**المحاضـرة العاشرة:**

# نظام إدارة أمن المعلومات الايزو 27000

## 1. مفهوم الايزو 27000:

**نظام إدارة أمن المعلومات ( الايزو 27000)** عبارة عن معيار عالمي يُعْنَى بحماية المعلومة، يتضمن مجموعة من المتطلبات و الذي أصدرته المنظمة العالمية للمواصفات، يحدد متطلبات الإلزامية لتأسيس و تطبيق و توثيق نظام إدارة المعلومات ،و تحديد متطلبات السيطرة لحماية المعلومات التي ستطبق وفق احتياجات المؤسسة.

## 3. أهمية تبني الايزو 27000:

من وراء ارتفاع التبادلات الرقمية، أنظمة المعلومات هي اليوم موصولة داخليا مع كل المخاطر الممكنة و مواصفة الايزو 27001 هي ضمان ثقة بين الشركاء و يمكن أن تصبح في عدّة حالات ضرورة، فأكثر من 5000 مؤسسة صادقت على أنظمة إدارة أمن المعلومات بالإمتثال للإيزو 27001، و العديد منها في الطريق لفعل ذلك نظرا لفعاليتها الواسعة للمساعدة في حماية تجهيزات و معلومات المؤسسة، فالتفعيل التدريجي لنظام إدارة أمن المعلومات يسمح للمؤسسات بتحقيق و بدون جهد كبير مستوى حماية قاعدي، اقتصادي أكثر، فاتباع خطوتين أو ثلاث خطوات إضافية يمكن المؤسسة من الحصول على نظام إدارة أمن المعلومات مطابق تماما للايزو 27001 و مناسب جدا لها، فكل مؤسسة بحاجة لضمان على الأقل الحد الأدنى من الأمن، فهذا المعيار أصبح اللغة المشتركة على مستوى المؤسسات، كما أن استخدامه يدعم ثقة الإدارة في المنهجية المتبعة من قِبل مسؤول أمن نظم المعلومات و مصداقيته، إذ تساعده على اتمام عمله بكل ارتياحية

## 3. فوائد الايزو ISO 27000 :

إن أهم الفوائد المتحققة من جراء استخدام ISO 27000 نظام إدارة أمن المعلومات تتمثل بما يأتي:

- تقدم هيكلية عامة تمكن المؤسسة من تطوير وتنفيذ نشاطات إدارة أمن المعلومات بصورة فاعلة.
- تقديم مدخل الخطر المعتمد ، والذي يعد نشاط أساسي ضمن هيكل تخطيط وتنفيذ النظام ، وينتج عنه زيادة فاعلية المستوى الأمني للمؤسسة.
- التأكيد على استخدام الأشخاص المؤهلين والعمليات والإجراءات والتقنيات المناسبة لحماية مصادر المعلومات.
- توفر حماية للمعلومات بكل موثوقية وسلامة و اتاحية.

## 4. أبعاد الايزو ISO 27000 :

تتمثل بما يأتي:

**1.4 سياسة الأمن:** يعمل هذا البعد على توثيق أهداف الـ (ISMS) لمساعدة إدارة المؤسسة على تقديم الدعم والتوجيه المناسبين.

**2.4 تنظيم أمن المعلومات:** يمكن هذا البعد إدارة المؤسسة من فرض سيطرة أمنية على كل المعلومات الخاصة بها والتي تقع تحت نطاق سيطرتها، عن طريق مجموعة من السياسات والإجراءات والمهام الأمنية والمسؤوليات.

**3.4 إدارة الموجودات:** يعمل هذا البعد على إدارة كل الموجودات الطبيعية والفكرية من خلال تقديم الحماية الملائمة لها، وذلك عن طريق تحديد ملكية ومسؤولية حماية مصادر المعلومات.

**4.4 أمن الموارد البشرية**: الغرض من هذا البعد هو تقليل المخاطر الناجمة عن الأخطاء البشرية، ويمكن إدارة الموارد البشرية من تقييم أداء كل العاملين في المؤسسة بصورة أكثر فاعلية، عن طريق المسؤوليات الأمنية المحددة لكل العاملين وضمن مواقعهم في التنظيم.

**5.4 الأمن الطبيعي والبيئي:** يساهم هذا البعد في تأمين المناطق المادية (تسهيلات معالجة المعلومات) وبيئة العمل داخل المؤسسة في إدارة أمن المعلومات بصورة فاعلة. إذ أن أي عنصر يقع ضمن نطاق عمل المؤسسة من تسهيلات وعاملين وزبائن وموردين يؤدي دورًا مهم في نجاح عملية حماية أمن معلومات المؤسسة.

**6.4 إدارة العمليات والاتصالات:** يوفر هذا البعد مجموعة من التسهيلات المتمثلة بـ (التسليم الآمن، وإدارة العمليات اليومية بصورة آمنة، ووسائل تشغيل البيانات والشبكات).

**7.4 السيطرة على الدخول:** إن السيطرة على العمليات دخول العاملين لنظام المعلومات، يعد بعدًا رئيسًا في حماية معلومات المؤسسة وحمايتها من الإختراقات الشبكية.

**8.4 تطوير أنظمة أمن المعلومات وصيانتها**: يهدف هذا البعد إلى تأكيد الأمن في نظم المعلومات والعمل على توفير متطلبات المحافظة عليها وصيانتها.

**9.4 الإدارة العرضية:** يساعد هذا البعد على مواجهة الحالات الطارئة وتحديد مواقع الضعف في إدارة أمن المعلومات وتقدم الحلول المناسبة من خلال بناء نظام اتصال فاعل بين المستويات التنظيمية المختلفة.

**10.4 إدارة استمرارية العمل:** يسمح هذا البعد بوجود مرونة مناسبة تسمح بمواجهة حالات الكوارث الطبيعية وحالات الفشل والعراقيل غير المتوقعة، تساعد على استمرارية أنشطة حماية المعلومات.

**11.4 الالتزام:** يسعى هذا البعد إلى تجنب أي ثغرات أو اختراقات لأي قوانين أو تشريعات مدنية أو جنائية، ويعرف الإلتزامات المتعاقد عليها ومتطلبات سياسات الأمن التنظيمية وفعاليات عمليات مراجعة النظام والإجراءات الأمنية.