المركز الإحصائي
لدول مجلس التعاون لدول الخليج العربية
GCC-STAT

تقرير ملخص عن شهادة الأيزو ISO/IEC 27001:2013 في أمن المعلومات

مايو-2018م

مقدمة:

شهادة الأيزو ISO/IEC 27001:2013 في أمن المعلومات:

هي معيار لتقييم مدى الإلتزام في تطبيق معايير أمن المعلومات، وانطلاقا من حرص المركز الاحصائي لدول مجلس التعاون لدول الخليج على حماية ما لديه من بيانات ومعلومات إحصائية، فقد عكف المركز على الإعداد والتحضير للخطوات والتجهيزات اللازمة والممكنة للحصول على شهادة الأيزو ISO/IEC 27001:2013 في أمن المعلومات، وذلك من أجل التخفيف من المخاطر فيما يخص أمن المعلومات.

هناك ثلاث أنواع من الضوابط (إجرائية-تقنية-مادية)، وسعيا من المركز الإحصائي لدول مجلس التعاون لدول الخليج العربية للعمل على وضع سياسة بطريقة تتوافق مع التشريعات والنظم المعمول بها، وتطبيق أفضل الممارسات من أجل حماية المعلومات من الاستخدام غير المصرح به، أو الكشف عن أي استخدام غير مشروع أو تجاوزات ممكن أن تحدث وتخفيف الضرر في حالة وقوع أي حادث أمني، وذلك من خلال تطبيق الضوابط المناسبة، فقد عمل المركز على مدى أربع سنوات من أجل الوصول لهذا الهدف.

الضوابط الإجرائية:

تشمل الضوابط الإدارية والقوانين واللوائح وكيفية تشغيل العمليات اليومية والتي تتمثل في الموافقات الخطية والإلكترونية والسياسات والإجراءات والمعايير والمبادئ التوجيهية.

الضوابط التقنية:

بالإعتماد على استخدام البرمجيات والبيانات لمراقبة ورصد طرق الولوج إلى الشبكات ونظم المعلومات والتحكم بها، على سبيل المثال: تأمين كلمات المرور لتسجيل الدخول إلى أنظمة التشغيل، ولقراءة البريد الإلكتروني وتصفح الإنترنت بالإضافة الى تفعيل طرق وأدوات حماية أمن المعلومات المتمثلة في (التأمين المادي للأجهزة والمعدات-تركيب أنظمة مراقبة الشبكة للتنبيه عن نقاط الضعف-نشر الوعي بأمن المعلومات بين الموظفين-تركيب أجهزة دعم عدم انقطاع التيار الكهربائي وتركيب الجدران النارية، بالإضافة الى تركيب مضاد فيروسات وتحديثه بشكل دوري).

الضوابط المادية:

تتمثل هذه الضوابط في فصل أماكن العمل في المجالات الوظيفية ورصد ومراقبة بيئة العمل بما يشمل الدخول والخروج، وعلى سبيل المثال أنظمة التحكم في فتح وقفل الأبواب، البوابات الالكترونية، وأجهزة تكييف الهواء، وأجهزة استشعار الدخان، وأجهزة إنذار الحريق، ونظم إخماد الحريق، وكاميرات المراقبة في خارج المبنى وأمام مداخل الأدوار، وداخل مركز البيانات، وتأمين الكوابل بالإضافة الى وجود أفراد الأمن.

أمن المعلومات من الناحية العلمية:

هي السـياسـات والاسـتراتيجيات التي ينبغي توخيها لحماية المعلومات من مختلف الاعتداءات التي قد تتعرض لها والمخاطر التي يمكن أن تهددها.

من الناحية العملية:

هي مجموعة الوسائل والتدابير والإجراءات التي يجب توفيرها لتأمين حماية المعلومات من المخاطر سواء من داخل بيئة المعلومات محل الحماية أو من خارجها.

صياغة سياسة المعلومات:

هي مجموعة القواعد التي تتعلق بالوصول إلى المعلومات والتصرف فيها ونقلها داخل هيكل يعتمد المعلومة عنصرا أساسيا في تحسين أدائه وبلوغ أهدافه.

منطلقات سياسة أمن المعلومات:

السياسات وتوفير الوسائل التقنية والإجراءات الضرورية لحماية المعلومات.

تحديد المخاطر:

يجب تحديد المخاطر التي قد تهدد أمن المعلومات بدءا بالمشاكل العادية.

وسائل الأمن:

هي الطرق الخاصة بتوفير أمن المعلومات ضد المخاطر في حدود الإمكانيات التنظيمية والميزانية المرصودة للحماية.

أهداف سياسة أمن المعلومات:

1. التقليل من مخاطر أمن المعلومات إلى أقل مستوى ممكن.
2. حماية جميع المعلومات بشكل مناسب والحفاظ على سريتها.
3. إيجاد بيئة آمنة محمية وفق ضوابط محدده.
4. تعزيز وعي الموظفين بأمن المعلومات.
5. تصنيف المعلومات وفقاً لدرجة أهميتها لحمايتها من التعديل أو الكشف غير المصرح به.
6. القيام بإجراءات تقييم مخاطر المعلومات ونظم المعلومات وتحليل هذه المخاطر وإدارتها بصورة مستمرة.

الغاية من أمن المعلومات:

- إتباع أفضل الممارسات.
- إيجاد أنظمة الحماية.
- تفادي الخلل في صيانة التجهيزات.
- تفادي الخلل في صيانة البرمجيات.
- التقليل من سوء الاستخدام.
- التقليل من حوادث اختراق النظم.
- إيجاد بدائل في حال انقطاع التيار الكهربائي عن البنية التحتية.

سياسة أمن المعلومات:

هي عبارة عن دليل لأمن المعلومات يحدد إطار السياسة العامة لبناء أمن المعلومات في المركز الإحصائي لدول مجلس التعاون لدول الخليج العربية، ويناقش كيفية إدارة المركز لهذه المعلومات الحساسة، وحمايتها وتوزيعها، ومن هذا المنطلق تأتي سياسة أمن المعلومات لتلبي متطلبات العمل فيما يخص أمن المعلومات لتطبيقها وتحسين إجراءات التنفيذ من قبل جميع موظفي المركز كلٌ في مجال اختصاصه، وتنقسم السياسة إلى جزأين هما:

1. السياسات عالية المستوى.
2. السياسات المفصلة.

1. **السياسات عالية المستوى:**

يتطرق هذا الجزء الى السياسات من منظور عالي، وهو يحتوي على ثلاث سياسات، وهي:

- سياسة ادارة أمن المعلومات:

هذه السياسة مدعومة من قبل الإدارة العليا وهي تؤسس توجه الإدارة ودعمها وإرتباطها تجاه مبادرات أمن المعلومات في المركز الإحصائي.

- سياسة الإستخدام المقبول:

هذه السياسة تُعنى بالممارسات المقبولة المتعلقة بإستخدام موارد معلومات المركز الإحصائي، والتي تضم – وليس على وجه التحديد – كل أجهزة الحاسب الآلي، البرمجيات، خدمات الشبكات، خدمات البريد الإلكتروني، خدمات الإنترنت ووسائط التخزين.

- سياسة التوعية بأمن المعلومات:

تُعنى هذه السياسة بتوعية الموظفين بأنّ أمن المعلومات هو مسؤولية الجميع، وأنّ الكل مطالب بأن يثقف نفسه حول أمن المعلومات، ويحضر الفعاليات والتدريب وورش العمل المتعلقة بأمن المعلومات.

2. **السياسات المفصلة:**

يقسم هذا الجزء سياسات الأمن إلى أحد عشر مجالاً رئيسياً:

حماية وملكية البيانات، مضادات الفيروسات والبرامج الضارة، السياسات المتعلقة بالإنترنت، ضوابط الدخول، سياسة الشبكات، تطوير التطبيقات، أمن المكان المادية، إدارة العمليات، سياسة إستمرارية العمل، وسياسة الأفراد، والطرف الثالث. وكما ينقسم كل مجال أيضا إلى سياسات إضافية مصوبة نحو مختلف المستويات من أمن المعلومات.

خطوات البدء في تطبيق إجراءات أمن المعلومات:

- ايقان ودعم الإدارة العليا لأهمية أمن المعلومات.
- صياغة مسودة سياسة أمن المعلومات.
- تعيين خبير متخصص في أمن المعلومات.
- تشكيل لجنة تسيير أمن المعلومات تضم قيادات المركز.
- اعتماد سياسة أمن المعلومات.
- البدء في عقد اجتماعات لجنة تسيير أمن المعلومات.
- الشروع في البدء بتطبيق سياسة أمن المعلومات.
- إقامة ورش التوعية في أمن المعلومات وذلك من خلال محاضرات التوعية ورسائل البريد الالكترونية.
- اجراء تقييم المخاطر.
- تشكيل فريق تدقيق داخلي لأمن المعلومات مكون من موظفي مختلف إدارات المركز وتدريبه.
- اجراء تدقيق داخلي لأمن المعلومات بواسطة المدققين الداخليين.
- اجراء اختبار الاختراق لأمن المعلومات على الشبكة الداخلية تبعه اختبار خارجي بواسطة بيت خبرة.
- اجراء اختبار الاخلاء للموظفين في حالة الطوارئ.
- التعاقد مع بيت خبرة لإجراء اختبار التقييم للحصول على شهادة الأيزو 27001 في أمن المعلومات.

التحضير لإجراء اختبار التقييم والحصول على شهادة الأيزو 27001 في أمن المعلومات.

مراحل الحصول على شهادة الأيزو ISO/IEC 27001:2013 في أمن المعلومات:

التحضيرات:

من جانب ادارة المركز:

- وجود سياسة لأمن المعلومات.
- وجود حماية أمنية (أفراد أمن).
- تأمين المداخل والمخارج بأجهزة التحكم.
- التأكد من اغلاق مداخل ومخارج كل دور.
- إلزام جميع الموظفين بضرورة ارتداء البطاقات التعريفية للموظفين.
- تشكيل فريق عمل اخلاء الموظفين في حالة الطوارئ.
- الموافقة على تنفيذ خطة الاخلاء.
- اجراء تدريب خطة اخلاء.
- قيام المركز بالتعاقد مع أحد الشركات المتخصصة في اجراء اختبار تقييم الاختراق لأمن المعلومات.

من جانب موظفي المركز:

الالتزام بسياسة أمن المعلومات، التركيز على نظافة سطح المكتب (الطاولة + الكمبيوتر)، ارتداء البطاقات التعريفية، استخدام كلمات المرور الخاصة بهم، قفل أجهزة الحاسب الآلي أثناء التواجد خارج المكتب.

مراحل التقييم من قبل المدققين الخارجيين:

وضع برنامج التدقيق الخارجي:

تم وضع برنامج التدقيق من قبل الشركة المنفذة للتدقيق الخارجي، حيث تم اجراء التدقيق على مدى يومين متتالين خلال الفترة من 14-15 مايو 2018م.

المرحلة الأولى:

دراسة الوثائق:

قيام فريق التدقيق الخارجي بالاطلاع على بعض الوثائق الخاصة بالمركز من بينها السياسات وإجراءات العمل والتأكد من وجودها على ارض الواقع، فضلا عن محاولة فهم الإجراءات واكتشاف أي قصور أو ثغرة. بعد ذلك قيام الفريق بتدوين الملاحظات والتحضير من أجل ابرازها في تقريره النهائي وتقديمه لإدارة المركز.
مراجعة ما تم عمله من وثائق ومتطلبات ومنها:

- وثيقة توضح الهدف من نظام امن المعلومات وتوضح نطاق العمل.
- سياسة أمن المعلومات.
- منهج تحليل وتقييم المخاطر.
- تقارير تقييم المخاطر.
- اجراءات التعامل مع الأحداث الأمنية.
- تقارير التقييم الداخلي.

المرحلة الثانية:

زيارة مواقع العمل ومراجعة نطاق العمل وتطبيقه على ارض الواقع:

القيام بزيارة بعض الإدارات والاطلاع على إجراءات العمل والالتقاء بالموظفين.

تنفيذ برنامج التدقيق:

تم البدء في هذه العملية بإجراء اجتماع افتتاحي بحضور سعادة مدير عام المركز ومدراء الإدارات أعضاء لجنة تسيير أمن المعلومات، حيث تم تقديم معلومات وتوضيحات حول إجراءات التدقيق، وإعطاء ملخص حول الأهداف والمنهجية التي سوف تستخدم، وبعد ذلك مباشرة تمت عملية البدء في تنفيذ التدقيق على حسب الخطة.

الاجتماع الختامي بعد الانتهاء من إجراءات التدقيق:

إنتهت عملية التدقيق الخارجي بإجتماع ختامي بحضور سعادة مدير عام المركز ومدراء الإدارات أعضاء لجنة تسيير أمن المعلومات، قدم فيه مسؤول التدقيق ملاحظاته واستنتاجاته، والذي أوضح فيه وجود بعض الملاحظات البسيطة ويجب العمل على إغلاقها من قبل المركز والذي على أساسها يتخذ القرار النهائي، حيث أنه مبدئيا مرشح للحصول على شهادة الأيزو ISO/IEC 27001:2013 في أمن المعلومات ولكن بعد إغلاق كافة الملاحظات، وسوف يتم ارسال رسالة ترشيح للمركز لنيل الشهادة بعد مراجعة رد المركز حول الملاحظات.

تقرير التدقيق وردّ المركز على تقرير الملاحظات:

بعد الإنتهاء من القيام بإجراءات التدقيق الخارجي بأسبوع، تم إرسال التقرير من قبل مسؤول التدقيق والذي قد أوضح فيه بعض الملاحظات البسيطة والتي تم التوصل لها من خلال القيام بإجراءات التدقيق، ومنها يتبين أن المركز قد اجتاز أصعب المراحل، وقد منح المركز 15 يوماً للردّ على ما جاء من ملاحظات في التقرير، إلا أن المركز بعد استلام التقرير قام على الفور بالبدء في إغلاق الملاحظات ووضع العمليات التصحيحية وتحديد تاريخ تنفيذها، وارسال ذلك رسميا للجهة المنفذة للتدقيق.

وجاري حاليا انتظار رد الجهة المنفذة للتدقيق الخارجي، حيث أنها سوف تسعى للتأكد من إغلاق الملاحظات، وتحديد فيما إذا كانت هناك حاجة للقيام بمعاودة التدقيق مرة أخرى، أو الاكتفاء بما جاء في رد المركز، والمضي قدما في إجراءات تسليم شهادة الأيزو ISO/IEC 27001:2013 في أمن المعلومات، والتي سوف تستغرق فترة 6-8 أسابيع من بعد تأكيد الجهة المنفذة للتدقيق أنها قد قبلت رد المركز.

قرار منح الشهادة (لمدة ثلاث سنوات):

بعد اجراء العمليات التصحيحية، تنفذ عملية تدقيق نهائية ويقدم تقرير نهائي بالملاحظات والاستنتاجات التي يتم التوصل لها ودراستها من طرف لجنة منح الشهادات والتي يمكن أن يكون قرارها إحدى القرارات التالية:

- منح الشهادة فوراً.
- منح الشهادة فوراً مع مراجعة المتابعة.
- رفض منح الشهادة.
- مراجعة تكميلية.

مراجعة المتابعة:

فترة صلاحية شهادة الأيزو هي ثلاث سنوات، وتكون المتابعة خلال هذه الفترة لكل ستة أشهر .

المراجعة التكميلية أو الإضافية:

بناء على ردّ المركز وتفسيره للانحرافات يمكن أن يقرر إجراء ما يلي:

- مراجعة تكميلية:

بهدف الحصول على معلومات أو دلائل حول العمليات التصحيحية للقضاء على الانحرافات التي تم اكتشافها.

- مراجعة إضافية:

يمكن أن تقرر الجهة المنفذة للتدقيق الخارجي إجراء مراجعة إضافية بعد الحصول على الشهادة دون القيام بمراجعات المتابعة أو التجديد.

التجديد:

عند انتهاء فترة صلاحية الشهادة، تعاد إجراءات التدقيق الخارجي من جديد للحصول على شهادة جديدة، والهدف هو معرفة إذا ما تزال شروط الحصول على الشهادة ما زالت مستمرة، ويعتبر هذا التدقيق مكملا للتدقيق السابق.

تطلعات المركز الاحصائي لدول مجلس التعاون لدول الخليج العربية المستقبلية لما بعد الحصول على شهادة الأيزو ISO/IEC 27001:2013 في أمن المعلومات

إن مرحلة الحصـــول على هذه الشـــهادة هي البداية فقط إن تحقق ذلك على أرض الواقع، وهي التحدي الأكبر للمركز، حيث أن الوصـــول للقمة غالبا ما يكون ســـهلا نوعا ما، وذلك بعد اجتياز الصـــعوبات والتغلب على التحديات، ولكن المحافظة على البقاء في القمة هو التحدي الأكبر والأشـق، لذا سـوف يسـعى المركز بكل ما أوتي من موارد للمحافظة على هذا الإنجاز والاحتفاظ به والسـعي للتحسـين في الإجراءات المتعلقة بالعمل فيما يخص أمن المعلومات، وهذا لن يتأتى إلا بتكاتف جميع موظفي المركز من قيادات عليا وبقية الموظفين والذي يعول عليهم الدور الأكبر في المحافظة على هذا الإنجاز والاحتفاظ به من خلال ممارسـة الضـوابط المعمول بها كجزء من الأعمال اليومية الروتينية وعدم التسـاهل أو الاسـتهتار بها وتكثيف التوعية بأمن المعلومات وتطبيق الأسـس والمعايير المنظمة من أجل الوصـول للجودة الشـاملة في تأدية الأعمال.