الدرس السابع

نظام أمن المعلومات ISO27001

نظام أمن المعلومات ISO27001

تمهيد:تعتبر المعلومات من الأصول القيمة التي تؤثر بشكل مباشر على تقدم أو تدهور الشركات،لذلك فعند ادارتها بشكل فعال فإنها تتيح للشركات إمكانية العمل بثقة تامة.

1.نشأة المواصفة ايزو27001 :لقد تم نشر المعيار BS7799 في الأصل من قبل المعهد البريطاني BSI في عام 1995 وقد تمت كتابته من قبل وزارة التجارة والصناعة في حكومة المملكة المتحدة وهو مكون من عدة أجزاء:

- الجزء الأول: والذي يتضمن افضل الممارسات في أمن المعلومات وقد جرى تنقيحه في العام 1998 بعد نقاش مطول بين هيئات المعايير العالمية ثم تم اعتماده في النهاية من قبل الايزو أي أي سي 17799 تقنية المعلومات–قواعد الممارسة لادارة أمن المعلومات . في العام 2000 تمت مراجعة الايزو 17799 في جوان 2005 ثم دمجها أخيرا ضمن عائلة معيار ايزو27000.
- الجزء الثاني:تم نشره من BS7799 لأول مرة من قبل المعهد البريطاني للمعايير BSI في عام 1999 والمعروفة باسم الجزء الثاني من لBS7799 بعنوان نظم إدارة أمن المعلومات– تعريف وارشاد الاستخدام.

  تم اعتماد الجزء الثاني من المواصفة BS7799 من قبل ايزو كأيزو 27000 في نوفمبر 2005.
- الجزء الثالث:تم نشر الجزء الثالث من المعيار BS7799 في العام 2005 الذي يغطي تحليل وإدارة المخاطر والذي ينسجم مع ايزو 27001:2005

2.تعريف المواصفة ايزو27001: يعتبر معيار ايزو27001 الدولي محرك عمل فعال لكل مؤسسة تسعى لتحقيق إدارة أصول معلومات آمنة وعالية الخصوصية الى جانب حمايتها.كما يساعد على فهم آلية العمل وتحسينها بصورة مستمرة لمواكبة التحديات الحالية والمستقبلية بطريقة استباقية.

3.هيكل سلسلة المواصفات ايزو27000: ويتضمن مايلي:

- **المواصفة ISO27001**:تهتم بالاسس والمفردات التي تخص نظم أمن المعلومات

- **المواصفة ISO27002**:تهتم بالقواعد والممارسات العملية لأنظمة أمن المعلومات
- **المواصفة ISO27003**:هي دليل لتنفيذ إدارة امن المعلومات
- **المواصفة ISO27004**:لقياس فاعلية نظم إدارة أمن المعلومات
- **المواصفة ISO27005**:هي لإدارة المخاطر في نظام أمن المعلومات
- **المواصفة ISO27006**:هي دليل لعملية المصادقة على نظام إدارة أمن المعلومات.

4.فوائد تبني المواصفة ايزو27000: وتتمثل في:

- ✓ تحديد المخاطر ووضع الضوابط المناسبة لادارتها او للتخلص منها
- ✓ المرونة في وضع الضوابط في العمل
- ✓ الحصول على ثقة أصحاب المصالح والعملاء في ان بياناتهم محمية.
- ✓ الامتثال للضوابط بمنح الشركة ثقة العملاء بأنها المورد الأفضل.
- ✓ رفع مستوى القدرة في تلبية متطلبات المناقصات وبالتالي الحصول على فرص عمل جديدة.
- ✓ يوفر هذا المعيار تقنيات محددة وواضحة تسير عليها الشركة لحماية معلوماتها.
- ✓ تحسين وعي الموظفين اتجاه الحوادث الداخلية التي يمكن ان تحدث في بيئة الشركة.
- ✓ دعم حماية الشركة ومعلوماتها الخاصة من الهجمات وجميع تهديدات أمن المعلومات .
- ✓ وضع الحلول التكنولوجية التي تساهم في مكافحة نقاط الضعف المتعلقة بأمن المعلومات واستخدام التقنيات الحاسوبية المتنوعة لصد هجمات مجرمي الانترنيت وحماية جميع البيانات على شبكة الشركة.

5.مراحل الحصول على شهادة الايزو27001:

- ❖ **المرحلة الأولى**: هي مراجعة أولية غير رسمية لنظام إدارة امن المعلومات مثل التحقق من وجود واكتمال الوثائق الرسمية مثل سياسة أمن المعلومات المنظمة وبيان قابلية التطبيق وخطة معالجة المخاطر.

- **المرحلة الثانية:**تكون اكثر تفصيلا وتدقيقا رسميا،حيث يتم اختبار نظام إدارة أمن المعلومات بشكل مستقل وفقا للمتطلبات المحددة في الايزو27000. يؤدي اجتياز هذه المرحلة الى اعتماد نظام إدارة أمن المعلومات متوافق مع الايزو أي أي سي 27001.
- **المرحلة الثالثة:**التحسين المستمر وفيه يتم اجراء مراجعات متتابعة أو عمليات تدقيق للتأكد من أن المنظمة لا تزال على حالة الامتثال للمعايير.

تتطلب عملية الاحتفاظ بالشهادة إجراء عمليات تدقيق دورية لإعادة التقييم للتأكد من استمرار نظام إدارة أمن المعلومات ISMS في العمل على النحو المحدد والمقصود ويتم ذلك مرة واحدة سنويا.

6.مزايا الحصول على شهادة ISO27001: تتميز الشركات الحاصلة على شهادة ايزو27001 بالعديد من المميزات:

1. حماية تفاصيل الموظفين والعملاء.
2. منح العملاء والموظفين مزيدا من الثقة حول سياسة الشركة
3. تحسين سمعة الشركة على المدى البعيد
4. زيادة الأرباح وتقليل الخسائر نتيجة تجنب حصول انتهاكات للبيانات والملكية الفكرية.