

تاريخ القبول: 2020/01/09

تاريخ الإرسال: 2019/06/02

تاريخ النشر: 2020/04/26

انتشار تطبيق نظام إدارة أمن المعلومات ISO27001 في منظمات الأعمال: دراسة تقييمية للفترة (2006-2017)

Spread Application of Information Security Management System ISO27001 in Business

Organizations: Evaluation Study for the Period (2006-2017)

¹. صحراوي إيمان / SAHRAOUI IMENE

جامعة سطيف 1 @yahoo.fr. imenesah

². بن سديرة عمر / Bensedira Amor

جامعة سطيف 1 . BensediraAmor @yahoo.fr

³. بوحروود فتيحة / Bouheroud Fatiha

جامعة سطيف 1 . BouhroudFatiha@yahoo.fr

الملخص:

هدفت هذه الدراسة إلى إبراز أهمية إدارة أمن المعلومات كمدخل حديث تتمكن من خلاله منظمات الأعمال من صناعة التميز في ظل بيئة أعمال تتسم بالتغيرات التكنولوجية الهائلة، هذه الأخيرة إلى جانب أنها تتيح مجموعة من فرص النمو والتطور للمنظمات فإنها تفرض مجموعة من التهديدات التي تتحكم في بقائها واستمراريتها، كما بينت نتائج تحليل المعطيات الإحصائية لمستوى انتشار معيار (ISO27001) لدى مختلف الأقاليم والدول، أن هناك اتجاها متصاعدا نحو اعتماد

هذا المعيار من طرف مختلف المنظمات العالمية سعيا منها للحفاظ عن خصوصية وسرية معلوماتها كمفتاح للنجاح في البيئة التنافسية الشديدة.

الكلمات المفتاحية: أمن المعلومات، إدارة أمن المعلومات، ISO27001، منظمات الأعمال.

Abstract:

This study aimed to highlight the importance of information security management as a modern entry through which contemporary organizations of the industry of excellence in the context of a business environment characterized by tremendous technological changes, the latter as well as providing a range of opportunities for growth and development of organizations, imposes a range of threats that control their survival and continuity, as illustrated by the analysis of the statistical data of the prevalence level of the ISO27001 standard in different regions and states, shows that there is a growing trend towards the adoption of this standard by various global organizations in an effort to preserve the privacy and confidentiality of their information as a key to success in The highly competitive environment.

Key Words: information security, information security management, ISO27001, Business Organizations.

المؤلف المرسل: بن سديرة عمر، الإيميل: BENSEDIRAAMOR @YAHOO.FR

المقدمة:

خلال السنوات القليلة الماضية انتقل العالم بقيادة الدول الصناعية المتقدمة عبر مرحلة انتقالية من عصر الثورة الصناعية إلى عصر ثورة المعلومات، بحيث تعتمد هذه المرحلة بشكل رئيسي عن المعلومات كمورد استثماري وكسلعة استراتيجية وكمصدر للدخل القومي، إضافة إلى كونها قوة محركة للتطور الاقتصادي السريع.

وواكب هذا العصر مجموعة من التطورات التكنولوجية السريعة التي أثرت بشكل أو بآخر على التقدم الاقتصادي وساعدت في تكوين العصر الاقتصادي الجديد.

وتشكل المعلومات البنية التحتية للمنظمات التي تمكنها من أداء مهامها، إذ أن نوع المعلومات وكميتها وطريقة عرضها تعتبر الأساس في نجاح عملية صنع القرارات داخل المنظمات المعاصرة، وعليه فإن للمعلومات قيمة عالية تستوجب وضع الضوابط اللازمة لاستخدامها وتداولها ووضع السبل الكفيلة بجيازتها، لذا فإن الإشكالية التي يجب أخذها في الاعتبار هي توفير الحماية لها وإبعادها عن الاستخدام غير المشروع.

إن حماية وأمن المعلومات يعد من بين أهم مجالات اهتمام منظمات الأعمال المعاصرة، خاصة في ظل تعدد الآثار التي أفرزتها المتغيرات البيئية الجديدة وما يترتب عنها من تهديدات تتعلق بسرية وخصوصية المعلومات التي يتم تبادلها بين الأطراف أثناء إبرام صفقات المعاملات الالكترونية، فالمعلومات أثناء تدفقها عبر شبكة الأنترنت يمكن أن تحول ويقرأ محتواها خصوصاً المعلومات المالية، كما يمكن أن تتعرض مواقع منظمات الأعمال إلى عمليات الاختراق والتخريب من طرف قراصنة الأنترنت مما حتم اللجوء إلى مجموعة من الآليات والأنظمة التي توفر السرية، الأمن والخصوصية.

- **إشكالية البحث:** من أجل توحيد وتأمين نظام المعلومات الخاص بالمنظمات، قامت منظمة التقييس الدولية بإعداد معيار ISO27001، بهدف رفع مستوى الوعي لدى المنظمات لإدارة أمن معلوماتها وحماية مصالحها في بيئتها التنافسية؛ وعلى هذا الأساس تم طرح الإشكالية التالية: ما مدى انتشار تطبيق نظام إدارة أمن المعلومات (ISO27001) في منظمات الأعمال ؟

- **فرضيات البحث:** وللإجابة عن هذه الإشكالية نضع الفرضية التالية:

- يوجد اختلاف في مدى انتشار نظام ISO27001 لدى منظمات الأعمال في شتى أنحاء العالم.

- **أهداف البحث:** يهدف البحث إلى تحقيق العناصر التالية:

- التعريف بنظام إدارة أمن المعلومات.
- شرح متطلبات ومضمون نظام إدارة أمن المعلومات ISO27001.
- إبراز أهمية تطبيق نظام ISO27001 في منظمات الأعمال لتحقيق التميز.
- تحليل مستوى تبني نظام أمن المعلومات ISO27001 على مستوى مختلف الدول والأقاليم.

- **أهمية البحث:** تبرز أهمية هذا البحث باعتباره إضافة للتراكم المعرفي الموجود في حقل إدارة أمن المعلومات كمدخل إداري معاصر يمكن المنظمات من المحافظة على أمن وسرية معلوماتها وبالتالي الصمود في وجه المنافسة، كما يتضمن إسهاما فكريا وتحليلا موضوعيا لتوجه الدول والمنظمات نحو اعتماده بشكل متزايد اعتبارا من 2006 التي توافق سنة أول إصدار لسلسلة مواصفات ISO27000.

أولا. مفهوم إدارة أمن المعلومات:

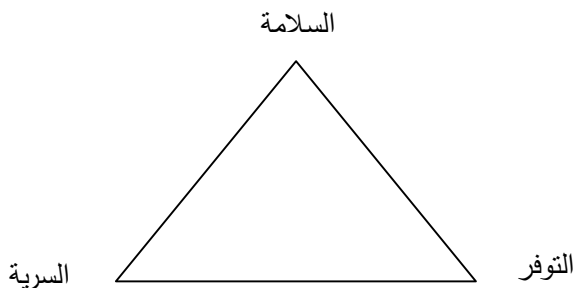
1. تعريف أمن المعلومات: يتضمن نظام المعلومات مجموعة متماسكة من الموارد لجمع المعلومات ومعالجتها وتخزينها ونشرها داخل المنظمة، وتعتبر المعلومات من الأصول الضرورية والتي هي بحاجة إلى الحماية الكافية؛ ويشير مفهوم أمن المعلومات إلى حماية سرية وسلامة أصول المعلومات، سواء أثناء عملية التخزين أم المعالجة أو النقل، من خلال الاعتماد على التكنولوجيا وتطبيق سياسات التعليم والتدريب¹. كما يعكس هذا المضمون أيضا المفاهيم والتقنيات والتدابير التكنولوجية والإدارية المستخدمة لحماية أصول المعلومات من الوصول غير المأذون به عمدا أو سهوا أو حيازتها أو الإضرار بها أو كشفها أو التلاعب بها أو تعديلها أو فقدانها أو إساءة استخدامها².

وعليه، فأمن المعلومات هو حمايتها من كل وصول غير مسموح أو غير مصرح به، وتأمين أنظمة المعلومات بما تشمله من البنى التحتية التي تسهل استخدامها كالتقنيات والعمليات والخدمات والمعلومات. بمعنى؛ التدابير والتوجيهات التي تصدرها إدارة المنظمة بهدف حماية مواردها التقنية وما تحويه من معلومات في

مختلف أشكالها، بغرض تحقيق سلامتها وتوافرها وسريتها وفق الصلاحيات والترتيبات المتعارف عليها.

2. تعريف إدارة أمن المعلومات: إدارة أمن المعلومات هي عبارة عن سلسلة من الأنشطة الإدارية التي تهدف إلى حماية وتأمين أصول المعلومات في إطار المنظمة ونظام المعلومات فيها، وتقييم أصول هذه المعلومات قد يختلف من منظمة إلى أخرى³. وتسعى المنظمات من خلال إدارة أمن المعلومات إلى تحقيق الثالوث (CIA Triangle) ويعني: السرية والخصوصية (Confidentiality)، التكاملية والسلامة (Integrity)، التوفر والإتاحة (Availability)؛ وهذه العناصر يمكن اعتبارها الخصائص الواجب توافرها في المعلومات كي تصبح ذات قيمة⁴؛ أو كما وصفتها هيئة معايير معالجة البيانات الاتحادية (Federal Information / FIPS Processing Standers) سنة 2004 بأحجار الزاوية لحماية المعلومات، وذلك من خلال تطبيق نظم إدارة حماية المعلومات، أو باستعمال معايير ISO27001 كدليل لتطوير ISMS⁵، كما في الشكل التالي:

الشكل (1): أبعاد إدارة أمن المعلومات



المصدر: علي عبد الستار عبد الجبار الحافظ، أحمد هاني محمد النعيمي، دور ISO 27001:2005 في تعزيز مفهوم إدارة دورة حياة المعلومات، متوفر على مستوى الموقع: <https://www.kantakji.com>، (تم الاطلاع في: 2019/02/10). ويمكن توضيح هذه الأبعاد الثلاثة فيما يلي⁶:

أ. السرية: هذا البعد يوفر للمنظمة السرية التامة لكافة المعلومات، حتى لو كانت المعلومات صغيرة وبسيطة.

ب. التكامل والسلامة: تقدم المواصفة ISO27001 معيار لحماية وكمال المعلومات وطرائق معالجتها، وهذا يضمن الاستمرارية وإعادة العمل في حالة وقوع الكوارث.

ج. التوفر: ويقصد به توفر المعلومات المقيد، إذ أن استخدام ISO27001 لحماية نظام المعلومات يؤكد للمنظمة بأن المستخدمين المخولين هم الوحيدين القادرين للوصول إلى هذه المعلومات وأصولها، وهذا يجعل إدارة حماية المعلومات مهمة سهلة المعالجة.

وتبرز أهمية إدارة أمن المعلومات من خلال قيام أمن المعلومات بتغطية جميع عمليات المعلومات المادية والإلكترونية؛ بحيث تقوم بحماية وسرية وإتاحة ونزاهة المعلومات في جميع مراحل دورة حياة المعلومات واستخدامها داخل المنظمة؛ ويتطلب ذلك استراتيجية أمنية شاملة مرتبطة بشكل مباشر وصريح بعمليات الأعمال واستراتيجية المنظمة، وتحتوي على عناصر وينود شاملة لكل العمليات والسياسات المتعلقة بالنواحي التكنولوجية والمادية في المنظمة.

ثانيا. مدخل إدارة أمن المعلومات لتمييز منظمات الأعمال:

1. معيار إدارة أمن المعلومات ISO27001:

أ. مفهوم معيار ISO27001: نظام إدارة أمن المعلومات (SMSI) هو جهاز يدير وينسق كيفية تنفيذ أمن المعلومات؛ إذ أنه يسمح بوضع إجراءات أمنية تضمن سرية الأصول الحساسة (البيانات الشخصية، الإدارية، الأعمال ...) للمنظمة، وسلامة المعلومات وكذلك توفر هذا النطاق للأشخاص المصرح لهم بالوصول إليه في حقل محدد بدقة.

إن معيار إدارة أمن المعلومات ISO 27001 يقدم نموذجاً مبنياً على منهج مخاطر الأعمال لإنشاء وتنفيذ وتشغيل ومراقبة ومراجعة وصيانة وتحسين أمن المعلومات تحقيقاً لأهداف المنظمة⁷. وهو نظام متقدم لحماية المعلومات؛ يمكن من خلاله تلبية متطلبات المنظمة، ويصلح لكافة المنظمات سواء كانت صناعية أو خدمية، فضلاً عن تطبيق وتشغيل ومراقبة ومراجعة النظام ككل، ويمكن اعتباره مدخلاً للتحسين المستمر لنظام توثيق وإدارة المعلومات.

وقد كان أول إصدار لهذا المعيار من قبل منظمة ISO في سنة 2005، وذلك بهدف تنسيق معايير ISO27001 مع معايير نظم الإدارة الأخرى ISO 9001:2000 الخاصة بإدارة الجودة، و ISO14001:2004 المتعلقة بإدارة البيئة. ولقد تم تعديل هذا المعيار وإصداره في سبتمبر 2013؛ كما أن تطبيق معيار إدارة أمن المعلومات ISO27001 هو خطوة لبناء أمن فعال لإدارة المعلومات، وذلك من خلال الالتزام بتطبيق المتطلبات التالية⁸:

*- تحديد (ISMS) في ضوء المواصفات الخاصة بأنظمة معلومات المنظمة من حيث الحجم، المصادر والأنواع في إطار الاحتياجات التنظيمية والتشريعية للمنظمة؛

*- وضع استراتيجية (ISMS) التي توضح الإجراءات والخطوات اللازمة لتطبيق هذا النظام وهذا يتطلب دعم والتزام كبير من قبل الإدارة العليا في المنظمة؛ * - تحديد المخاطر واكتشافها عن طريق منهجية مناسبة، والتمييز بين المخاطر التي تهدد أمن المعلومات، وفهم وتقييم المخاطر الحالية والمستقبلية من أجل ضمان الاستخدام الفعال للموارد المتاحة؛ * - تقييم خيارات معالجة المخاطر واختيار أهداف الرقابة المناسبة؛ * - الحصول على موافقة الإدارة والبدء في التطبيق.

إن التطبيق الفعال لمعيار ISO27001 يوفر للإدارة وسائل السيطرة على أمن المعلومات بينما يقلل من أخطار العمل الناتجة من عدم الحصول على

المعلومات بالدقة المطلوبة، وخطر تسرب المعلومات⁹. وبغرض إدارة مشاكل أمن المعلومات في المنظمة، يستخدم نظام إدارة أمن المعلومات (ISMS) نموذج (PDCA)* ومداخلات هذا النموذج هو متطلبات وتوقعات أمن المعلومات والنتائج المتوقعة هو أمن المعلومات المدارة (المسيرة)؛ كما هو موضح في الشكل التالي:

الشكل (2): نموذج PDCA (Plan-Do-Check-Act)



المصدر: رؤى يونس، دراسة واقع إدارة أمن نظم المعلومات في المؤسسات الآسيوية،

مجلة جامعة البعث، سوريا، المجلد 39، العدد 31، 2017، ص 72.

في مرحلة الخطة Plan، يتم وضع سياسة وأهداف خاصة بنظام (ISMS) ذات الصلة بإدارة المخاطر وتحسين أمن المعلومات من أجل تحقيق النتائج بما يتفق مع سياسات وأهداف للمنظمة، وفي مرحلة التنفيذ Do يتم تنفيذ سياسة ISMS وضوابطها وإجراءاتها، وفي مرحلة التدقيق Check يتم قياس أداء العملية والأهداف والخبرات العملية وإعداد التقارير عن النتائج. وفي مرحلة التنفيذ Act يتم اتخاذ إجراءات تصحيحية ووقائية بناء على نتائج مراجعة ISMS الداخلية ومراجعة الإدارة أو غيرها من المعلومات ذات الصلة؛ لضمان التحسين المستمر لنظام (ISMS).

ب. أبعاد نظام إدارة أمن المعلومات ISO27001:

تتمثل الأبعاد المكونة لـ (ISMS) في العناصر التالية¹⁰: * - سياسة الأمن: يعمل هذا البعد على توثيق أهداف (ISMS) لمساعدة المنظمة على تقديم الدعم والتوجيه المناسبين. * - تنظيم أمن المعلومات: يمكن المنظمة من السيطرة على كل المعلومات الخاصة بها عن طريق مجموعة من السياسات والجراءات والمهام الأمنية والمسؤوليات. * - إدارة الموجودات (الأصول): الطبيعية والفكرية من خلال تقديم الحماية الملائمة لها؛ بتحديد ملكية ومسؤولية حماية مصادر حماية المعلومات. * - أمن الموارد البشرية: بغرض الحد من المخاطر الناتجة عن الأخطاء البشرية. * - الأمن الطبيعي والبيئي: يساهم في تأمين المناطق المادية (تسهيلات معالجة المعلومات) وبيئة العمل داخل المنظمة في إدارة أمن المعلومات بصورة فعالة. * - إدارة العمليات والاتصالات: وهي مجموعة التسهيلات المتمثلة بالتسليم الآمن، إدارة العمليات اليومية بصورة آمنة، ووسائل تشغيل البيانات والشبكات. * - السيطرة على عمليات دخول العاملين لنظام المعلومات: وبعد بعدا رئيسيا في حماية معلومات المنظمة وحمايتها من الاختراقات الشبكية. * - تطوير أنظمة أمن المعلومات وصيانتها لضمان استمرارية حماية المعلومات. * - الإدارة العرضية: من خلال بناء نظام اتصالات فعال بين المستويات التنظيمية المختلفة لمواجهة الحالات الطارئة وتحديد مواطن الضعف في إدارة أمن المعلومات. * - إدارة استمرارية العمل: يسمح هذا البعد بوجود مرونة مناسبة لمواجهة حالات الكوارث الطبيعية وحالات الفشل والمعوقات غير المتوقعة مما يساعد على استمرارية أنشطة أمن المعلومات. * - الالتزام: يحدد هذا البعد الالتزامات المتعاقد عليها ومتطلبات سياسات الأمن التنظيمية وفعاليات عمليات تدقيق النظام والإجراءات الأمنية.

2. أهمية إدارة أمن المعلومات للمنظمات: يعد ISO27001 من بين أهم المعايير الأمنية لتوفير التوجيه اللازم وضمان وجود مستوى معين من الحماية للمعلومات،

إضافة إلى التأكد من أن كافة العناصر ذات الصلة بالأمن تتم معالجتها ضمن استراتيجية الأمن داخل المنظمة، والتأكد من أن الموارد الالكترونية للمنظمة يتم استخدامها بشكل مسؤول؛ فتطبيق المنظمات لنظام ISO27001 يتيح لها تحقيق مجموعة من المنافع ويمكنها من بلوغ الأهداف الاستراتيجية المرجوة من تطبيقه مما يخدم أهداف المنظمة ككل¹¹؛ كما يعتبر أمن المعلومات إحدى معايير قياس نجاح نظم المعلومات، أي أنه أصبح أحد الركائز المهمة في تقييم جودة نظم المعلومات. وإلى جانب ذلك، يمكن إبراز أهمية أمن المعلومات بالنسبة لتمييز المنظمات اعتمادا على العناصر التالية¹²:

- أ. أمن المعلومات هي جزء أساسي من عمليات الإدارة الناجحة.
 - ب. أمن المعلومات يجب أن تحقق رؤية وأهداف المنظمة.
 - ج. أمن المعلومات يجب أن تنفذ برؤية اقتصادية فعالة.
 - د. نظام أمن المعلومات هو مدخل شامل ومتكامل.
 - هـ. تمتد مسئولية المعنيين بأنظمة المعلومات إلى خارج المنظمة.
 - و. تحقيق أمن المعلومات يتطلب دراسة واعية لإدارة المخاطر.
 - ن. أمن المعلومات يتأثر بالعوامل الاجتماعية.
 - ي. تتطلب برامج أمن نظم المعلومات إعادة تقييم دورية.
- إلى جانب ذلك، فنظام إدارة أمن المعلومات يحقق مجموعة من المزايا للمنظمات المعاصرة، أبرزها¹³:

- المصادقية وزيادة الثقة.
- تحسين الشراكة (العمل مع الشريك).
- زيادة ثقة الزبائن وأصحاب المصلحة.
- التنظيم وحماية الشريك التجاري.

- شهادة تفيد بأن المنظمة مؤهلة ومطبقة لكل القوانين السارية والتعليمات.

- المفاضلة بين المنافسين وكذلك الحصول على تعليمات بكلف منخفضة.

ومن منظور داخلي، فإن إدارة أمن المعلومات تتعكس بشكل إيجابي في عدة مجالات أبرزها ما يلي¹⁴:

- تقدم هيكلية عامة تمكن المنظمة من تطوير وتنفيذ نشاطات إدارة أمن المعلومات بصورة فاعلة.

- تقديم مدخل الخطر المعتمد والذي يعد نشاطا رئيسيا ضمن هيكل تخطيط وتنفيذ نظام إدارة أمن المعلومات وينتج عنه زيادة فعالية المستوى الأمني للمنظمة.

- التأكيد على استخدام المؤهلات والعمليات والإجراءات والتقنيات المناسبة لحماية مصادر المعلومات.

- توفير حماية للمعلومات بكل موثوقية وسلامة وإتاحة.

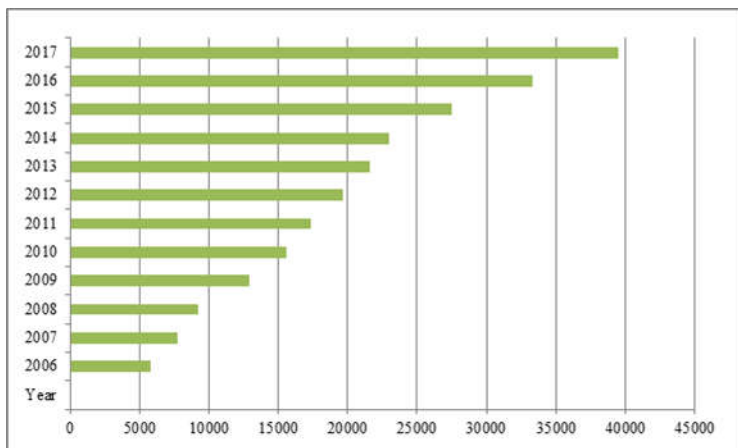
- تعد مكملة لمجموعة المواصفات الدولية المستخدمة في مجال إدارة الأعمال ISO9001، و ISO14001 أو ما يصطلح عليه بنظام الإدارة المدمجة.

ثالثا. تقييم مستوى انتشار معيار إدارة أمن المعلومات ISO27001:

اعتمادا على إحصائيات المنظمة العالمية للتقييس ISO والخاصة بعدد شهادات ISO27001 الممنوحة، وعدد الدول المعتمدة لهذه الشهادات يمكن تقييم مستوى انتشار نظام إدارة أمن المعلومات وفقا لعدة مستويات.

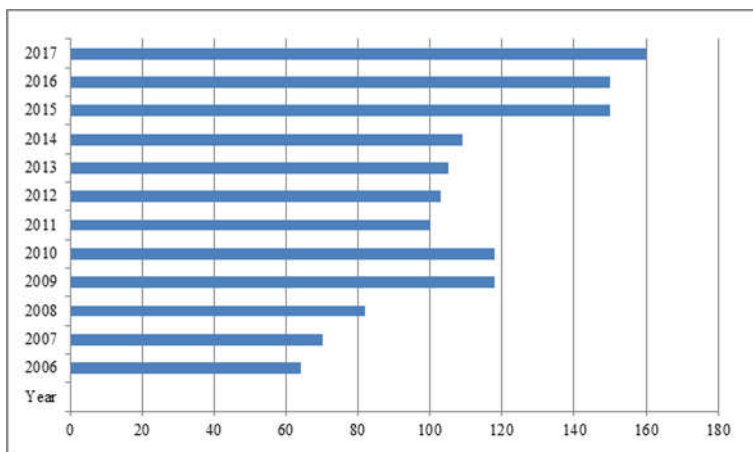
1. على المستوى العالمي: نستعرض تطور عدد الشهادات الممنوحة وعدد الدول المعتمدة لنظام أمن المعلومات ISO27001 على المستوى العالمي من خلال الشكلين التاليين:

الشكل (3): تطور عدد شهادات ISO27001 الممنوحة على المستوى العالمي للفترة (2006 – 2017)



المصدر: من إعداد الباحثين اعتمادا على: www.ISO.org، (2018/12/01).

الشكل (4): تطور عدد الدول المعتمدة لنظام إدارة أمن المعلومات ISO27001 للفترة (2006 – 2017)



المصدر: من إعداد الباحثين اعتمادا على: www.ISO.org، (2018/12/01).

من خلال الشكلين يتضح أن عدد شهادات ISO27001 الممنوحة على

المستوى العالمي في تزايد اعتبارا من سنة 2006، حيث بلغ عددها 5797 شهادة

موزعة على 64 دولة، ثم تطور هذا العدد بنسب متباينة ليصبح 39501 شهادة. وبالمقابل تزايد عدد الدول ليصل إلى 160 دولة في سنة 2017؛ وتجدر الإشارة إلى اختلاف مستوى اعتماد نظام إدارة أمن المعلومات ISO27001 من دولة إلى أخرى، وفي هذا الصدد يوضح الجدول (1) الدول الأكثر اعتمادا لهذا النظام وفقا لإحصائيات سنة 2016.

الجدول (1): الدول العشر الأكثر اعتمادا لنظام إدارة أمن المعلومات ISO27001

المرتبة	عدد الشهادات	الدولة	المرتبة	عدد الشهادات	الدولة
6	1220	إيطاليا	1	8945	اليابان
7	1115	الو م أ	2	3367	المملكة المتحدة
8	1087	تايبيه، الصينية	3	2902	الهند
9	752	اسبانيا	4	2618	الصين
10	670	هولندا	5	1338	ألمانيا

المصدر: من إعداد الباحثين اعتمادا على: www.ISO.org، (2018/12/01).

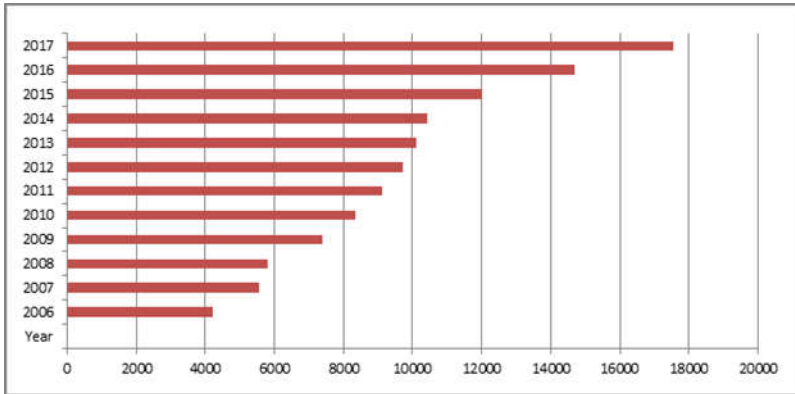
وفقا لهذه المعطيات، فاليابان أكثر الدول اعتمادا لنظام ISO27001، إذ في سنة 2016 بلغ عدد الشهادات الممنوحة لمختلف الشركات اليابانية 8945 شهادة، تتبعها المملكة المتحدة، ثم الهند والصين، وبقية الدول ألمانيا، إيطاليا، الو م أ، ... إلخ. وهي دول صناعية تتميز باقتصاديات قوية مقارنة ببقية دول العالم.

2. شرق آسيا والباسيفيك:

يمكن توضيح مستوى انتشار معيار إدارة أمن المعلومات ISO27001؛

في هذه المنطقة من خلال الشكل التالي:

الشكل (5): تطور عدد شهادات ISO27001 الممنوحة في شرق آسيا
والباسيفيك للفترة (2006 – 2017)



المصدر: من إعداد الباحثين اعتماداً على: www.ISO.org, (2018/12/01).

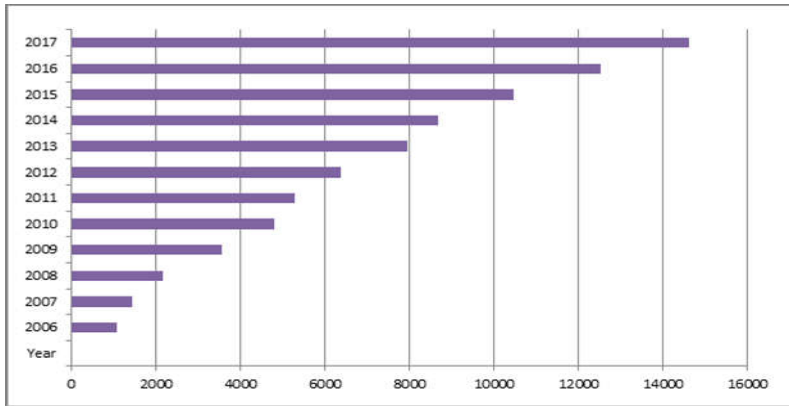
يتضح من الشكل أن عدد الشهادات الممنوحة لدول شرق آسيا والباسيفيك في تزايد مستمر وذلك اعتباراً من سنة 2006 حيث بلغ عددها 4210 شهادة، ليصل إلى 17562 شهادة في سنة 2017. وتعتبر كل من اليابان والصين من أكثر الدول اعتماداً لهذا المعيار بـ 9161 شهادة و5069 شهادة على التوالي خلال سنة 2017.

3. على المستوى الأوروبي:

يمكن توضيح مستوى انتشار معيار إدارة أمن المعلومات ISO27001؛

في هذه المنطقة من خلال الشكل التالي:

الشكل (6): تطور عدد شهادات ISO27001 الممنوحة على المستوى الأوروبي
للفترة (2006 – 2017)



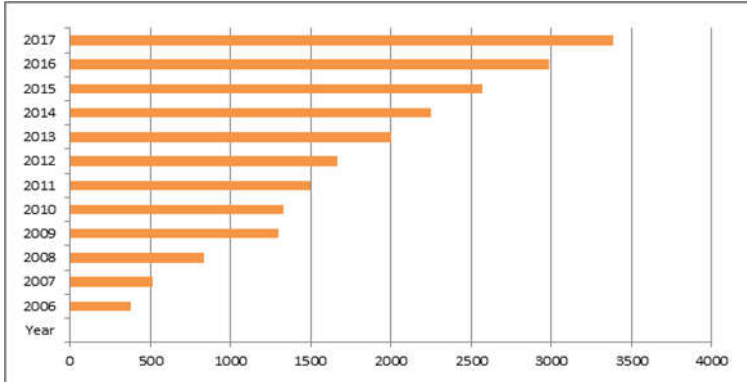
المصدر: من إعداد الباحثين اعتمادا على: www.ISO.org، (2018/12/01).

إن عدد شهادات ISO27001 الممنوحة لدول الاتحاد الأوروبي في تزايد مستمر وينسب متزايدة خلال الفترة المشار إليها، حيث قدر العدد في سنة 2006 بـ 1064 شهادة، وارتفع خلال سنة 2017 إلى 14605 شهادة، ومن جهة أخرى، تعتبر المملكة المتحدة، ألمانيا، إيطاليا، هولندا وإسبانيا من أكثر الدول الأوروبية اعتمادا لنظام ISO27001 .

4. وسط وجنوب آسيا:

يمكن توضيح مستوى انتشار معيار إدارة أمن المعلومات ISO27001؛ في هذه المنطقة من خلال الشكل التالي:

الشكل (7): تطور عدد شهادات ISO27001 الممنوحة في وسط وجنوب آسيا للفترة (2006 - 2017)

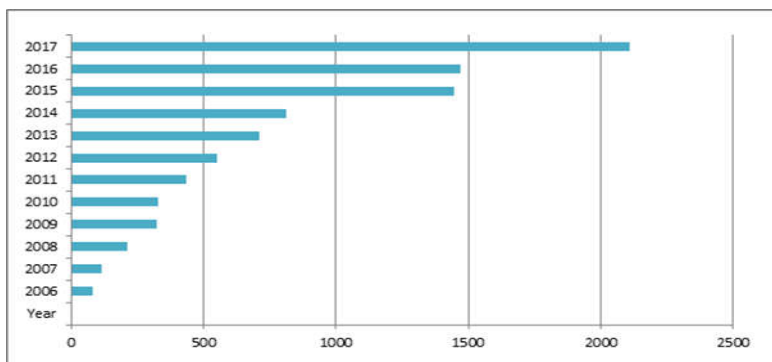


المصدر: من إعداد الباحثين اعتماداً على: www.ISO.org، (2018/12/01).

وفقاً للشكل فقد تطور عدد الشهادات في دول وسط وجنوب آسيا؛ إذ انتقل من 383 شهادة سنة 2006 إلى 3382 شهادة سنة 2017، وتعتبر الهند هي أكثر الدول اعتماداً لمعيار ISO27001 إذ قدر عدد الشهادات الممنوحة لها خلال سنة 2017 بـ 3272؛ أي حوالي 96% من أصل 3382 شهادة لسنة 2017.

5. شمال أمريكا: يمكن توضيح مستوى انتشار معيار إدارة أمن المعلومات ISO27001؛ في هذه المنطقة من خلال الشكل التالي:

الشكل 8: تطور عدد شهادات ISO27001 الممنوحة في شمال أمريكا للفترة (2017 - 2006)



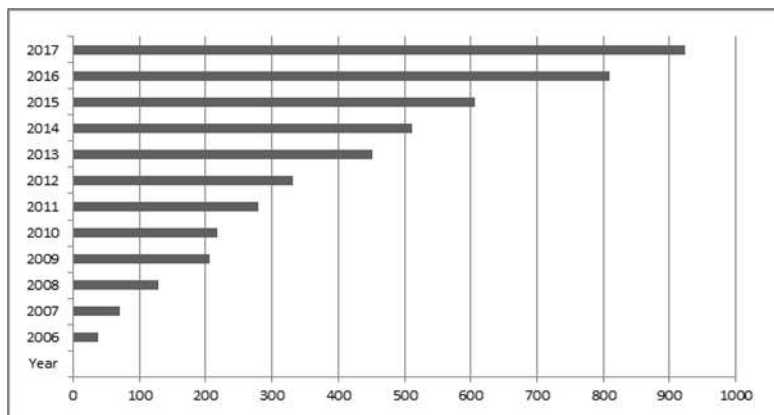
المصدر: من إعداد الباحثين اعتمادا على: www.ISO.org، (2018/12/01).

إن عدد الشهادات في دول شمال أمريكا قد تزايد بنسب متباينة من سنة 2006 إلى سنة 2014، واعتبارا من سنة 2015 ارتفعت نسبة الزيادة في عدد الشهادات إلى غاية سنة 2017. وللاشارة فالو م أ هي أكثر الدول اعتمادا لمعيار ISO27001 حيث قدر عدد الشهادات الممنوحة لها بـ: 1517 شهادة خلال سنة 2017، مقارنة بكندا والمكسيك بـ 276 و 315 شهادة على التوالي لنفس السنة.

6. الشرق الأوسط:

يمكن توضيح مستوى انتشار معيار إدارة أمن المعلومات ISO27001؛ في هذه المنطقة من خلال الشكل التالي:

الشكل (9): تطور عدد شهادات ISO27001 الممنوحة في الشرق الأوسط
للفترة (2006 - 2017)



المصدر: من إعداد الباحثين اعتمادا على: www.ISO.org، (2018/12/01).

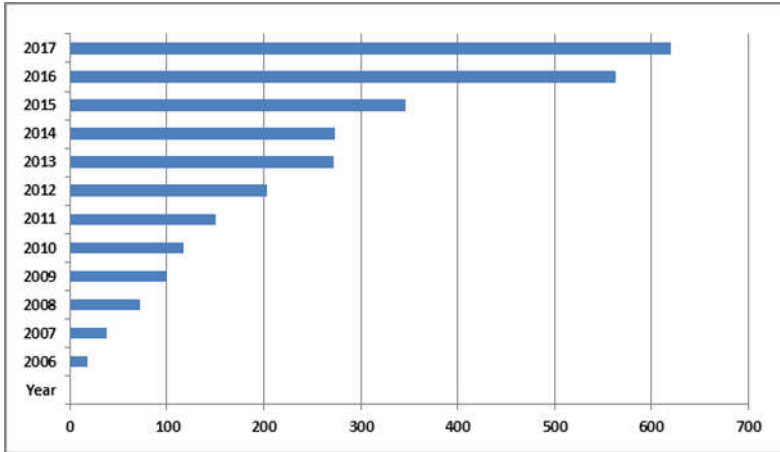
لقد تطور عدد الشهادات في دول الشرق الأوسط بنسب متقاربة اعتبارا من سنة 2006، حيث كان في حدود 37 شهادة، ثم 606 شهادة في سنة 2015، ثم 923 شهادة في سنة 2017. وتعتبر إسرائيل والإمارات العربية المتحدة من أكثر دول الشرق الأوسط اعتمادا لمعيار ISO27001 حسب إحصائيات سنة 2017.

7. جنوب أمريكا:

يمكن توضيح مستوى انتشار معيار إدارة أمن المعلومات ISO27001؛ في

هذه المنطقة من خلال الشكل التالي:

الشكل (10): تطور عدد شهادات ISO27001 الممنوحة في جنوب أمريكا للفترة
(2017 - 2006)



المصدر: من إعداد الباحثين اعتماداً على: www.ISO.org، (2018/12/01).

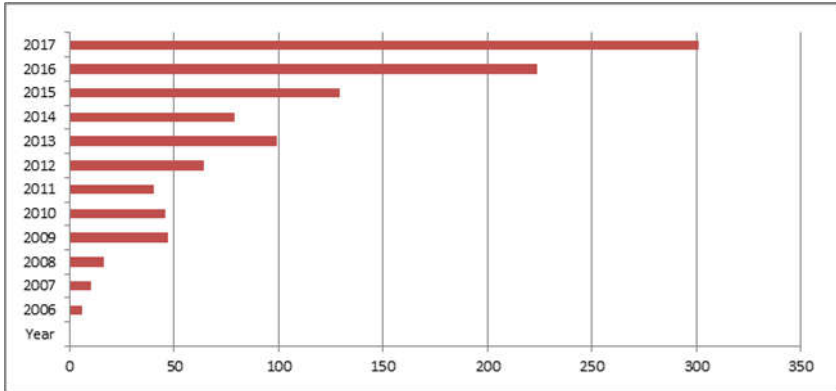
يتضح من الشكل أن هناك تطور ملحوظ لعدد الشهادات في دول جنوب أمريكا؛ حيث انتقل هذا العدد من 18 شهادة سنة 2006 إلى 620 شهادة سنة 2017، ومن جانب آخر تعتبر البرازيل وكولومبيا من أكثر دول المنطقة اعتماداً لمعيار ISO27001 بـ 170 و 148 شهادة على التوالي وفقاً لإحصائيات سنة 2017.

8. على المستوى الإفريقي:

يمكن توضيح مستوى انتشار معيار إدارة أمن المعلومات ISO27001؛ في

هذه المنطقة من خلال الشكل التالي:

الشكل (11): تطور عدد شهادات ISO27001 الممنوحة على المستوى الإفريقي للفترة (2006 - 2017)



المصدر: من إعداد الباحثين اعتمادا على: www.ISO.org، (2018/12/01).

إن عدد الشهادات في الدول الإفريقية يتزايد بنسب متباينة؛ فمن 6 شهادات سنة 2006، إلى 99 شهادة سنة 2013، ثم انخفض إلى 79 شهادة سنة 2014 ليصل إلى 301 شهادة سنة 2017. كما أن أبرز الدول المعتمدة لمعيار ISO27001 هي جنوب إفريقيا بـ 69 شهادة، نيجيريا بـ 54 شهادة، المغرب بـ 30 شهادة، مصر بـ 25 شهادة. وتجدر الإشارة إلى محدودية اعتماد معيار ISO27001 في الجزائر بالمقارنة مع تطور اعتماد هذا المعيار في مختلف الدول الإفريقية خلال الفترة 2006-2017 كما هو مبين في الجدول التالي:

الجدول (2): تطور عدد الدول الإفريقية المعتمدة لمعيار إدارة أمن المعلومات
ISO27001 للفترة (2006-2017)

السنة	الدول الإفريقية	الجزائر	السنة	الدول الإفريقية	الجزائر
2006	06	/ /	2012	64	1
2007	10	/ /	2013	99	7
2008	16	/ /	2014	79	0
2009	47	/ /	2015	129	0
2010	46	/ /	2016	224	4
2011	40	1	2017	301	5

المصدر: من إعداد الباحثين اعتمادا على: www.ISO.org, (2018/12/01).

من خلال الجدول، نلاحظ ما يلي:

- محدودية انتشار معيار ISO27001 في بيئة الأعمال الجزائرية.
- تأخر اعتماد هذا المعيار في الجزائر إلى غاية 2011، بالمقارنة مع بداية تطبيقه في الدول الإفريقية ومختلف دول العالم المشار إليها سابقا بداية من سنة 2006.
- نسبة تقدم ضعيفة جدا في اعتماد هذا المعيار خاصة سنتي 2014 و2015؛ أي الفترة التي تلت الإصدار الثاني للمعيار ابتداء من سنة 2013.

وفي سياق متصل فإن مستوى اعتماد معيار ISO27001 بالنسبة للدول العربية ضعيف جدا، وهذا يفسر وفقا لعدة جوانب، منها ضعف اعتماد نظام الحوكمة على مستوى هذه الدول وفقا لمؤشرات البنك العالمي¹⁵، كما يشير تقرير البنك الدولي الموسوم بالحوكمة الجيدة لأجل التنمية في الشرق الأوسط وشمال إفريقيا أن التنمية في هذه الدول يعيقها ضعف إدارة الحكم العام والتي تتأخر فيها دول المنطقة عن بقية دول العالم¹⁶.

الخاتمة:

لقد تبين من خلال استعراض مختلف الجوانب المرتبطة بموضوع الدراسة أهمية إدارة أمن المعلومات في منظمات الأعمال المعاصرة خاصة في ظل تزايد التحديات التكنولوجية وما تفرضه من تهديدات لسلامة تواجد هذه المنظمات، كما أنها تمثل جانبا رئيسيا في تفعيل نظام الحوكمة في شتى مجالاتها وهو ما يعزز موقعها التنافسي في السوق ويمكنها من تحقيق التميز في مجال الأعمال.

والى جانب ذلك، فقد أبرزت هذه الدراسة أهمية اعتماد ISO27001 لإدارة أمن وتكنولوجيا المعلومات في المنظمات الساعية للاندماج في الاقتصاد المعرفي. واستنادا إلى المعطيات الإحصائية التي تمت من خلالها دراسة مستوى انتشار اعتماد معيار ISO27001 على مستوى مختلف الدول والأقاليم يمكن استخلاص مجموعة من الاستنتاجات؛ أبرزها ما يلي:

- اتضح مدى الاختلاف في التوجه نحو اعتماد هذا المعيار بين مختلف الأقاليم والدول، ففي الاقتصاديات المبنية على المعرفة يوجد تسارع المنظمات بشكل متزايد نحو تبني نظام إدارة أمن المعلومات، على عكس الاقتصاديات النامية وحديثة العهد بالتكنولوجيا فبيئة الأعمال الخاصة بها تميزت بمحدودة اعتمادها على معيار ISO27001.

- وجود تفاوت كبير في اعتماد معيار ISO27001 في مختلف المناطق على المستوى العالمي؛ حيث أن شرق آسيا والباسيفيك، والاتحاد الأوروبي هي الأكثر اعتمادا لهذا المعيار مقارنة ببقية المناطق.

- تعتبر منطقة الشرق الأوسط، جنوب أمريكا وإفريقيا ضعيفة التوجه نحو اعتماد معيار إدارة أمن المعلومات ISO27001.

- يرتبط اعتماد معيار ISO27001 بمستوى التقدم الاقتصادي والتطور التكنولوجي للدول؛ إذ نجد أن اليابان، الصين، المملكة المتحدة، ألمانيا، إيطاليا، هولندا، إسبانيا،

الهند، الو م أ هي الدول الأكثر توجها لاعتماد معيار إدارة أمن المعلومات، ويمكن تفسير ذلك باعتبارها دول رائدة في مجال إرساء قواعد الحوكمة وتطبيقها في بيئة الأعمال.

الهوامش والمراجع:

¹ Michael E. Whitman, Herbert J. Mattord, (2017), Principles of Information Security, 6th Edition, USA.

² ذيب بن عايض القحطاني (2015)، أمن المعلومات، مكتبة الملك فهد للنشر، ص 58.

³ Kazemi Mehdi, Khajouei Hamid and Nasrabadi Hashem, (2012), Evaluation of Information Security Management System Success Factors: Case study of Municipal Organizations, African Journal of Business Management, Vol 6 (14), p 498.

⁴ رؤى يونس، دراسة واقع إدارة أمن نظم المعلومات في المؤسسات السورية، مجلة جامعة البعث، سوريا، المجلد 39، العدد 31، 2017، ص 70.

⁵ علي عبد الستار عبد الجبار الحافظ، أحمد هاني محمد النعيمي، دور ISO 27001:2005 في تعزيز مفهوم إدارة دورة حياة المعلومات، متوفر على مستوى الموقع: <https://www.kantakji.com>، (تم الاطلاع في: 2019/02/10).

⁶ نفس المرجع السابق.

⁷ رؤى يونس، مرجع سابق، ص 72.

⁸ يوسف حجيم الطائي، محمد عاصي العجيلي، ليث عبد الحكيم (2009)، نظم إدارة الجودة في المنظمات الإنتاجية والخدمية، دار اليازوري للنشر والتوزيع، الأردن، ص 422.

⁹ M. Tolga et al, GOVERNING INFORMATION SECURITY IN CONJUNCTION WITH COBIT AND ISO 27001, <https://arxiv.org/ftp/arxiv/papers/1108/1108.2150.pdf>, (22/01/2019).

* PDCA: Plan; Do; Check; Act.

¹⁰ يوسف حجيم الطائي، محمد عاصي العجيلي وليث عبد الحكيم، (2009)، مرجع سابق، ص 423.

- ¹¹ على محمود مصطفى خليل، منى مغربى محمد إبراهيم، الدور التأثيرى لحوكمة أمن المعلومات في الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية دراسة ميدانية، متوفر على مستوى الموقع: <http://www.bu.edu.eg>، (تم الاطلاع في: 2019/01/22).
- ¹² أيمن محمد فارس الدنف، (2013)، واقع إدارة نظم أمن المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها، مذكرة ماجستير، الجامعة الإسلامية، فلسطين، ص 47.
- ¹³ علي عبد الستار عبد الجبار الحافظ، أحمد هاني محمد النعيمي، مرجع سابق.
- ¹⁴ يوسف حجيم الطائي، محمد عاصي العجيلي، ليث عبد الحكيم، (2009)، مرجع سابق، ص 426.
- ¹⁵ علي بن يحيى عبد القادر، قديد عبد القادر، تأثير طبيعة نظام الحوكمة على الأداء التنموي للأقطار العربية، مجلة الاقتصاد والمالية، العدد 1، 2015، ص 07.
- ¹⁶ جنوحات فضيلة، قطوش بشرى، دور تطبيق الحوكمة ومكافحة الفساد في تحقيق التنمية المستدامة في الدول العربية، مجلة البحوث الاقتصادية والمالية، المجلد 5، العدد 1، 2018، ص 91.