المادة التعليمية: إدارة تكنولوجيا المعلومات

E-mail Centre Univ. Mila

المحور الثالث: بعض الإشكاليات الحديثة في إدارة تكنولوجيا المعلومات

المحاضرة الحادي عشر: نظم إدارة أمن المعلومات

Information Security Management Systems (ISMS)

د. سفيان خلوفي

الأيزو 27000 لأنظمة
إدارة أمن المعلومات

مفاهيم أساسية حول
نظم إدارة أمن
المعلومات

تجربة مايكروسوفت

مفاهيم أساسية حول نظم إدارة أمن المعلومات

1- إدارة أمن المعلومات: إحدى وظائف الإدارة:

تُعد وظيفة **مراقبة** نظام أمن المعلومات إحدى الوظائف الرئيسية لمدير نظم المعلومات، وهو بدوره يشكل جزءاً من الإدارة العامة للمنظمة. الهدف من المراقبة هو التأكد من أن نظام المعلومات الإداري قد تم تنفيذه كما هو مخطط، ومن أن النظام يعمل فعلاً لتحقيق الأهداف التي وضع من أجلها، ومن أن العمليات آمنة من الاستخدام السيئ.

غياب نظام الرقابة يمكن أن يؤدي إلى انتهاك أمن البيانات والمعلومات انتهاكاً متعمداً أو غير متعمد، وينتج عن ذلك تعديل أو تدمير أو إفشاء للمعلومات.

مفاهيم أساسية حول نظم إدارة أمن المعلومات

ينبغي على **نظام المراقبة** أن يكتسب ثلاث خواص أساسية، هي:

1- **السلامة:** يكون النظام سليماً إذا كان يعمل طبقاً لمواصفاته.

2- **القابلية للمراجعة المالية:** يكون النظام قابلاً للمراجعة المالية إذا ما كان قابلاً أن يخضع **للمحاسبة** وقابلاً للرؤية؛ وتعنى مقدرة المحاسبة أن المسؤولية محددة لكل عملية جارية كما تعنى الرؤية أن الاستثناءات من الأداء النمطي تصل إلى مدير النظم لتحظى باهتمامه.

3- **القابلية للمراقبة:** تسمح القابلية للمراقبة للمدير بأن يحتفظ بتأثير **توجيهي** للنظام.

مفاهيم أساسية حول نظم إدارة أمن المعلومات

2- فوائد إدخال (إدماج) أنظمة لإدارة أمن المعلومات

- **الامتثال للقوانين والتشريعات:** تضمن أنظمة إدارة أمن المعلومات الامتثال للقوانين المحلية والدولية التي تنظم حماية البيانات والخصوصية (مثل GDPR أو ISO 27001)، مما يقلل من المخاطر القانونية والمالية المرتبطة بعدم الامتثال.
- **تحسين الفعالية التشغيلية والحد من المخاطر(المالية والتشغيلية):** تسهم في تقليل التعقيد التشغيلي من خلال توحيد الإجراءات الأمنية وتعزيز الكفاءة في إدارة البيانات، مما يتيح تخصيص الموارد بفعالية.
- **تخفيض التكاليف (الكفاءة):** تقلل الأنظمة من التكاليف المرتبطة بالتهديدات الأمنية والانتهاكات، وتخفض النفقات الناتجة عن التعويضات أو فقدان السمعة، مع تحسين إدارة الموارد.

مفاهيم أساسية حول نظم إدارة أمن المعلومات

- **الاستعداد لاسترجاع المعلومات واستمرارية العمل وحماية البيانات الحساسة:** توفر خطط استرجاع المعلومات وأنظمة النسخ الاحتياطي أدوات لاستعادة البيانات بسرعة وضمان استمرارية العمليات في حالات الطوارئ، مما يعزز المرونة المؤسسية.
- **تحقيق الميزة التنافسية وتعزيز الثقة مع العملاء والشركاء:** يعزز الاستثمار في أمن المعلومات سمعة المنظمة، ويزيد ثقة العملاء والشركاء، مما يمنحها ميزة تنافسية في الأسواق المعتمدة على أمن البيانات.

مفاهيم أساسية حول نظم إدارة أمن المعلومات

إذن:

نظام إدارة أمن المعلومات هو من **نظم الإدارة الشاملة**، ويستند إلى منهج إدارة المخاطر في مجال إدارة الأعمال، ويهدف إلى إنشاء نظام لأمن المعلومات، وتنفيذه، وتشغيله، ومراقبته، ومراجعته، وصيانته وتطويره.

نظام إدارة أمن المعلومات يشمل إيجاد بنية تنظيمية، ووضع سياسات أمنية وتخطيط أنشطة الأمن المعلوماتي، وتحديد المسؤوليات، والممارسات والإجراءات، والعمليات والموارد اللازمة لإدارة أمن المعلومات بكفاءة وفاعلية.

مفاهيم أساسية حول نظم إدارة أمن المعلومات

النظام الأوروبي العام لحماية البيانات

General Data Protection Regulation، اختصار: جي دي بي آر (GDPR)

هو قانون لحماية البيانات والخصوصية في الاتحاد الأوروبي، يهدف إلى تمكين الأفراد من التحكم في بياناتهم الشخصية، وتنظيم تصدير البيانات خارج الاتحاد. يساهم النظام في توحيد القوانين داخل الاتحاد لتسهيل العمليات التجارية الدولية. تم اعتماده في 14 أفريل 2016 وأصبح نافذًا في 25 ماي 2018، مستبدلًا قانون حماية البيانات لعام 1995. كونه تنظيمًا مباشرًا وملزمًا، لا يتطلب تشريعات وطنية إضافية للتطبيق.

مفاهيم أساسية حول نظم إدارة أمن المعلومات

أمن المعلومات والأمن السيبراني

الأمن الحاسوبي أو الأمن السيبراني

أمن السايبر:

مجموعة من الممارسات والتقنيات المصممة لحماية أنظمة المعلومات والشبكات والبيانات من الهجمات الإلكترونية، بهدف ضمان السرية والنزاهة والتوفر للمعلومات الرقمية ووسائلها.

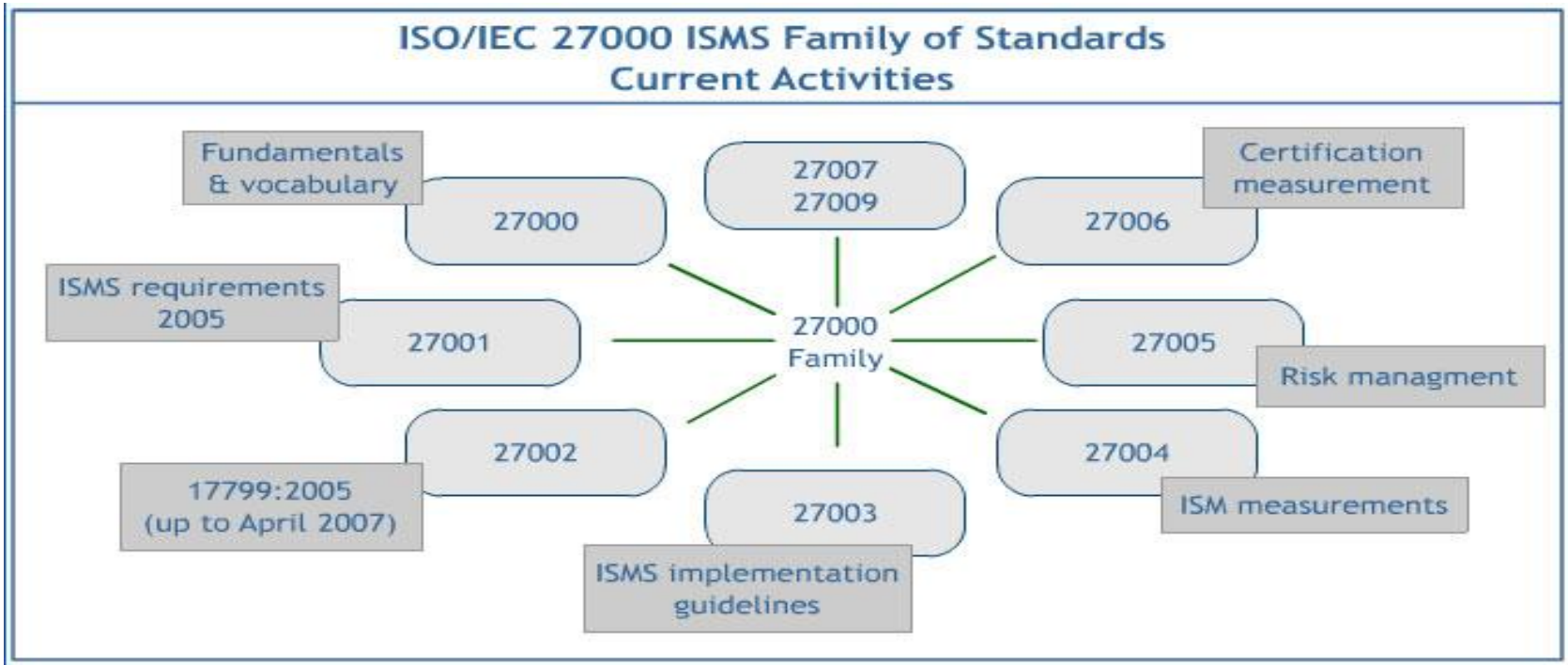
الأيزو 27000 لأنظمة إدارة أمن المعلومات

الايزو هو **الاسم المختصر لـ International Organization for Standardization** أي **"المنظمة الدولية لتوحيد المقاييس** منظمة التقييس الدولية، أو **ISO**، هي منظمة دولية مستقلة غير حكومية وغير ربحية، تعمل على تطوير ونشر معايير دولية موحدة تغطي مجموعة واسعة من الصناعات والقطاعات. يقع مقرها في جنيف، سويسرا، وتضم في عضويتها هيئات التقييس الوطنية من مختلف دول العالم.

المعهد الجزائري للتقييس: IANOR

الأيزو 27000 لأنظمة إدارة أمن المعلومات

لقد ظهر تعبير نظم إدارة أمن المعلومات **ISMS** رسمياً كأحد معايير الجودة، وأحد مكونات النظم الإدارية مع ظهور معيار الأيزو **ISO/IEC 17799** ويعرف أيضاً بالجزء الأول، ويحوي على 133 بنية معيارية مصنفة تحت أحد عشرة عنواناً رئيسياً، وبعد ذلك تتطور إلى المعيار **ISO/IEC27002** ويعرف أيضاً بالجزء الثاني، وهو أحد أفراد عائلة نظم إدارة أمن المعلومات المعيارية **ISO/IEC27000** الذي نشر لأول مرة عام 2000



الأيزو 27000 لأنظمة إدارة أمن المعلومات

ISO 27000

يُعتبر المعيار الأساسي الذي يحدد **المفاهيم والمصطلحات** المتعلقة بنظام إدارة أمن المعلومات.

يقدم نظرة شاملة عن أهداف ومعايير هذه العائلة.

ISO 27001

أهم معيار في العائلة، لأنه يحدد متطلبات إنشاء وتنفيذ وصيانة وتحسين **نظام إدارة أمن المعلومات** هو المعيار الوحيد في العائلة الذي يمكن للمؤسسات أن تحصل على شهادة مطابقة له.

يركز على:

- تقييم المخاطر الأمنية.
- وضع ضوابط لحماية البيانات.
- تحسين الإجراءات الأمنية باستمرار.

الأيزو 27000 لأنظمة إدارة أمن المعلومات

ISO 27002

يقدم **إرشادات عملية** حول كيفية تنفيذ ضوابط أمن المعلومات المحددة في المعيار ISO 27001.

يحتوي على قائمة بأفضل الممارسات الأمنية مثل:

- التحكم في الوصول.
- إدارة الأصول.
- التشفير.

ISO 27003

يُركز على **إرشادات تطبيق ISO 27001.**

يساعد المؤسسات على فهم كيفية تصميم نظام إدارة أمن المعلومات ISMS

الأيزو 27000 لأنظمة إدارة أمن المعلومات

ISO 27004

يتعلق بقياس **فعالية نظام إدارة أمن المعلومات**.

يقدم طرقًا لتقييم الأداء وضمان أن الإجراءات الأمنية تحقق أهدافها.

ISO 27005

يُركز على **إدارة المخاطر** في أمن المعلومات.

يقدم إطارًا لتحليل وتقييم المخاطر ووضع خطط للتخفيف منها.

ISO 27006

يحدد متطلبات الجهات التي تُصدر شهادات ISO 27001.

يضمن أن عمليات التدقيق والشهادات تتم بمعايير عالية الجودة.

الأيزو 27000 لأنظمة إدارة أمن المعلومات

ISO 27017

يقدم **إرشادات إضافية** للأمن في **بيئة الحوسبة السحابية**.

يساعد المؤسسات التي تستخدم خدمات السحابة على حماية بياناتها.

ISO 27018

يركز على **حماية البيانات الشخصية** في الحوسبة السحابية.

يضمن الامتثال لمتطلبات خصوصية البيانات.

ISO 27031

يتعلق بإدارة استمرارية الأعمال Business Continuity في سياق أمن المعلومات.

يساعد المؤسسات على التعامل مع الكوارث واستعادة الأنظمة بسرعة.

الأيزو 27000 لأنظمة إدارة أمن المعلومات

ISO 27701

معيار حديث يُركز على إدارة **الخصوصية**.
يُعتبر امتدادًا لـISO 27001 و ISO 27002، ويغطي متطلبات حماية البيانات الشخصية (مثل الامتثال لـ GDPR

عائلة ISO 27000 ليست مجرد مجموعة من الوثائق، بل هي دليل شامل يساعد المؤسسات على تحقيق أعلى مستويات الأمان. إنها مرجع عالمي لكل من يسعى لفهم أو تطبيق نظام إدارة أمن المعلومات.

تجربة مايكروسوفت

قدم خبير مايكروسوفت جون هوي John Howie من مركز أمن المعلومات المتميز، خبرة شركة مايكروسوفت في مجال أمن المعلومات، وفيما يلي الدروس الستة التي استخلصتها الشركة من تجربتها. في تطبيق أنظمة إدارة أمن المعلومات ISMS:

الدرس الأول: لا تقضم أكثر مما تمضغ

التعبير المجازي لهذا الدرس واضح، فعلى الشركات والمنظمات أن تبدأ بمشروعات أمن وحماية صغيرة ثم تتوسع، لأن المشروعات الصغيرة قابلة للسيطرة وبالتالي يحالفها النجاح أكثر ومن ثم التقيد بخطوات ديمنغ Deming: خطط، ومن ثم نفذ، وبعدها راجع، وأخيراً قيّم، وأن لا نتردد بالاستعانة بالخبراء الخارجين.

الدرس الثاني: أحصل على رعاية الإدارة العليا:

إن رعاية الإدارة العليا لمشروع إدخال أنظمة لإدارة أمن المعلومات يسهل عملية التنفيذ ويبرهن على الفائدة من المشروع والتكيف مع التطورات. فدعم الإدارة العليا يساعد على إحداث التغيير، ومرّكزة الأصول، وإدخال الإجراءات الجديدة والتغلب على مقاومة التغيير.

الدرس الثالث: اصبر وخذ الوقت الكافي

إن إدخال أنظمة جديدة، عادة، يأخذ وقت، فالخطط تحتاج إلى مراجعة أكثر من مرة، ويجب أن نتأكد من أن السياسات والأهداف مصاغة بشكل صحيح قبل الحصول على موافقة الإدارة، وكذلك مراجعة حقوق الوصول إلى المعلومات، أو منع الوصول إليها تأخذ وقت، وتحتاج إلى عقود واتفاقات مع الأطراف ذات العلاقة. العوائق والصعوبات التي تواجه المشروع الجديد، يجب أن لا تُحبط العزائم، وذلك لأن النتائج ذات قيمة مضافة عالية.

الدرس الرابع: ركز على الاتصالات الفعّالة

يجب التأكد من أن جميع أصحاب المصالح والأطراف ذات العلاقة على إطلاع بشكل واضح على مجريات المشروع الجديد، ويجب الإبلاغ عن جميع الأخطار والمشكلات ساعة ظهورها، وكذلك عن التقدم والنجاحات والاحتفال بها، حتى لو كان بعد عدة محاولات فاشلة.

الدرس الخامس: ابحث عن الفرص

بعد أن تكون أنظمة أمن المعلومات قد وضعت موضوع التطبيق، ينبغي العمل على تحسين أداء النظام الجديد أينما كان ذلك واضحاً، ابحث عن قضايا العمل والأخطار الجوهرية التي يمكن معالجتها لاحقاً لتحسين الأعمال. ولا تتردد في السير على الخط المحاذي للقضايا العالقة حتى تمر .Sidetracked

الدرس السادس: وثق ثم وثق أعمالك

التوثيق هو الجذع المشترك لنجاح مشروع نظام إدارة أمن المعلومات، وهذا التوثيق يجب أن يشمل:

-التصميم والتنفيذ. - فريق إدارة المشروع.

- المدققون الداخليون والخارجيون. - إجراءات الحصول على الشهادة...

وهذا، بالطبع يتطلب فريق عمل يتحلى بالحرفية والمهارة .

نهايـة العـرض

وشكـرًا لكـم