المعايير الدولية الحديثة المتعلقة بأمن وخصوصية المعلومات

أصدرت المنظمة الدولية للمعايير (أو التوحيد القياسي) ISO مجموعة من المعايير المتعلقة بأمن وخصوصية المعلومات التي منها معيار المنظمة ISO/IEC ٢٧٠٠٥ لعام ٢٠١١ الذي يعطي المديرين والعاملين في مراكز وإدارات تكنولوجيا المعلومات إطار عمل مفصل لتنفيذ وتطبيق مدخل متكامل لإدارة المخاطر والتهديدات التي تواجههم في إدارة نظم أمن المعلومات بمنظماتهم. وتعرض مخاطر وتهديدات أمن المعلومات تهديدا متناميا لمنشآت الأعمال المختلفة مما قد يؤدي وبالمنشأة ذاتها. وتعتبر إدارة المخاطر أحد العناصر الرئيسية في الحد من عمليات الاحتيال والخداع علي الخط، وتعريف السرقات التي تتم، وتوضيح الضرر والأذي فيما يتعلق بمواقع الويب، وفقد البيانات الشخصية وكثير من المعلومات الأخرى لحوادث الأمن. وبدون تطبيق مدخل وإطار إدارة المخاطر في المنشأة المتسم بالرسوخ، فإن منشآت الأعمال والمنظمات المختلفة تعرض نفسها لأنواع كثيرة من أضرار الفضاء الخارجي الأكتروني.

ويرتبط هذا المعيار بتكنولوجيا المعلومات حيث يختص بأساليب الأمن المتعلقة بإدارة مخاطر أمن المعلومات وما يرتبط بها من أفعال مما يسهم في تمكين كل المنشآت باختلاف أنواعها في ترشيد وتحسين سبل الأمن بها. كما يساند هذا المعيار المفاهيم العامة المحددة في المعيار التي أصدرتها المنظمة في السابق وهي ISO/IEC 27001 لعام 2005 الذي يتعلق بتكنولوجيا المعلومات وأساليب الأمن ونظم إدارة أمن المعلومات ومتطلبات ذلك حيث أنه يعتبر معيار ضروري لمن يريد إدارة المخاطر التي يتم مواجهتها بفعالية عند الإلتزام به. وفي هذا الشأن، تعابر إدارة المخاطر ذات طبيعة حرجة لحوكمة الأعمال الجيدة، ومساعدة المنشآت بالنصيحة عن لماذا تدار مخاطر أمن المعلومات؟ وتحديد ماهيتها وكيفية أدائها في مساندة أهداف الحوكمة للأعمال المختلفة. وقد تم تحديث هذا المعيار لكي يعكس مختوي وثائق إدارة المخاطر المتمثلة في المعايير التالية:

- معيار ISO 31000 لعام 2009 عن مبادئ وتوجيهات إدارة المخاطر.
- معيار ISO/IEC 31010 لعام 2009 عن أساليب تقدير وتقييم المخاطر المتصلة بإدارة المخاطرة
- دليل معيار ISO Guide 73 لعام 2009 عن المصطلحات المختلفة المتضمنة في إدارة المخاطر.

وعلي ذلك فإن معيار ISO/IEC 27005 لعام 2011 يرتبط بطريقة مباشرة مع معيار ISO 31000

لعام 2009 بهدف مساعدة منشآت الأعمال والمنظمات المختلفة في إدارة مخاطر أمن معلوماتها بطريقة متشابهة للطريقة التي تداوِر بها أنواع المخخاطر الأخرى وخاصة المخاطر الطبيعية. وعلي هذا الأساس فإن ISO/IEC 27005 سوف يساعد مستخدميه في تنفيذ معيار /ISO IEC 27001 لعام 2005 المتعلق بنظام إدارة أمن المعلومات المبني علي مدخل إدارة المخاطر. وعلي الصعيد الدولي يعتبر كل من معيار ISO/IEC 27001 ومعيار ISO/IEC 27002 لعام 2005 الخاصين بتكنولوجيا المعلومات وأساليب الأمن وأكواد المزاولة لإدارة أمن المعلومات مما يعتبر مهما لفهم تلك المعايير الدولية بطريقة كاملة.

مما تقدم فإن عملية إدارة المخاطر تتضمن المهام التالية:

- **إنشاء السياق العام**
- **تقديم وتقييم المخاطر**
- **قبول المخاطر**
- **اتصال المخاطر**
- **مراجعة وضبط المخاطر**

وعلي ذلك، فإن هذا المعيار لا يقدم أي منهجية معينة لإدارة مخاطر أمن المعلومات، وكنه يمثل مدخلا عضويا لذلك. كما أنه يعتمد علي المنشأة أو المنظمة أن تعرف مدخلها لإدارة المخاطر بها التي تتعلق بإدارة أمن المعلومات المبني علي سياق المخاطر.

إلي جانب ما سبق عرضه من معايير أمن المعلومات صدر حديثا معيار ISO/IEC 15944-8 لعام 2012 الخاص بالرؤية التشغيلية للأعمال فيما يتعلق بتعريف متطلبات حمايى خصوصية المعلومات لقيد خارجي علي معاملات الأعمال. وقد طور هذا المعيار لمساندة نمذجة المتطلبات الدولية العضوية لتعريف وتقديم حماية خصوصية المعلومات الشخصية فيما يتصل بتكنولوجيا الاتصالات والمعلومات المبنية علي معاملة العمال المتعلقة بالأفراد من العملاء أو المستهلكين. ويقدم هذا المعيار للمستخدمين والمصممين المنهجية والأدوات التي تخاطب المتطلبات المفروضة من خلال المجالات التشريعية والقانونية. وفي نفس الوقت يوجه هذا المعيار الرؤية التشغيلية للأعمال التي سبق تطويرها في المعيار السابق ISO/IEC 14662 وما يرتبط به من معيار ISO/IEC 15944-1 ومعيار ISO/IEC 15944-5 بالإضافة لكثير من المراجع الدولية في هذا النطاق.

وينمذج معيار ISO/IEC 15944 متطلبات المجالات التشريعية القانونية كقيود خارجية علي إنشاء واستخدام وتبادل وإدارة بيانات دورة خياة المعلومات، أما معيار SO/IEC 15944-8 لعام 2012 يخاطب سياق متطلبات السياسة العامة المتعلقة بالمجالات التشريعية التي تراقب استخدام المعلومات الشخصية وتتضمن التنظيمات والإجراءات المتطلبة لحماية العميل وحماية خصوصيته وتوفر إمكانية الوصول الفردي للمعلومات، إلخ.

ويعرف هذا المعيار (11) مبدءا عضويا ودوليا ترتبط بحماية الخصوصية بواسطة متطلبات المنشآت والمنظمات الدولية والأقليمية، حيث ينمذج كل من المساحة التعاونية المتعلقة بأي معاملة أو تصرف أعمال، واللإلتزام بتبادل المعاملات واتصرفات المختلفة، كما يقدم المبادئ والقواعد التي تحكم إنشاء وإدارة واستخدام هويات الأفراد المتضمنة الاستخدام القانوني الخاص بالأسماء المعرفة وتحديد الهويات وتوضيح طرق عدم التعرف علي الهويات كاستخدام الأسماء المستعارة وغير المحددة للأسماء الشخصية.

إلي جانب ما تقدم، يوفر هذا المعيار المبادئ التي تتحكم في إدارة دورة حياة النظام وتحديد القواعد والمجالات المشفرة أو المكودة التي تختص بتقبل المعلومات وتجميعها، وتحديد التعبيرات المتعلقة بها، والتخلص من السجلات غير الضرورية واستبعادها، وكل ذلك يسهم في توضيح متطلبات حماية خصوصية المعلومات.