزيعها علىالهيئات الوطنية للتصويت. و يتطلب اصدار هذه المشاريع كمواصفات دولية موافقة ٧٥% على الأقل من الهيئات الوطنية التي يحق لها التصويت.

و نود لفت الانتباه إلى احتمالية أن تكونبعض عناصر هذه الوثيقة خاضعة لحقوق براءة الاختراع.و لن تتحمل المنظمة الدولية للتقييس (ISO)مسؤولية تحديد أيّامن هذه الحقوق أو جميعها .

المواصفة الدولية أيزو/أي إي سي ٢٧٠٠٣ تم اعدادها بواسطة اللجنة الفنية المشتركة ISO\IEC JTC1، تكنولوجيا المعلومات ، اللجنة الفرعية SC27، تقنيات تأمين تكنولوجيا المعلومات.

مقدمة

الغرض من هذه المواصفة الدولية هو توفير دليل ارشادي عملي لتطوير وتنفيذ خطة لنظام ادارة تأمين المعلومات (ISMS) داخل المنشأه بما يتوافق مع المواصفة القياسية الدولية أيزو /أي إي سي ٢٧٠٠١:٢٠٠٥ . التطبيق الحقيقي لنظام التأمين (ISMS) ينفذ عامة كمشروع.

العملية الموصفة داخل هذه المواصفة تم تصميمها لتوفر دعما لتطبيق المواصفة الدولية المواصفة القياسية الدولية أيزو /أي إي سي ٢٧٠٠١:٢٠٠٥؛ (الأجزاء ذات العلاقة محصورة في البنود ٤و٥و٧)والمستند:

أ) اعداد بدايات خطة تطبيق نظام ادارة تأمين المعلومات ISMS في المنشأة، تعرف الهيكل التنظيمي للمشروع والحصول على الموافقات الادارية.

ب) الأنشطة الحرجة لمشروع نظام ادارة التأمين (ISMS).

ج) أمثلة لتحقيق متطلبات المواصفة القياسية الدولية أيزو /أي إي سي ٢٧٠٠١:٢٠٠٥.

تستطيع المنشأة تطوير عملية لإدارة تأمين المعلومات باستخدام هذه المواصفة القياسية الدولية ، مما يعطى الجهات ذات الصلة الاطمئنان أن مخاطر أصول المعلومات يتم حصرها بصورة مستمرة داخل حدود تأمين معلومات مقبول كما تعرفه المنشأة.

لا تغطى هذه المواصفة القياسية الدولية الأنشطة التشغيلية وأنشطة نظام ادارة التأمين ISMS الأخرى ، بل تغطي المفاهيم التي على أساها يتم تصميم هذه الأنشطة التي ستنتج بعد بدء عمليات النظام ISMS. حيث ينتج المفهوم من الخطة النهائية لتطبيق مشروع نظام ISMS.

تكنولوجيا المعلومات – تقنيات التأمين – دليل ارشادي عن تطبيق نظام تامين تكنولوجيا المعلومات

١. المجال

تركز هذه المواصفة الدولية على الجوانب الحيوية اللازمة لنجاح تصميم وتنفيذ نظام إدارة أمن المعلومات (ISMS) وفقا للمواصفة أيزو /أي إي سي ٢٧٠٠١: ٢٠٠٥. إذ تصف عمليات توصيف نظام إدارة تأمين المعلومات وتصميمه من البداية حتى إخراج خطط التنفيذ. كما تصف عملية الحصول على اعتماد الإدارة لتنفيذ نظام إدارة تأمين المعلومات. وتضع مشروع تنفيذه (الذى يسمى فى هذه المواصفة مشروع نظام إدارة تأمين المعلومات)، وتقدم إرشادات عن كيفية التخطيط للمشروع، بحيث نحصل فى النهاية على خطة نهائية لتنفيذ المشروع.

ويقصد من هذه المواصفة الدولية أن تستخدم من قبل المنشآت التي تطبق نظاما لإدارة تأمين المعلومات. تنطبق هذه المواصفة على المنشآت بجميع أنواعها (مثل المؤسسات التجارية و الهيئات الحكومية، والمنظمات غير الهادفة للربح) وعلى اختلاف أحجامها. كل منظمة متفردة بتعقيداتها وسوف تحدد خصوصية متطلباتها طريقة تطبيق نظامها لإدرة تأمين المعلومات. ومن هنا ستجد المنشآت الأصغر حجما أن الأنشطة المذكورة فى هذه المواصفة تنطبق عليها، بطريقة مبسطة. أما المنشآت الكبيرة الحجم أو الأكثر تعقيدا فقد تجد أنها بحاجة إلى هيكل إداريمتعدد الطبقات أو نظام إدارة منفصل لإدارة أنشطة هذه المواصفة الدولية على نحو فعال. وفي كلتا الحالتين، يمكن التخطيط للأنشطة ذات الصلة باستخدام هذه المواصفة الدولية.

تقدم هذه المواصفة الدولية توصيات وشروحا ، ولا تحدد أية متطلبات.ويقصد بهذه المواصفة أن تستخدم جنبا إلى جنب معأيزو /أي إي سي ٢٧٠٠١: ٢٠٠٥ و أيزو /أي إي سي ٢٧٠٠٢: ٢٠٠٥ ولكن ليس المقصود منها تعديل أو خفض المتطلبات الواردة فى أيزو /أي إي سي ٢٧٠٠١: ٢٠٠٥أو التوصيات الواردة فى أيزو /أي إي سي ٢٧٠٠٢: ٢٠٠٥. ومن غير المناسب الإدعاء بالتطابق مع هذه المواصفة.

٢. المراجع التكميلية

تعتبر الوثائق المرجعية التالية اساسية لتطبيق هذه الوثيقة . بالنسبة للمراجع المؤرخة يلزم تطبيق النسخ المذكورة أما بالنسبة للمراجع غير المؤرخة فإنه يلزم تطبيق آخر إصدار من الوثيقة المرجعية (متضمنا اى تعديلات):

أيزو /أي إي سي ٢٧٠٠٠: ٢٠٠٩ تكنولوجيا المعلومات – تقنيات التأمين – نظام تامين تكنولوجيا المعلومات- نظرة عامة ومفردات.

أيزو /أي إي سي ٢٧٠٠١: ٢٠٠٥تكنولوجيا المعلومات – تقنيات التأمين – نظام تامين تكنولوجيا المعلومات- المتطلبات.

٣. المصطلحات والتعاريف

لأغراض هذه المواصفة تطبق المصطلحات والتعاريف الواردة فى أيزو /أي إي سي ٢٧٠٠٠: ٢٠٠٩ و أيزو /أي إي سي٢٧٠٠١: ٢٠٠٥ بالإضافة للتالي:

١/٣ مشروع نظام ISMS

أنشطة منظمة تقوم بها المنشأة لتنفيذ نظام إدارة تأمين المعلومات ISMS.

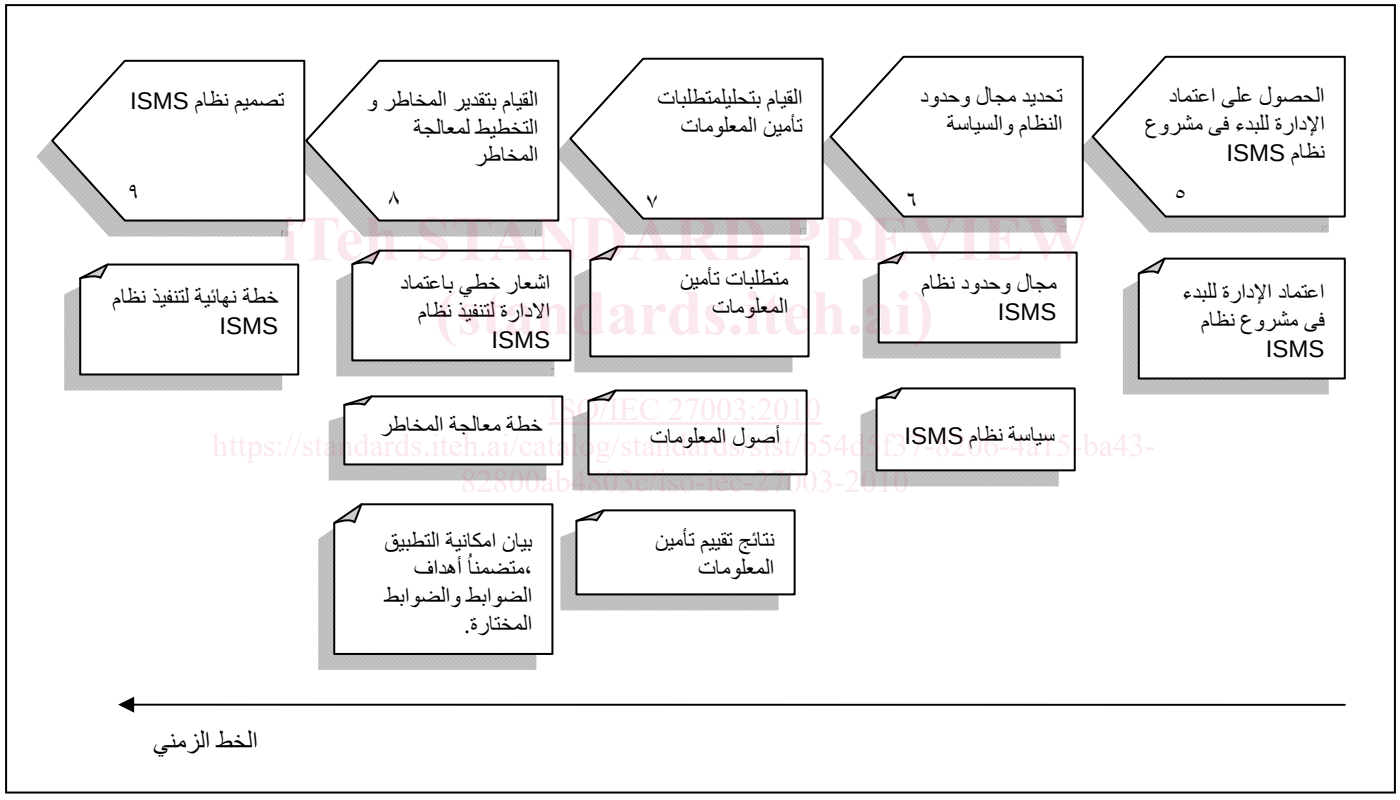
٤. هيكل هذه المواصفة الدولية

١/٤الهيكل العام لبنود هذه المواصفة

يعد تنفيذ نظام إدارة تأمين المعلومات نشاطا مهما ، وينفذ عموما كمشروع من مشروعات المنشأة. يشرح هذا المستند تنفيذ نظام(ISMS) بالتركيز على البدء والتخطيط والتعريف للمشروع. كما تتضمن عملية التخطيط للتنفيذ النهائى للنظام خمسة مراحل ، تمثل كل مرحلة منها بندا منفصلا. ولكل البنود نفس الهيكل، كما هو موصوف فيما يلى . والمراحل الخمسة هى :

أ) الحصول على اعتماد الإدارة للبدء فى مشروع نظام إدارة تأمين المعلومات (البند الخامس)
ب) تحديد مجال النظام والسياسة (البند السادس)
ت) القيام بتحليل المنشأة (البند السابع)
ث) القيامبتقدير المخاطر وخطة معالجة المخاطر (البند الثامن)
ج) تصميم نظام إدارة تأمين المعلومات (البند التاسع)

يبين الشكل ١ المراحل الخمسة للتخطيط لمشروع نظام إدارة تأمين المعلومات مع الإشارة إلى المواصفات القياسية ISO/IEC ووثائق المخرجات الرئيسية.



شكل ١: مراحل مشروع نظام إدارة تأمين المعلومات

المزيد من المعلومات واردة فى الملاحق المرفقة. وهذه الملاحق هي :

ملحق أ : ملخص للأنشطة مع الإشارة إلى مرجعيته في المواصفة القياسيةأيزو /أي إي سي ٢٧٠٠١:٢٠٠٥

ملحق ب : أدوار ومسئوليات تأمين المعلومات

ملحق ج : معلومات حول التخطيط للمراجعات الداخلية

ملحق د : هيكل السياسات

ملحق هـ : معلومات حول التخطيط للمراقبة والقياس

٢/٤ الهيكل العام لبند من بنود المواصفة

يحتوى كل بند على ما يلى :

أ) واحد أو أكثر من الأهداف مع ذكر ما يتحقق منها فى البداية من كل بند فى مربع نص
ب) واحد أو أكثر من الأنشطة الضرورية لتحقيق هدف أو أهداف المرحلة
يوصف كل نشاط على حدة فى بند فرعى

وصف النشاط فى كل بند فرعى مقسم على النحو التالى :

النشاط:

يعرف النشاط ما هو ضرورى لاستيفاء جوانب هذا النشاط بما يكفل تحقيق كل أهداف المرحلةأو جزء منها.

المدخل:

تصف المدخلات نقاط البداية ، مثل وجود قرارات موثقة أو مخرجات من أنشطة أخرى موصوفة فى هذه المواصفة الدولية. يمكن أيضا أن يشار إلى المدخلات إما كمخرجات كاملة من نشاط بمجرد ذكر للبند ذى الصلة أو قد تضاف معلومات بعينها من نشاط ما بعد الإشارة المرجعية للبند.

الإرشادات

توفر الإرشادات معلومات تفصيلية تمكن من أداء النشاط . بعض الإرشادات قد لا تكون مناسبة فى جميع الحالات، فقد تكون هناك أساليب أكثر ملائمة لتحقيق النتائج.

المخرجات

تصف المخرجات النتائج أو المستلمات عند استكمال النشاط ،مثل: الوثائق. تتماثل المخرجات ، ايا ما كان حجم المنشأة أو نطاق نظام إدارة تأمين المعلومات.

معلومات أخرى

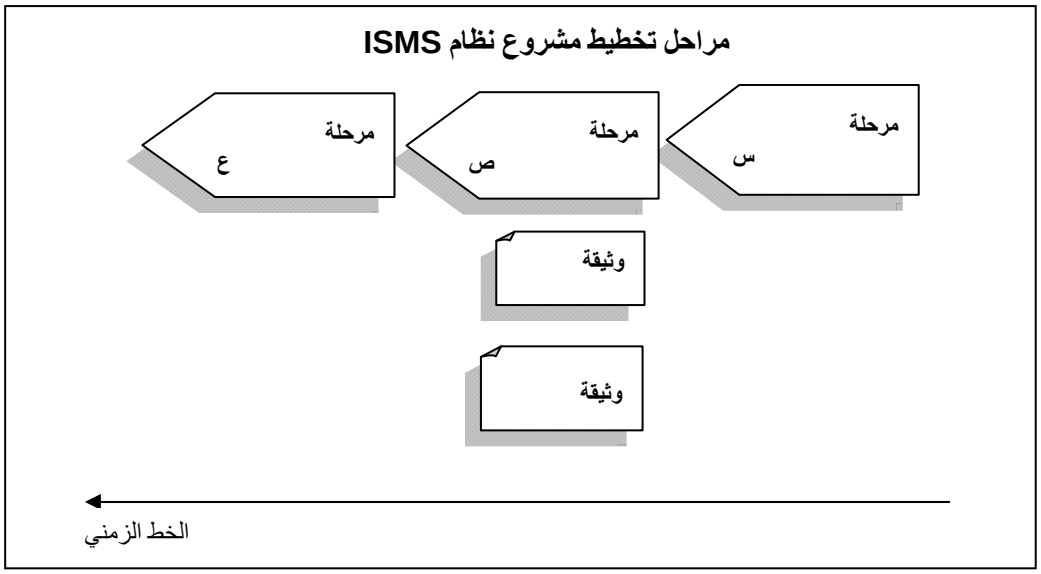
توفر المعلومات الأخرى أى معلومات إضافية يكون من شأنها المساعدة فى أداء النشاط، مثل الإشارات للمرجعية لمواصفات أخرى.

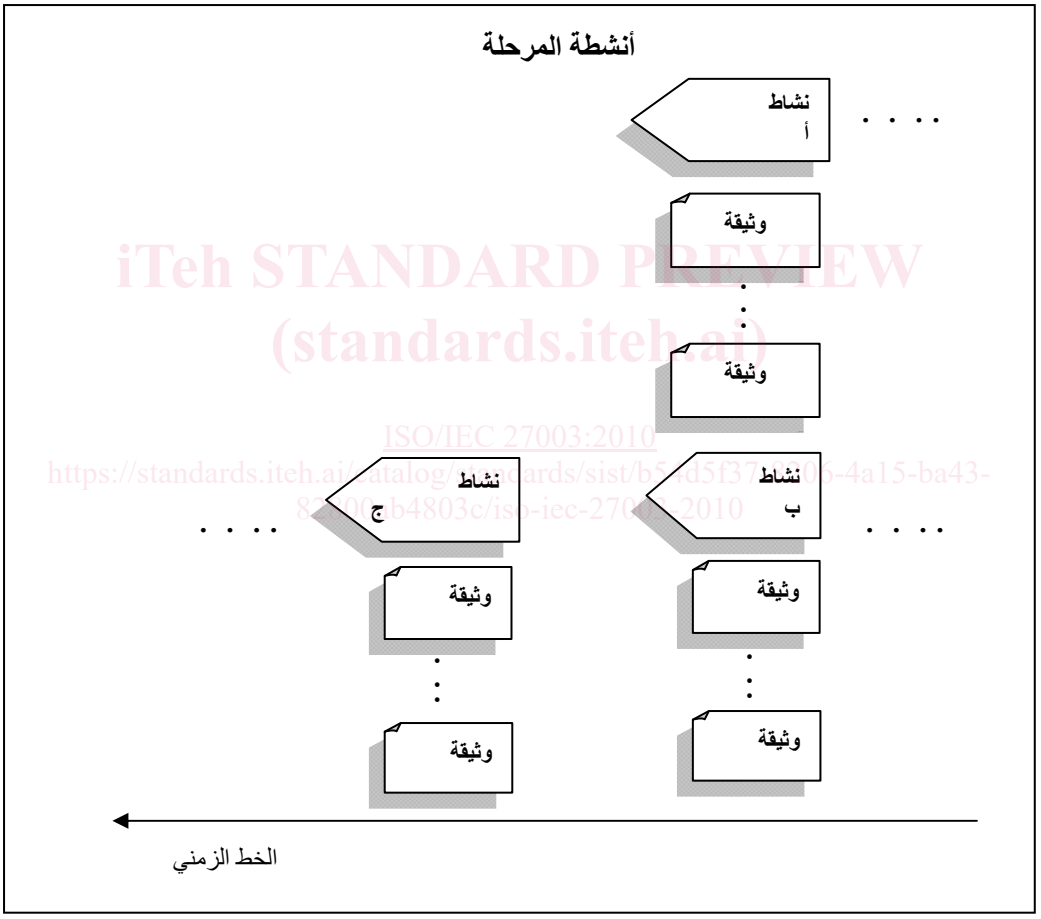
ملحوظة: تتضمن المراحل والأنشطة الموصوفة فى هذا المستند تسلسل مقترح لأداء الأنشطة مبنى على الاعتمادات المحددة عبر مدخلات ومخرجات كلاً من هذه الأنشطة . ومع ذلك فقد تختار المتشأة نشاطاتها بأى ترتيب تقتضيه الضرورة للإعداد والتنفيذ لنظام إدارة تأمين المعلومات وذلك اعتمادا على العديد من العوامل المختلفة (مثل: فعالية نظام الإدارة المطبق حاليا و فهم ما يتعلق بأهمية تأمين المعلومات و أسباب تطبيق نظام إدارة تأمين المعلومات .

٣/٤ الرسومات البيانية (التخطيطية)

يوضح المشروع غالبا فى شكل رسوم تخطيطية أو رسوم بيانية تظهر نظرة عامة للأنشطة والمخرجات.

يبين الشكل ٢ تفسير للرسومات الموضحة فى البند الفرعى نظرة عامة في كل مرحلة . تضع الرسومات منظورا عاما كليا للأنشطة الواردة فى كل مرحلة.





شكل ٢: تفسير لتدفق الرسومات البيانية

يوضح المربع العلوي مراحل التخطيط للمشروع، ثم تؤكد وثائق المخرجات الرئيسية من كل مرحلة الشرح الوارد في البند الخاص بها .

يتضمن الرسم السفلي (أنشطة كل مرحلة) الأنشطة الأساسية المتضمنة فى المرحلة موضع الشرح فى المربع العلوي ووثائق المخرجات الرئيسية لكل نشاط.

الخط الزمنى فى المربع السفلي مؤسس على الخط الزمنى فى المربع العلوي.

يمكن تنفيذ النشاط ين أ و ب فى نفس الوقت. بينما النشاط ج ينبغي أن يبدأ بعد الانتهاء من النشاطين أ و ب.

٥. الحصول على اعتماد الإدارة للبدء فى مشروع نظام إدارة تأمين المعلومات .

٥/١نظرة عامة عن الحصول على اعتماد الإدارة للبدء فى مشروع نظام ISMS

هناك العديد من العوامل أو المؤثرات التى يجب أخذها فى الاعتبار عند اتخاذ القرار بتنفيذ نظام إدارة تأمين المعلومات ، وفى سبيلاستهدافهذه العوامل ، يجب أن نتفهم الإدارة دراسة حالة الأعمال لمشروع تنفيذ نظام إدارة تأمين المعلومات وتوافق عليه ، لذلك فالهدف من هذه المرحلة هو :

الهدف:

الحصول على موافقة الإدارة للبدء فى مشروع نظام إدارة تأمين المعلومات بتعريفدراسة حالة الأعمال وخطة المشروع .

ومن أجل طلب اعتماد الإدارة ، ينبغي للمنشأة أن تنشيء دراسة حالة الأعمال التى تتضمن الأولويات والأهداف لتنفيذ نظام إدارة تأمين المعلومات ، بالإضافة الى الهيكل لتنظيمي للمنشأه من أجل نظام ISMS. كما ينبغي أيضا انشاء الخطة المبدئية لنظام إدارة تأمين المعلومات .

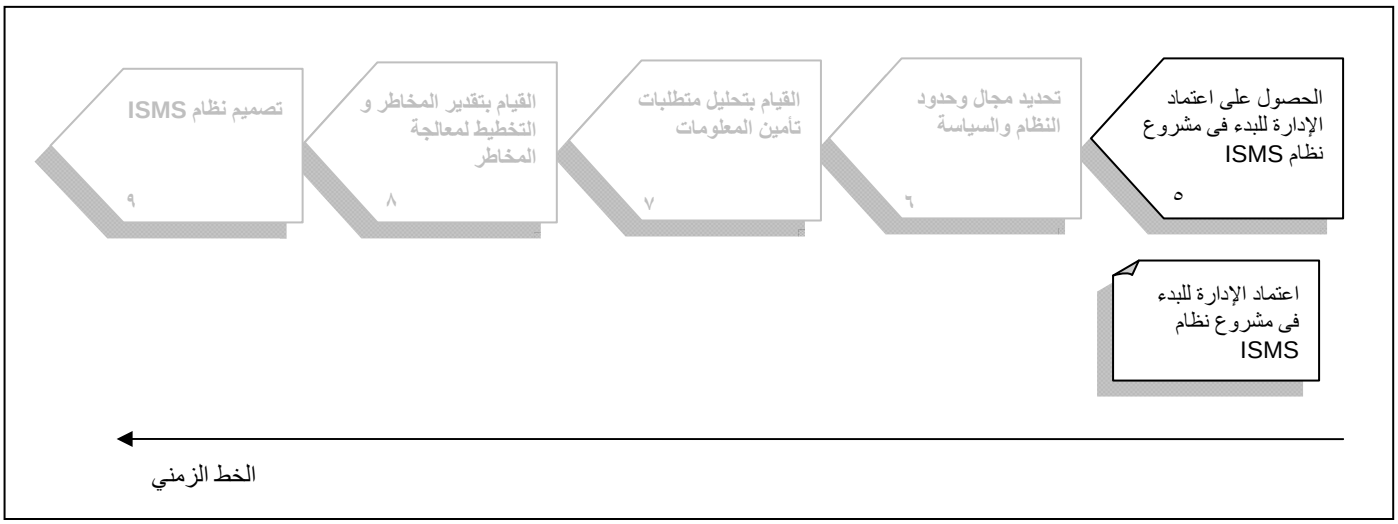
العمل المُؤدَّى فى هذه المرحلة سوف يُمَكِّن المنظمة من فهم مدى أهمية نظام ادارة تأمين المعلومات ، و توضيح الأدوار والمسئوليات المطلوبةلتأمين المعلومات داخل المنظمة لمشروع ادارة نظام تأمين المعلومات .

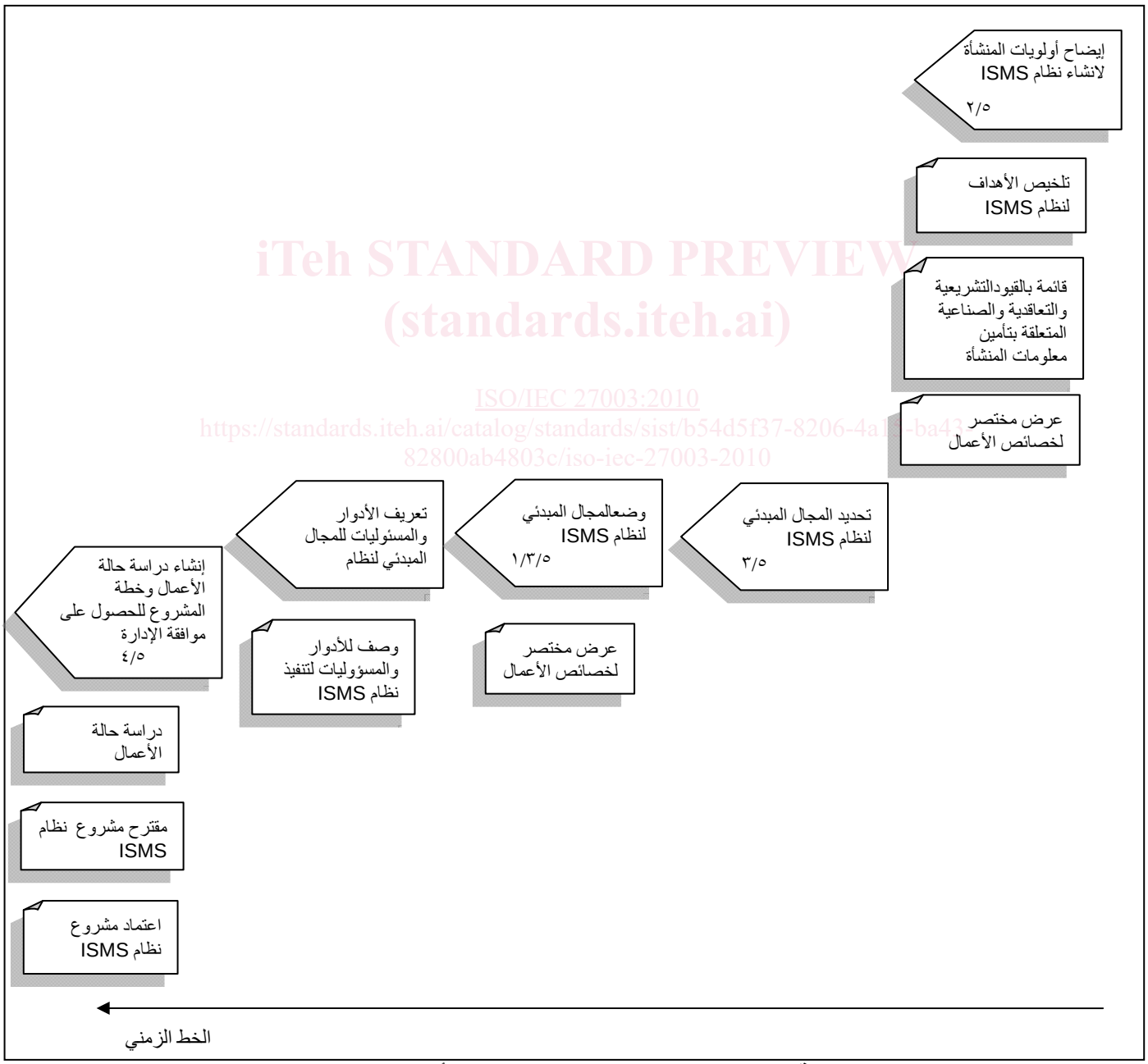
والمخرجات المتوقعة من هذه المرحلة ستكون الاعتماد المبدئي للإدارة والتزامها بتنفيذ نظام لإدارة تأمين المعلومات وأدائها للأنشطة الموصوفة فى هذه المواصفة الدولية ، والمستلمات من هذا البند تتضمن مستند دراسة حالة الأعمال ومسودة خطة مشروع نظام إدارة تأمين المعلومات مع المعالم المميزه.

يبين الشكل ٣ عملية الحصول على موافقة الإدارة للبدء فى مشروع إدارة نظام تامين المعلومات .

ملحوظة :

مُخرجالبند الخامس (التزام من الإدارة موثق بالتخطيط والتنفيذ لنظام إدارة تأمين المعلومات) وإحدى مُخرجات البند السابع (وثيقةمختصرة لحالة تأمين المعلومات) لا يُعدا من متطلبات المواصفة أيزو/أي إي سي ٢٧٠٠٠:٢٠٠٥ ، وعلى الرغم من ذلك ، فمخرجات هذه الأنشطة هى مدخلات يوصى بها للأنشطة الأخرى الموصفة فى هذا المستند .





شكل ٣: نظرة عامة عن الحصول على اعتماد الادارة لبدأ التخطيط لنظام ISMS

٢/٥ إيضاح أولويات المنشأةلانشاء نظام إدارة تأمين المعلومات

النشاط :

ينبغيادراج الأهداف لتطبيق نظام ادارة تأمين المعلومات مع أخذ أولويات ومتطلبات تأمين المعلومات للمنشأة في الاعتبار .

المدخلات :

ا) أهداف المنشأه الاستراتيجية.

ب) نظرة عامة على أنظمة الإدارة الحالية

جـ) قائمة بمتطلبات تأمين المعلومات القانونية والتشريعية والتعاقدية المنطبقة على المنشأة.

الإرشادات :

اعتماد الإدارة مطلوب عادةللشروع فى أي مشروع لنظام إدارة تأمين المعلومات ،لذلك فإن أول نشاط ينبغي البدء به هو جمع المعلومات الهامة والتى تمثل قيمة لنظام إدارة تامين المعلومات للمنشأة .وينبغى على المنشأة إيضاح مدى مساس الحاجة الى نظام إدارة تامين المعلومات وتقرير أهداف تطبيق هذا النظام والبدء فى مشروع النظام .

يمكن أن تتحدد أهداف تطبيق نظام إدارة تامين المعلومات من خلال الإجابة على الاسئلة التالية :-

أ) ادارة المخاطر – كيف ينشأ عن نظام إدارة تأمين المعلومات إدارة أفضل لمخاطر تأمين المعلومات ؟

ب) الكفاءة - كيف يمكن لنظامإدارة تأمين المعلومات تحسين ادارة تأمين المعلومات ؟

حـ) الميزة السوقية : كيف يتسنى للنظام خلق ميزة تنافسية للمنشأة؟

ومن أجل الإجابة على الأسئلة السابقة ، يجب استهداف أولويات ومتطلبات المنشأة بالعوامل المختلفة التالية :-

أ) الأعمال والمجالات التنظيمية الحيوية.

١-ما هى الأعمال والمجالات التنظيمية الحيوية.

٢-أى المجالاتالتنظيمية أمدادا بالأعمال ولأي درجة ؟

٣-ما هى العلاقات والاتفاقيات القائمة مع الطرف الثالث؟

٤-هل هناك أية خدمات يستعان بجهة خارجية للقيام بها؟

ب) المعلومات الحيوية أو الثمينة :

١-ما هي المعلومات الحيوية للمنشأة ؟

٢-ما هى التبعات المحتمل حدوثها إذا ما تم الكشف عن معلومات بعينها لبعض الأطراف غير المصرح لهم بذلك (مثال ذلك : فقدان الميزة التنافسية ، انهيار الاسم التجارى أو السمعة ، اجراءات قانونية ..... إلخ)

حـ) القوانين التى تحتم تدابيرلتأمين المعلومات

١- ما هى القوانين ذات العلاقة بمعالجة المخاطر أو تأمين المعلومات وتنطبق على المنشأة ؟

٢- هل المنشأة جزء من منظمة عمومية كبرى تتطلب أن يكون لها تقارير مالية لجهات خارجية ؟

د) الاتفاقيات التعاقدية أو التنظيمية ذات العلاقة بتامين المعلومات

١- ما هى متطلبات التخزين (شاملة فترات الاحتفاظ) للبيانات المخزونة ؟

٢- هل هناك أى متطلبات تعاقدية ترتبط بالسرية أو الجودة (مثال ذلك : اتفاقيات مستوى الخدمة (SLA))؟

هـ) متطلبات الصناعة التى توصف ضوابط تدابير بعينها لتأمين المعلومات :

١- ماهى المتطلبات المتعلقة بخصوصيات القطاع والمنطبقة على حالة المنشأة ؟

و) بيئة التهديد:

١- أى أنواع الحماية مطلوب وضد أية تهديدات ؟

٢- ما هى التصنيفات المميزة للمعلومات والتى تتطلب حماية ؟

٣- ما هى الأنواع المميزة لأنشطة المعلومات التى تحتاج الى الحماية ؟

ز) محفزات التنافس:

١- ما هو الحد الأدنى من متطلبات السوق لتأمين المعلومات ؟

٢- ما هى الضوابط الإضافية لتأمين المعلومات والتى تقدم ميزة تنافسية للمنشأة؟

ح) متطلبات استمرارية الأعمال :

١-ما هى عمليات الأنشطة الحيوية ؟

٢- ما المدة التى يمكن للمنظمة من خلالها احتمال انقطاعات عمليات أنشطتها ؟

يحدد المجال المبدئيلنظام إدارة تامين المعلومات بالإجابة على الأسئلة السابقة ، وهذا مطلوب أيضا لإنشاء حالة الأعمال والخطة الكليةلمشروع نظام إدارة تأمين المعلومات للحصول على اعتماد الإدارة . بينما يتم تعريف المجال التفصيلي لنظام ISMSأثناء المشروع .

وتلخص المتطلبات المذكورة فى أيزو /أي إي سي ٢٠٠٥:٢٧٠٠١ فى الفقرة١/٢/٤ أ) المجال بدلالة خصائص الأعمال والهيكل التنظيمى والموقع والأصول والتقنيات ، وتؤيد المعلومات الناتجة مما سبق هذا التحديد .

الموضوعات التى ينبغي أخذها فى الاعتبار عند صنع القرارات المبدئية فيما يختص بالمجال تتضمن ما يلى :

أ) ما هى حتميات ادارة تأمين المعلومات المؤسس من قبل ادارة المنشأة والالتزامات الخارجية المفروضة على المنشأة ؟

ب) هل يتحمل مسئوليات محتوى المجال المقترح للنظام أكثر من فريق من فرق الإدارة (مثلاً: الأفراد فى إدارات أدنى أو إدارات مختلفة) ؟

حـ) كيف ستوصل المستندات ذات العلاقة بنظام إدارة تأمين المعلومات عبر المنشأة (مثلاً:على الورق أو من خلال الشبكة الداخلية) ؟

د) هل يمكن لنظم الإدارة الحالية دعم احتياجات المنشأة ؟ هل تعمل هذه المنشأة بكامل طاقاتها وهل تصان بعناية وهل تعمل كما هو مخطط لها ؟

أمثلة لاهداف الإدارة التى قد تستخدم كمدخلات لتعريف المجال المبدئيلنظام إدارة تـأمين المعلومـات تتضـمن :

أ) تسهيل استمرارية العمال والإصلاح بعد الكوارث.

ب) تحسين القدرة على التعامل بمرونة مع الوقائع.

حـ) استهداف الالتزامات القانونية والتعاقدية .

د) التمكين من الحصول على شهادات طبقا لمواصفات دولية أيزو /أي إي سي أخرى .

هـ) التمكين من التطور التنظيمي للمنشأه ومكانتها.

و) خفض تكلفة ضوابط التأمين

ز) حماية الأصول ذات القيمة الاستراتيجية

ح) بناء بيئة ضبط داخلى صحيحة وفعالة .

ط) تقديم ما يؤكد للأطراف المعنية أن الأصول المعلوماتية تتمتع بالحماية المناسبة .

المخرجات :

مستلمات هذا النشاط هى :

أ) وثيقة تلخص الأهداف وأولويات تأمين المعلومات والمتطلبات التنظيمية لنظام ادارة تأمين المعلومات .

ب) قائمة بالمتطلبات التشريعية والتعاقدية ومتطلبات الصناعة ذات العلاقة بتأمين المعلومات فى المنشأة .

جـ) عرض مختصر لخصائص الأعمال والمنشأة وموقعها وأصولها وتقنياتها .

معلومات أخرى

أيزو/ أي إي سي ٩٠٠١ :٢٠٠٨ ، أيزو/ أي إي سي ١٤٠٠١ :٢٠٠٤، أيزو/ أي إي سي ٢٠٠٠٠-١ :٢٠٠٥ .

٣/٥ تحديد المجال المبدئى لنظام إدارة تأمين المعلومات

١/٣/٥ وضع المجال المبدئى للنظام

النشاط :

يجب أن تتضمن أهداف تنفيذ نظام إدارة تأمين المعلومات تعريف المجال ، الذى هو ضرورى لمشروع ادارة تأمين المعلومات .

المدخلات :

توضح مخرجات النشاط ٢/٥ أولويات المنشأة فى وضعها لنظام إدارة تأمين المعلومات .

الإرشادات :

فى سبيل تنفيذ مشروع نظام ادارة تأمين المعلومات ، يجب تعريف هيكل نظام إدارة تأمين المعلومات . والآن ينبغي تعريف المجال المبدئي للنظام، ليقدم للإدارة إرشادات لقرارات التنفيذ ولدعم المزيد من الأنشطة .

هذا المجال المبدئى ضروري لإنشاء دراسة حالة الأعمال وخطة المشروع المقترحة للاعتماد من قبل الإدارة .