EU Twinning Project on
Statistics in Jordan

دائرة الإحصاءات العامة
Department of Statistics

# مقدمة عن معايير ISO/IEC 27001

## النشاط 1.4.6:
## سياسة الأمن وسرية البيانات

عمان، 8 كانون الثاني 2024

# الأجندة

- لماذا يتم اعتماد معيار ISO/IEC 27001
- ISO/IEC 27001 المفاهيم الأساسية
- ISO/IEC 27001 المتطلبات
- ISO/IEC 27001 الضوابط

# منظمات المعايير الدولية

- والمنظمة الدولية للمعايير ISO واللجنة الكهروتقنية الدولية IEC هما منظمتان دوليتان غير حكوميتين مستقلتان وتتمتعان بعضوية العديد من هيئات المعايير الوطنية، وتشاركان في وضع المعايير الدولية من خلال لجان فنية تنشئها المنظمة المعنية لمعالجة مجالات معينة من مجالات النشاط الفني.
- أعدت النسخة الثالثة من المعيار (ISO/IEC 27001:2022) من قبل اللجنة الفنية المشتركة ISO/IEC JTC 1، تكنولوجيا المعلومات، اللجنة الفرعية SC 27، أمن المعلومات والأمن السيبراني وحماية الخصوصية

# أمن المعلومات

- وتتعرض جميع المعلومات التي تحتفظ بها المنظمة وتجهزها للتهديد بالهجوم أو الخطأ أو الطبيعة (مثل الفيضان أو الحريق)، وما إلى ذلك، وتخضع لمواطن الضعف الكامنة في استخدامها. ويستند مصطلح أمن المعلومات عموما إلى المعلومات التي تعتبر أصولا لها قيمة تتطلب حماية مناسبة، مثلا، من فقدان التوافر والسرية والسلامة.
- وينطوي أمن المعلومات على تطبيق وإدارة الضوابط المناسبة التي تنطوي على النظر في طائفة واسعة من التهديدات، بهدف ضمان استمرار نجاح الأعمال واستمراريتها، والتقليل إلى أدنى حد من عواقب الحوادث الأمنية المتعلقة بالمعلومات.

# لماذا يتم اعتماد معيار ISO/IEC 27001

- ولا يؤخذ أمن المعلومات دائما في الاعتبار عند تصميم وتطوير نظم المعلومات. علاوة على ذلك، غالبًا ما يُنظر إلى أمن المعلومات على أنه حل تقني. بيد أن أمن المعلومات الذي يمكن تحقيقه بالوسائل التقنية محدود ويمكن أن يكون غير فعال دون أن تدعمه الإدارة والإجراءات المناسبة.

# لماذا يتم اعتماد معيار ISO/IEC 27001

- يعزز اعتماد ISO/IEC 27001 ثقافة تنظيمية واعية بالأمن ويضمن استمرار الامتثال والتحسين
- ISO/IEC 27001 ليس مطلبًا قانونيًا، ولا يعتبر أي من الضوابط إلزاميًا عالميًا للامتثال، لكن اعتماد معيار الأمن الدولي يضمن أفضل الممارسات والاستراتيجيات الأمنية لتعزيز أمن المعلومات في المنظمة.
- قد يقلل تنفيذ ISO/IEC 27001 من التعرض لاختراق البيانات وفقدان ثقة المستخدمين نتيجة لذلك.

# ISO/IEC 27001 المفاهيم الأساسية

- نظام إدارة أمن المعلومات: يتألف نظام إدارة المعلومات من السياسات والإجراءات والمبادئ التوجيهية والموارد والأنشطة المرتبطة بها، التي تديرها منظمة ما بصورة جماعية، لحماية أصولها من المعلومات.
- يستند إلى تقييم المخاطر ومستويات قبول المخاطر في المنظمة، وهو مصمم لمعالجة المخاطر وإدارتها بشكل فعال.
- ومن المتوقع أن يكون اعتماد نظام إدارة المعلومات قراراً استراتيجياً للمنظمة، ومن الضروري أن يكون هذا القرار متكاملاً بسلاسة وأن يتم تحسينه وتحديثه وفقاً لاحتياجات المنظمة.

# المبادئ الأساسية لنظام إدارة أمن المعلومات

- الوعي بالحاجة إلى أمن المعلومات
- تحديد المسؤوليات المتعلقة بأمن المعلومات
- التزام الإدارة
- دمج مصالح أصحاب المصلحة
- تقييم المخاطر لتحديد الضوابط المناسبة لتحقيق مستوى مقبول من المخاطر
- دمج الأمن كعنصر أساسي في المشاريع ونظم المعلومات
- منع الحوادث الأمنية المتعلقة بالمعلومات والكشف عنها بفعالية
- مواصلة إعادة تقييم أمن المعلومات وإجراء التغييرات عند الاقتضاء

# متطلبات ISO/IEC 27001

يتم تقسيم المعيار إلى بنود يتعين على كل منظمة تنوي أن تكون متوافقة مع ISO/IEC 27001 اتباعها.

- **سياق المنظمة**
- **القيادة**
- **التخطيط**
- **الدعم**
- **التنفيذ والعمليات**
- **تقييم الأداء**
- **التحسين**

# متطلبات ISO/IEC 27001

## سياق المنظمة

- الغرض من هذا الشرط هو التأكد من أن المنظمة تنشئ، تنفيذ نظام لإدارة أمن المعلومات وصيانته وتحسينه باستمرار، لديه فهم شامل لبيئته الداخلية والخارجية، يحدد ويفهم احتياجات وتوقعات أصحاب المصلحة فيه، حدود ونطاق نظام المنظمة لإدارة أمن المعلومات من أجل إدارة مخاطر أمن المعلومات بفعالية.

# متطلبات ISO/IEC 27001

## القيادة

- يوضح هذا المطلب أن الإدارة العليا للمنظمة يجب أن تظهر القيادة والالتزام بنظام إدارة أمن المعلومات. تقوم الإدارة برصد وتقييم نظام إدارة أمن المعلومات لضمان فعاليته.
- يجب أن يكون لدى المنظمة سياسة لأمن المعلومات توافق عليها الإدارة العليا. تعمل هذه السياسة كمبدأ توجيهي لإدارة أمن المعلومات في المنظمة ويجب أن تأخذ في الاعتبار عوامل مختلفة مثل استراتيجية العمل واللوائح والتشريعات والمخاطر والتهديدات المتعلقة بأمن المعلومات.
- يجب أن تحدد المنظمة الأدوار والمسؤوليات والسلطات المتعلقة بأمن المعلومات وتحددها.

# متطلبات ISO/IEC 27001

## التخطيط

- مطلوب من المنظمة تحديد وتطبيق عملية تقييم مخاطر أمن المعلومات لتحديد وتحليل وتقييم مخاطر أمن المعلومات.
- واستنادا إلى معايير قبول المخاطر، يجب تحديد وتطبيق عملية لمعالجة المخاطر المتعلقة بأمن المعلومات لاختيار الخيارات المناسبة لمعالجة المخاطر المتعلقة بأمن المعلومات وتحديد جميع الضوابط اللازمة لتنفيذ معالجة المخاطر المتعلقة بأمن المعلومات. ويقدم المعيار قائمة بالضوابط اللازمة (الملحق أ)
- يجب على المنظمة تحديد أهداف أمن المعلومات ووضع خطة لتحقيقها. ومن الضروري إجراء استعراض منتظم لأهداف وخطط أمن المعلومات لضمان جدواها وفعاليتها. يجب النظر في أي تغييرات في المنظمة وإدراجها في الخطط.

# متطلبات ISO/IEC 27001

## الدعم

- ويكفل هذا البند حصول المنظمة على الموارد اللازمة للحفاظ على أمن نظم معلوماتها. ويشمل ذلك تحديد وتوثيق الموظفين والمعدات والبرامجيات والموارد الأخرى اللازمة لأمن المعلومات. وتكفل المنظمة توافر هذه الموارد وسهولة الوصول إليها عند الاقتضاء، وكفاءة الموظفين وإدراكهم لأهمية أمن المعلومات وأدوارهم ومسؤولياتهم في الحفاظ عليها.
- يجب أن تضع المنظمة ممارسات تواصل فعالة مع أصحاب المصلحة المعنيين لضمان تحقيق أهداف أمن المعلومات.
- يجب توثيق وتحديث كل ما يتعلق بـ ISMS.

# متطلبات ISO/IEC 27001

## التنفيذ والعمليات

- يركز هذا المطلب على ضمان أمن معلومات المنظمة من خلال تخطيط عملياتها والتحكم فيها. يتضمن ذلك تحديد وتقييم المخاطر المرتبطة بعمليات المنظمة وتنفيذ ضوابط أمنية مناسبة للتخفيف من هذه المخاطر.

# متطلبات ISO/IEC 27001

## تقييم الأداء

- يتطلب هذا البند من المنظمة تقييم كيفية أداء ISMS والنظر في فعالية نظام إدارة أمن المعلومات. تحدد المنظمة ما يلزم رصده وقياسه، بما في ذلك عمليات وضوابط أمن المعلومات، وأساليب الرصد والقياس والتحليل والتقييم.
- تجري المنظمة مراجعات داخلية منتظمة للحسابات على فترات مقررة لتقييم نظام إدارة أمن المعلومات وتقديم معلومات عما إذا كان نظام إدارة أمن المعلومات ينفذ ويحافظ عليه بفعالية ويلبي متطلبات المنظمة.
- كما أن المنظمة مطالبة بإجراء استعراضات إدارية منتظمة لتقييم كيفية أداء نظام إدارة المعلومات والنظر في فعالية هذا النظام.

# متطلبات ISO/IEC 27001

## التحسين

- تعمل المنظمة باستمرار على تحسين ملاءمة وكفاية وفعالية نظام إدارة أمن المعلومات. وهذا يعني أن المنظمة بحاجة إلى مراجعة وتحديث ISMS بانتظام لضمان توافقها مع أهداف المنظمة والمتطلبات القانونية والتنظيمية ومعيار ISO/IEC 27001.
- وينبغي رصد عملية التحسين المستمرة واستعراضها لضمان فعاليتها، وينبغي إجراء أي تغييرات ضرورية لتعزيز ملاءمة وكفاية وفعالية نظام إدارة أمن المعلومات.

# تقييم المخاطر

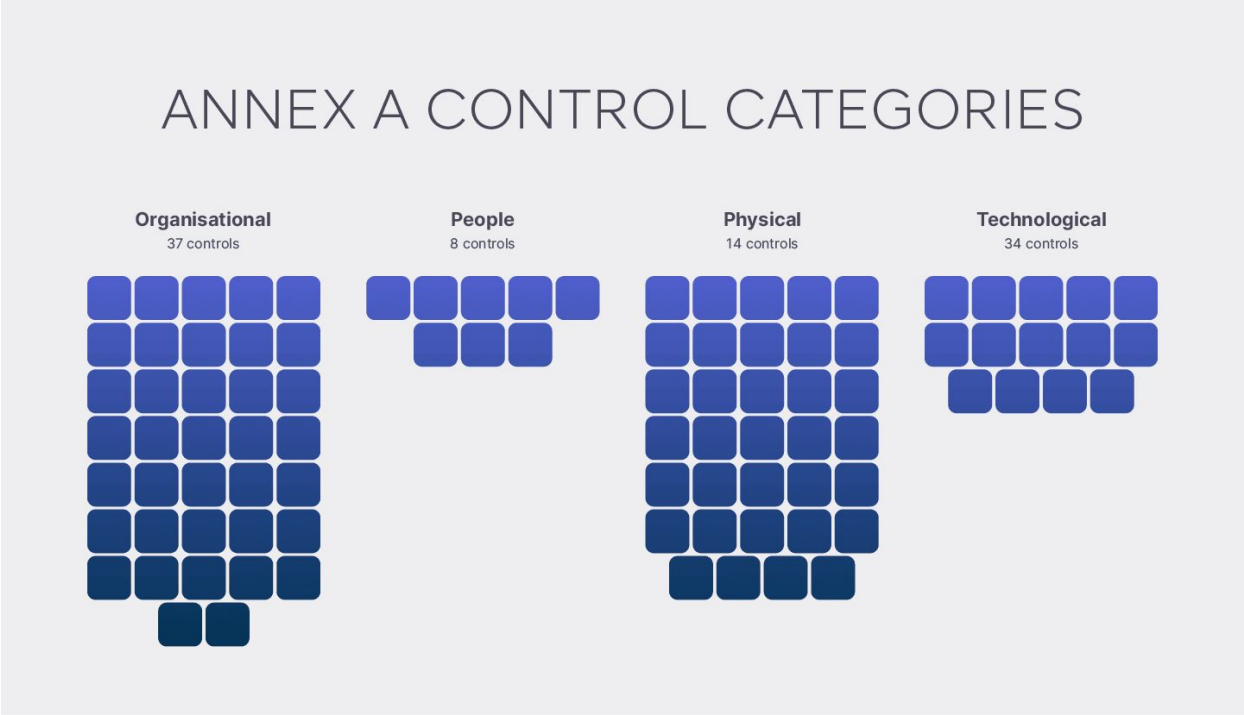
- ينبغي أن يحدد تقييم المخاطر المخاطر ويقيّمها كمياً ويحدد أولوياتها مقارنة بمعايير قبول المخاطر والأهداف ذات الصلة بالمنظمة. وينبغي أن توجه النتائج وتحدد الإجراءات والأولويات الإدارية المناسبة لإدارة مخاطر أمن المعلومات ولتنفيذ الضوابط المختارة للحماية من هذه المخاطر.
- يتضمن تقييم المخاطر ما يلي:
  - النهج لتقدير حجم المخاطر (تحليل المخاطر)
  - عملية مقارنة المخاطر المقدرة بمعايير المخاطر لتحديد أهمية المخاطر (تقييم المخاطر).
- وينبغي إجراء تقييم للمخاطر بصورة دورية لمعالجة التغيرات في متطلبات أمن المعلومات وفي حالة المخاطر.

# معالجة المخاطر

- وينبغي للمنظمة أن تحدد معايير لتحديد ما إذا كان يمكن قبول المخاطر أم لا، على سبيل المثال، إذا تم تقدير أن المخاطر منخفضة أو أن تكلفة حلها ليست فعالة من حيث التكلفة بالنسبة للمنظمة.
- بالنسبة لكل من المخاطر التي تم تحديدها بعد تقييم المخاطر، يجب اتخاذ قرار لمعالجة المخاطر. الخيارات الممكنة هي:
  - تطبيق ضوابط مناسبة للحد من المخاطر ؛
  - وقبول المخاطر، شريطة استيفائها لسياسة المنظمة ومعايير قبولها للمخاطر ؛
  - وتجنب المخاطر بعدم السماح باتخاذ إجراءات تتسبب في حدوث المخاطر ؛
  - تقاسم المخاطر المرتبطة بذلك مع أطراف أخرى، مثل شركات الموردين.
- وبالنسبة للمخاطر التي يكون فيها قرار معالجة المخاطر هو تطبيق ضوابط مناسبة، ينبغي اختيار هذه الضوابط وتنفيذها.

# المحلق أ ISO/IEC 27001

- الملحق أ في «ISO/IEC 27001» هو جزء من المعيار الذي يسرد مجموعة من الضوابط الأمنية السرية التي تستخدمها المنظمات لإثبات الامتثال لـ ISO/IEC 27001



# المحلق أ ISO/IEC 27001

- **الضوابط التنظيمية:** هي القواعد والتدابير التي تحكم النهج العام للمؤسسة لحماية البيانات عبر مجموعة واسعة من القضايا. تشمل هذه الضوابط السياسات والقواعد والعمليات والإجراءات والهياكل التنظيمية والمزيد..
- **ضوابط الأشخاص:** تنظيم المكون البشري لبرنامجهم لأمن المعلومات من خلال تحديد كيفية تفاعل الموظفين مع البيانات والمعدات. وتشمل هذه الضوابط الإدارة الآمنة للموظفين، وأمن الموظفين، والتوعية والتدريب.

# المحلق أ ISO/IEC 27001

- **الضوابط المادية:** هي تدابير تُستخدم لضمان أمن الأصول المادية. ويمكن أن تشمل نظم الدخول، وبروتوكولات الوصول إلى الضيوف، وإجراءات التصرف في الأصول، وبروتوكولات وسائط التخزين، والسياسات المكتبية الواضحة، وهي ضرورية لحماية المعلومات السرية.
- **الضوابط التكنولوجية:** هي قواعد وإجراءات رقمية يجب على المنظمات اعتمادها لتنفيذ بنية تحتية لتكنولوجيا المعلومات محمية ومتوافقة، من تقنيات التوثيق إلى تسجيل المعلومات.

# العمل من أجل الامتثال ل "ISO/IEC 27001"

ويمكن للقائمة التالية لأفضل الممارسات أن تعد شهادة ISO 27001:

- التشاور مع أصحاب المصلحة وتحديد توقعاتهم المتعلقة بأمن المعلومات
- تحديد نطاق نظام إدارة أمن المعلومات وضوابط أمن المعلومات
- وضع سياسة أمنية واضحة
- تحديد أصول المعلومات وما يرتبط بها من متطلبات أمن المعلومات
- إجراء تقييم للمخاطر لتحديد أي مخاطر قائمة ومحتملة تتعلق بأمن المعلومات
- تقييم مخاطر أمن المعلومات ومعالجة مخاطر أمن المعلومات
- اختيار الضوابط ذات الصلة وتنفيذها لإدارة المخاطر غير المقبولة
- إجراء تقييم مستمر لقوة ممارسات أمن المعلومات وتقييم المخاطر على أساس منتظم
- رصد وصيانة وتحسين فعالية الضوابط المرتبطة بأصول معلومات المنظمة

EU Twinning Project on
Statistics in Jordan

دائرة الإحصاءات العامة
Department of Statistics

# شكراً لحسن استماعكم