ما تحتاج إلى معرفته قبل تنفيذ معايير ISO 27001

نتحدث في هذا المقال عن معايير وكيفية كتابة سياسات أمن المعلومات، مع التركيز على معايير ISO27001/ISMS، وذلك بالإجابة عن بعض التساؤلات حولها بالنسبة للمؤسسات. بالإضافة إلى النقاط الرئيسية التي يجب معرفتها قبل البدء في تطبيق هذه المعايير، والأخطاء الشائعة في التطبيق، ومتى يجب الحصول على شهادة ISO27001 الدولية.

يبدأ المقال بالتعريف بمصطلح أمن المعلومات ومفاهيمه الأساسية، ومعايير ISO27001، ثم مناقشة المعايير وأهميتها وشرح الفوارق بينها. وتأتي الخاتمة بتقديم بعض الحلول والتوصيات التي يجب الأخذ بها قبل تطبيق المعايير أو سياسات أمن المعلومات.

محدودية البحث

- لا يشمل القواعد والضوابط لـ ISO27001/ISMS
- لا يوجد قواعد إرشادية لتطبيق ISO27001/ISMS
- التعريف والإيضاح على شهادة ISO27001/ISMS لمعرفة الحاجة للحصول عليها أو الاكتفاء بالامتثال بالمعايير.

مقدمة

يعرف أمن المعلومات بأنه حماية نظام المعلومات من التهديدات المقصودة وغير المقصودة. وللشروع في تطبيق أمن المعلومات لابد من تحديد مكونات النظام والتهديدات، وكيفية اتخاذ الإجراءات المناسبة لمنع هذه التهديدات، أو التقليل من ضررها على المؤسسة.

يتكون نظام أمن المعلومات من عدة مكونات وهي المادي والبرمجي والبيانات وأنظمة قواعد البيانات والتطبيقات والشبكة والمستخدمين، مع العلم بأن كل جزء من هذه المنظومة قد يتعرض لمجموعة مختلفة من التهديدات. ويُعرف التهديد بأنه أي حالة أو حدث سواء كان مقصودًا أو غير مقصود ذات تأثير سلبي على نظام المؤسسة، ولا يمكن حصر التهديدات بصورة كاملة، لذلك يجب تحديد التهديدات الأكثر خطورة واتخاذ الإجراءات المناسبة من حيث الكلفة لمنعها أو التقليل من تأثيرها.

تعريف سياسات وإجراءات أمن المعلومات

تعرف بأنها قواعد عملية وفنية موثقة لحماية المؤسسة من مخاطر أمن المعلومات التي قد تلحق بأعمالها وبنيتها التحتية، وتقدم وثائق السياسات المكتوبة وصفاً عاماً للضوابط المختلفة التي ستستخدمها المؤسسة لإدارة مخاطر أمن المعلومات لديها، حيث تعد سياسات أمن المعلومات إعلاناً رسمياً عن نية الإدارة لحماية أصول المعلومات لديها من المخاطر المحتملة أو ذات العلاقة. وقد تكون سياسات أمن المعلومات مدعومة بإجراءات لأمن المعلومات توضح الأنشطة الرئيسية اللازمة لتطبيق تلك السياسات.

الهدف من استخدام معايير أمن المعلومات

إن الهدف الرئيسي من إعداد معايير أمن المعلومات هو توفير مرجعية تساعد المؤسسات على الآتي:

- إنشاء إدارات مستقلة تُعنى بإدارة أمن المعلومات داخل المؤسسة.
- تقييم المخاطر والتهديدات الأمنية المحدقة بمعلومات المؤسسة وأصول معالجة المعلومات.
- تطبيق الضوابط اللازمة لحماية معلومات المؤسسة ومرافق معالجة المعلومات.
- قياس مستوى إدارة أمن المعلومات.

الضوابط:

الضوابط Controls هي الإجراءات المضادة للمخاطر، ولها عدة أنواع:

- ضوابط التوجيه والتي عادة ما تكون إدارية، مثل وضع السياسات، والمطالبة بالعمل بمقتضى تلك السياسات.
- الضوابط الوقائية التي تحمي نقاط الضعف وتجعل الهجوم فاشلاً أو تَحدُ من آثاره، مع الضرورة توفير الرقابة المستمرة لعناصر النظام.
- ضوابط الكشف المؤدية لاكتشاف الهجمات.
- الضوابط التصحيحية للتقليل من تأثير الهجوم أو منعه.
- ضوابط الإنعاش، والتي غالبا ما ترتبط مع استمرارية الأعمال والتعافي من الكوارث.

التحديات الرئيسية

نشرت مؤسسة (Gartner) مجموعة كبيرة من المقالات التي تقدم إرشادات حول تطوير سياسة أمن المعلومات، ولا تزال الكثير من المنظمات تصارع لكتابة هذه السياسات على النحو التالي:

- صياغة ضوابط ذات طبيعة مرنة.
- صياغة سياسات لمنع كل شيء سيء من الحدوث، في مقابل ما يمكن منعه بشكل عملي.
- إن السياسة التي تعد منقولة أو تمت كتابتها لمؤسسة معينة لا يمكن نقلها لمؤسسة أخرى؛ وذلك لاختلاف طبيعة العمل مما قد يجعلها غير فعالة للحد من المخاطر للمؤسسة المنقولة إليها.
- السياسات التي لا علاقة لها في المخاطر التشغيلية في المؤسسة من الصعب، إن لم يكن من المستحيل تطبيقها.

*المصدر Gartner

ما هي معايير ISO/IEC 27000 series ؟

1. **معيار ISO / IEC 27000 :** سلسلة من معايير إدارة أمن المعلومات المنشورة من قبل المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الدولية الإلكترونية (IEC) المصممة لإدارة المخاطر والضوابط الأمنية داخل المؤسسة. يتم استخدام ISO دوليًا ويتم التعرف عليه على أنه شريط عالي المستوى للحصول على شهادة الأمان. ويمكن العثور على مزيد من المعلومات على الرابط التالي: http://www.iso.org/iso/home/standards/management-standards/iso27001.html

2. معيار **ISO 27002**: ضوابط تصف متطلبات نظام إدارة أمن المعلومات ولا تشمل أمن المعلومات لكنها تتضمن مجموعة من الضوابط التي من خلالها يمكن إدارة أمن المعلومات، فإذا قمت بعمل ضوابط للعمليات التشغيلية لأمن المعلومات في المكان الصحيح، ستكون إدارتك لأمن المعلومات الخاص فعّالة.

الأخطاء الشائعة في التطبيق

هناك العديد من الأخطاء الشائعة التي تعيق تطبيق سياسات ومعايير أمن المعلومات، وهي:

- **إسناد عمل السياسات لشركات غير متخصصة أو محترفة في ذلك.**
- **إسناد عمل السياسات لفريق تقنية المعلومات فقط.**
- **العمل بالسياسات التي يحتمل أن يكون تأثيرها على عمل المؤسسة بالكامل،** حيث يفضل أن يتكون فريق العمل من ممثلي الأقسام الأساسية في المؤسسة.
- **تطبيق معايير ISO27001 للحصول على الشهادة دون الدراسة الفعلية للحاجة إليها،** في كثير من الأحيان طبيعة عمل المؤسسة لا تتطلب الحصول على شهادة ISO27001 ولكن تتطلب مطابقة المعايير فقط وذلك لتقليل التكاليف، فعلى سبيل المثال: (العديد من المؤسسات الحكومية طبيعة عملها تنظيمي او تشريعي فلا يوجد لها منافس ولا توجد قوانين تلزمها للحصول على الشهادة، لذا تكتفي المؤسسة بتطابق معايير ISO2700).
- **الاتفاق مع شركات ذات سمعة عالمية،** الشركات العالمية، ذات خبرة طويلة لتنفيذ سياسات ISO27001 ولديهم خبراء متخصصين لفعل ذلك، ولكن نلاحظ بأن ممثلي المحليين لبعض الشركات الدولية ليسوا من ذوي الخبرة، بالإضافة لا تأخذ ثقافة المجتمع – أحياناً – بالحسبان، مما يجعل السياسة غير مناسبة للمؤسسة وبالتالي تصبح السياسات شكلية وغير فعالة.
- **النسخ واللصق:** بعض الشركات الاستشارية التي تنفذ المعايير والسياسات تقوم بعملية نسخ السياسات التي تم إعدادها لمؤسسة معينة وإعطائها لمؤسسة أخرى ويعكس ذلك عدم الأمانة وغياب الاحترافية، وجهل المؤسسة المنقول إليها بالمعايير ومواصفاتها .

هل يجب أن تحصل المؤسسة أو الشركة على شهادة ISO 27001؟

الشهادة ليست إلزامية - لذلك عليك أن تسأل نفسك سؤالًا مهمًا: **هل المؤسسة بحاجة للحصول على شهادة ISO27001** حقًا؟

هنالك الكثير من المؤسسات العالمية التي تطبق معايير أمن المعلومات دون الحصول على الشهادة، علما بأن العديد من الدول تضع قوانين وإجراءات صارمة للغاية لتنفيذ وضمان أمن المعلومات لاستمرارية الأعمال. ويجب الإشارة هنا إلى أن العديد من المؤسسات قامت بذلك باستخدام ISO 27001، ولكن القليل منها حصلت على شهادة ISO 27001. وقد اجمعوا جميعهم على: *(إن لم يكن هناك سبب لأخذ الشهادة إذاً نكتفي بالالتزام أو مطابقة معايير ISO 27001).* وهذا هو بالضبط ما تحتاج إلى القيام به والنظر فيه بعناية.

الأسباب المحتملة التي قد تجعلك تجد الشهادة مفيدة:

- **التسويق**: يمكنك استخدم الشهادة للحصول على بعض العملاء الجدد مثل المناقصات أو البقاء في العمل (على سبيل المثال، إذا كان منافسيك حصلوا على الشهادة).
- **طبيعة عمل المؤسسة**: إذا كانت المؤسسة تتعامل مع بيانات عملاء حساسة جداً وهنا يكون من الجيد الحصول على الشهادة لتنال ثقة العملاء.
- **الامتثال:** في حالات نادرة تتطلب منك بعض اللوائح أو القوانين حصولك على شهادة ISO 27001، وقد يكون لديك حالات توقع فيها عقودًا مع عملاء تلزمك بتطبيق أمن المعلومات أو استمرارية العمل المتوافقة مع هذه المعايير. وبدلاً من الاضطرار لأثبات تطبيق معايير أمن المعلومات لكل عميل، يمكن الحصول على الشهادة ISO 27001 كأثبات بالتزامك للعملاء.

إذا لم تجد المؤسسة إحدى هذه النقاط فعاله لها، فربما لا تحتاج إلى الشهادة على الإطلاق - يمكن أن تكون مؤسستك واحدة من تلك الشركات العديدة التي طبقت ISO 27001، لأنهم علموا أن القيمة الحقيقية في منهجية تطبيق المعايير، والشهادة فقط لتأكيد تطبيق المعايير وإعلان الحصول عليها.

الأخطاء التي يجب تجنبها في تنفيذ ISO27001

1. خطوات التنفيذ لا تتبع منطق المعيار
   - البدء في تنفيذ الضوابط دون القيام بتقييم المخاطر أولاً.
   - إجراء تقييم المخاطر قبل معرفة المتطلبات القانونية.
   - تحديد النطاق قبل معرفة سياق المنظمة.
   - المبالغة في تعقيد تقييم المخاطر.
2. كتابة الكثير من الوثائق
   - يفضل كتابة الوثائق على ألا تتعدى أكثر من 3 صفحات لكل سياسة.
3. كتابة وثائق غير قابلة للاستخدام
   - استخدام لغة فنية يصعب فهمها.
   - تطوير بعض القواعد الجديدة غير القابلة للتطبيق عند ممارسة السياسات.
4. شخص واحد فقط يعمل على المشروع
   - تنفيذ المعايير وكتابة السياسات عبارة عن إجراءات وعمل متتالي ويحتاج لفريق عمل وليس لشخص واحد فقط
5. مشاهدة تطبيق ISO 27001 كمشروع لتكنولوجيا المعلومات.
6. الإدارة العليا لا تدرك الفائدة الحقيقية من تنفيذ معايير ISO27001 وبتالي لا تقدم الدعم المناسب.

7. التوقع بأن تقوم الأدوات الخاصة بالمعايير بمعظم العمل كالآتي:
   - عدم الفهم الكافي أن تطبيق ISO27001 يدور حول تغيير سلوك الأشخاص
   - الاعتماد على قوائم المراجعة بدل من قراءة الوثائق الخاصة بالشركة.
   - شراء أدوات مكلفة أو معقدة فقط لتطبيق المعايير.

8. سيحقق تنفيذ ISO2700 أكبر الفوائد إذا جعلت جميع هذه القواعد الجديدة جزءًا من العمليات اليومية العادية.

الخلاصة:

عند الشروع لتنفيذ أي معايير يجب أولاً اختيار المعايير المناسبة لطبيعة عمل المؤسسة، ويجب على سياسات المؤسسة أن تتوافق مع الأنظمة والقوانين المنظمة لطبيعة عملها، فلا يصح عمل سياسات داخلية غير متوافقة مع الأنظمة والقوانين المحلية في الدولة التي تعمل بها. كما يجب على المؤسسة النظر بعناية إذا كانت بحاجة إلى الشهادة، وإن لم يكن هناك سبب لأخذ الشهادة إذاً تكتفي بالالتزام أو تطبيق معايير ISO 27001.

إبراهيم بن خليفة الشعيلي