دور المواصفة الدولية ISO/IEC 27001 في الرفع من مصداقية نظام إدارة أمن المعلومات في المؤسسة.

The role of ISO/IEC 27001 in raising the credibility of the ISMS in the organization

فيلالي أسماء، جامعة أبو بكر بلقايد بتلمسان (الجزائر)، asma.filali@univ-tlemcen.dz

تاريخ الاستلام: 2020/12/06 تاريخ القبول: 2021/03/16 تاريخ النشر: 2021/03/27

ملخص:

يعتبر أمن المعلومات من أهم المواضيع التي تهتم بها المؤسسات، إذ أصبح يوجد بها وخصوصا الكبيرة منها نظام لإدارة أمن المعلومات، ولتفادي التطبيق العشوائي ظهرت الحاجة إلى مجموعة من المعايير من أجل اقتباس أفضل التطبيقات والممارسات، ومعرفة الطريق الصحيح في التطبيق الجيد، وأفضل معيار يمكن اعتماده في مجال أمن المعلومات هو المواصفة الدولية ISO/IE27001. وعليه تهدف هذه الدراسة لعرض كيفية مساهمة المواصفة الدولية ISO/IEC27001 في إرساء قواعد نظام إدارة أمن المعلومات داخل المؤسسة على فرض أن المواصفة ترفع من مصداقية النظام، وتوصلت الدراسة إلى أن تطبيق معيار الإيزو 27001 أمر ضروري لكل مؤسسة حتى لو لم تتحصل على الشهادة، إذ أن هذه المواصفة ترفع من فعالية ومصداقية نظام إدارة أمن المعلومات.

كلمات مفتاحية: إيزو/ أي إي سي 27001؛ نظام إدارة أمن المعلومات؛ تحسين مستمر؛ نموذج (خ.ن.إ.ص)؛ إيزو.

تصنيفات JEL : M15, L86, L15

Abstract:

Information security is one of the most important topics that organizations care about, as it has-especially the large ones- a system for managing information security. and to avoid random application, the need for references appeared to cite the best applications and practices, and the best reference that can be adopted in the field of information security is the

ISO/IE 27001 standard. Therefore, this study aims to show how the international standard ISO/IEC 27001 contributes to establishing the rules of ISMS within the organization. The study concluded that applying the ISO 27001 standard is necessary for every organization, as the standard improves the effectiveness and credibility of the ISMS.

Keywords: ISO/IEC 2700; ISMS; Continuous Improvement; PDCA Form; ISO.

Jel Classification Codes: M15,L86, L15

1. مقدمة:

أمن المعلومات مفهوم دائم التجدد والتطور، وذلك حسب تطور التهديدات المعلوماتية التي تتغير وتتعقد بشكل مستمر، فهو مفهوم شامل وعام هدفه حماية المعلومة بكل أشكالها، سواء في شكلها المعلوماتي أو الورقي أو الشفهي أو غيرها، وعملية تطبيقه ليست بالأمر البسيط، بل تحتاج إلى تخطيط وتجنيد للموارد المادية والبشرية، ودراسة لمحيط المؤسسة وتحديد النطاق الذي تسعى لحمايته، ودراسة كل التهديدات المحيطة والممكنة والتخطيط لطرق التعامل معها ومعالجتها، ولتجنب التطبيق العشوائي لأمن المعلومات ظهرت اليوم معايير خاصة بذلك وأشهرها معيارISO/IEC 27001 الخاص بنظام إدراة أمن المعلومات الذي يبيّن الإطار العام لتطبيق الأمن داخل المؤسسة، وعليه أصبحت هذه الأخيرة تعتبره مرجعا مهمًّا لاقتباس أفضل التطبيقات والممارسات، ومعرفة الطريق الصحيح في التطبيق الجيّد، فالمؤسسة حتى لو لم تتحصل على الشهادة أو المصادقة من طرف المعيار إلا أنها يمكن أن تتبنى العديد من التطبيقات الموجودة فيه، وكغيره من معايير الإيزو الأخرى فإن هذا المعيار بدوره يمكن تطبيقه في إطار دورة ديمنغ أو ما يسمى بدورة PDCA (**خ**(خطط).**ن**(نفذ).إ(إفحص).**ص**(صحح)) للتحسين المستمر.

إشكالية الدراسة:

نظرا لتزايد أهمية المعلومات والأنظمة المعلوماتية بسبب الاعتماد الكلي اليوم على الرقميات، أصبح لزاما على المؤسسات والهيئات الدولية تقنين تداول المعلومات والتعامل مع الأنظمة الخاصة بها، فأصدرت المنظمة العالمية للتقييس"الإيزو" (ISO) مواصفة قياسية تحت اسم ISO/IEC27001:نظام إدارة أمن المعلومات، ولمعرفة أكثر عن الموضوع والتطرق لكل جوانبه تم طرح الاشكالية التالية:

كيف تساهم المواصفة القياسية الدولية ISO/IEC 27001 في إرساء قواعد نظام إدارة أمن المعلومات في المؤسسة والرفع من مصداقيته ؟

للإجابة على الاشكالية المطروحة يجب أوّلا الإجابة على مجموعة الأسئلة التالية:

- ما هي المواصفة القياسية ISO/IEC 27001 ؟ وما هي المعايير المتعلقة بها ؟

- ما هو نظام إدارة أمن المعلومات وما علاقته بالمواصفة القياسية ISO/IEC 27001 ؟

- كيف تساهم مواصفة ISO/IEC 27001 في الرفع من مصداقية نظام إدارة أمن المعلومات ؟

- ما المقصود بدورة PDCA ؟ وكيف يمكن تطبيق نظام إدارة أمن المعلومات من خلالها ؟

فرضيات البحث: للإجابة على الإشكالية والأسئلة المطروحة تم الانطلاق من الفرضيتين التاليتين:

- المواصفة القياسية ISO/IEC 27001 ترفع من مصداقية نظام إدارة أمن المعلومات في المؤسسة.

- تطبيق دورة PDCA يساهم في تحسين مستوى نظام إدارة أمن المعلومات في المؤسسة.

أهمية البحث: تكمن أهمية هذا البحث في كونه يتطرق لموضوع حديث نوعا ما خصوصا على مستوى المؤسسات العربية،، فالجميع يعرف مواصفة إيزو 9000 الخاصة بنظام إدارة الجودة، أما مواصفة الإيزو 27001 لنظام إدارة أمن المعلومات فلا تزال موضوع حديث الطرح نظرا لحساسية الأنظمة المعلوماتية والسياسات الأمنية في المؤسسات.

أهداف البحث: يهدف هذا البحث إلى تحقيق النقاط التالية:

- تعريف نظام إدارة أمن المعلومات والمواصفة القياسية ISO/IEC 27001 .

- تبيان دور مواصفة ISO/IEC 27001 في الرفع من مصداقية نظام إدارة أمن المعلومات.

- شرح طريقة تطبيق دورة التحسين المستمر على أنظمة إدارة أمن المعلومات.

منهجية البحث: تم الاعتماد في هذا البحث على المنهج الوصفي للتعريف بالمواصفة القياسية ISO/IEC 27001 وتوضيح عناصر أنظمة الادارة بصفة عامة ونظام ادارة أمن المعلومات بصفة خاصة، والمنهج التحليلي لتحليل العلاقة بين هذا الأخير وبين معيار الإيزو27001، وتوضيح مدى القدرة على تطبيق دورة التحسين المستمر الخاصة بإدارة الجودة الشاملة على إدارة امن المعلومات.

خطة البحث: تم تناول الموضوع من خلال ثلاث محاور رئيسية:

1. ماهية المواصفة القياسية ISO/IEC 27001.
2. نظام إدارة أمن المعلومات وعلاقته بالمواصفة القياسية ISO/IEC 27001.
3. تطبيق نظام إدارة أمن المعلومات حسب نموذج PDCA.

2. ماهية المواصفة القياسية الدولية ISO/IEC 27001

المنظمة العالمية للتقييس"الإيزو" (ISO) هي منظمة عالمية ظهرت سنة 1947 متكونة من ممثلي منظمات قياس وطنية في حوالي 150 بلد، وإضافة إلى معايير"إيزو" المعروفة عالميا، هناك معايير أخرى وطنية وعالمية ويكون ممثليها عموما أعضاء الإيزو مثل: CEN(اللجنة الأوروبية للقياس)، BSI(المنظمة البريطانية للقياس)، ANSI(المعهد الوطني الأمريكي للقياس)، AFNOR(الجمعية الفرنسية للقياس)، ولكن تبقى المعايير المرجعية لأمن نظم المعلومات هي بالتأكيد الخاصة بالإيزو 27000. (Del Duca & Planche, 2012, p. 110)

تمت كتابة ISO/IEC 27001 من قبل مجموعة عمل في لجنة مشتركة من ISO(المنظمة الدولية للتوحيد القياسي) هي المسؤولة عن التقييس في جميع المجالات وIEC(اللجنة الكهروتقنية الدولية)، ويتم إدارة ISO/IEC 27001 من قبل هاتين الهيئتين الدوليتين، لهذا السبب من المهم عدم كتابة ISO 27001 فقط.(Gallotti, 2019, p. 232) ويعتبر هذا المعيار الأول من سلسلة معايير أمان المعلومات الدولية والتي تحتوي كلها على أرقام ISO 2700X.

1.2 تاريخ المواصفة القياسية الدولية ISO/IEC 27001

مر معيار الإيزو27001 بالعديد من المراحل، إلى أن وصل إلى الشكل الذي هو عليه الآن:

- **1995**: في مارس 1995 تم اطلاق معيار BS7799-1 من طرف BSI منظمة القياس البريطانية، وهو عبارة عن وثيقة لأحسن التطبيقات التي تغطي الجوانب التنظيمية، الاجتماعية، القانونية، والمعايير الممكن اتخاذها في مجال أمن المعلومة، مواضيع لا يتم معالجتها في المعايير التي تهتم بالجوانب التقنية مثل ايزو 15408 (Linlaud, 2003, p. 7.8)

- **1998**: منظمة القياس البريطانية BSI أضافت جزءًا ثانيا لهذا المعيار وسمته $BS7799^{-2}$، "$^{-2}$" لا يعني هنا الطبعة 2 ولكن الجزء2، هذه الإضافة تبين المتطلبات التي تحتاجها المنظمة لوضع نظام إدارة أمن المعلومات.(Fernandez-Toro, 2016, p. 15)
- **2000**: في ديسمبر 2000 تم تبني المعيار $BS7799^{-1}$ رسميا من طرف الإيزو واللجنة الكهروتقنية الدولية IEC تحت مرجع ISO/IEC1779 :2000 (Linlaud, 2003, p. 7) ، مع اثرائها ببعض المعايير الأمنية الإضافية حيث أن ISO17799 هو مرجع لا يعالج أكثر من مسألة نظام إدارة أمن المعلومات.(Fernandez-Toro, 2016, p. 15)
- **2002**: بالتوازي مع أعمال الإيزو، BSI تابعت عملها على $BS7799^{-2}$ ونشرت طبعة ثانية وهي $BS7799^{-2}$:2002.(Fernandez-Toro, 2016, p. 15)
- **2005**: في جوان 2005 أخرجت طبعة جديدة تحت مرجع ISO/IEC17799 :2005 (Calder, 2013, p. 17)، وفي أكتوبر 2005 الإيزو يتبنى أخيرا $BS7799^{-2}$ تحت مرجع ISO/IEC 27001:2005، الإيزو 27001 يحدد إذا المتطلبات التي يجب أن تجيب المنظمة من أجل وضع نظام إدارة أمن المعلومات.(Fernandez-Toro, 2016, p. 15)
- **2007**: الإيزو يعيد تسمية ISO17799 إلى ISO/IEC 27002. (Fernandez-Toro, 2016, p. 15)
- **2013**: امتدادا لاتساع التشاورات بين أعضاء منظمة ISO/IEC. الطبعة الأخيرة ل ISO/IEC 27001 تمت في أكتوبر 2013.(Calder, 2013, p. 25)

إذا من خلال تاريخ هذه المعايير نستنتج أنه يوجد اليوم معيارين :

- **ISO/IEC 27001**:التي تحدد متطلبات من أجل نظام إدارة أمن المعلومات.
- **ISO/IEC 27002**:التي تستقبل التطبيقات الجيدة في مادة أمن المعلومات.

2.2 التوافق بين ISO/IEC 27001 وISO/IEC 27002

يجب أن تكون العلاقة بين ISO/IEC 27001 وISO/IEC 27002 واضحة للغاية، فISO/IEC 27001 يعتمد إلى حد كبير على الاستخدامات التي تفرضها ISO/IEC 27002،

حيث تم إنشاء الارتباط بين المعيارين عام 1999 عندما تم نشر BS7799 لأول مرة كمعيار من جزأين، الجزء الأول كان مدونة ممارسات والجزء الثاني عبارة عن مواصفة لنظام إدارة أمن المعلومات الذي نشر عناصر التحكم المحددة من مدونة الممارسات، وتستمر هذه العلاقة اليوم بين مواصفات نظام إدارة أمن المعلومات الواردة في جزء واحد من المعيار الموحّد، والإرشادات التفصيلية حول ضوابط أمن المعلومات التي يجب أخذها في الاعتبار عند تطوير وتنفيذ نظام إدارة أمن المعلومات والواردة في الجزء الآخر من المعيار المشترك. (Vasudevan, 2015, p. 17)

ISO/IEC 27002 أيضا يزود إدارة التجهيزات الأساسية بكيف أن الفرد المسيطر يجب أن يكون قريبا. أي شخص ينفذ أو يحقق نظام إدارة أمن المعلومات ISO/IEC27001 يحتاج أن يحصل ويدرس نسخة كلا من ISO/IEC27001 وISO/IEC27002، في حين أن ISO/IEC 27001 في الواقع يأمر باستخدام ISO/IEC27002 كمصدر للتوجيهات بشأن الضوابط واختيار السيطرة وتطبيقات التحكم، فإنه لا يحد من اختيار المنظمة للضوابط، وتنص المواصفات على: "أهداف الرقابة والضوابط الواردة في المرفق A ليست شاملة، وأهداف الرقابة والضوابط الإضافية يمكن الإحتياج إليها".

كلا المعيارين يعترفان أن أمن المعلومات لا يمكن أن يتحقق من خلال الوسائل التكنولوجية فقط، كما أنه يجب أن لا يتم التنفيذ بالطريقة الخاطئة، والتي قد تؤدي بالمؤسسة للخطر أو تخلق صعوبات لعملياتها التجارية.(Calder, 2013, pp. 17-18)

3.2 أصناف ISO/IEC 27000: نستطيع تقسيم أصناف الإيزو27000 إلى 3 أنواع: (**Bellefin**, **2008**, **p**. **4**)

- **معايير التصديق:** تصف المعايير التي يجب الالتزام بها من أجل الحصول على الشهادة مثل: ISO/IEC 27001 (معيار تعريف وضع نظام إدارة أمن المعلومات) وISO/IEC 27006 (تعرف المتطلبات الواجب تطبيقها للمنظمات المعتمدة من أجل تطبيق الشهادة بأنفسهم)

- **معايير التوصية:** هذه المعايير تقترح الممارسات الجيدة الواجب اتباعها من أجل تعريف نظام الإدارة وتحديد معايير الحماية مثل: ISO/IEC 27002 , ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005.
- **المعايير القطاعية والتقنية:** الإيزو يحضّر أيضا "أنظمة إدارة أمن المعلومات قطاعية" مثل ISO/IEC 27011 (الاتصالات)، و ISO/IEC 27799 (الصحة).

وسنقوم بتعريف كل معيار على حِدا مع التركيز على ISO/IEC27001 و ISO/IEC 27002.

- **معيار ISO/IEC 27001:نظام إدارة أمن المعلومات**

ISO/IEC 27001 هو معيار مصادقة نظام إدارة أمن المعلومات، هدفه السماح بتصور تخطيط وتفعيل نظام التحسين المستمر لتنظيم أمن المعلومات على مستوى المؤسسة وهناك طبعتين :

- **ISO/IEC 27001:2005**: ينتمي إلى عائلة المعايير المتعلقة بأنظمة إدارة الأمن المعلوماتي والتي هي موجهة إلى كل المنظمات والمؤسسات باختلاف حجمها وقطاع أعمالها، وهو معيار مرن في الإجابة على احتياجات المؤسسات الصغيرة والمتوسطة والكبيرة، كما أنه قابل للتطبيق على كل القطاعات الاقتصادية، المنظمات العمومية، والمعاهد الجامعية.
- **ISO/IEC 27001:2013**:العنوان الرسمي لهذا المعيار هو: تكنولوجيا المعلومات –التقنيات الأمنية –نظام إدارة أمن المعلومات–المتطلبات، منذ أكتوبر2013 جاء محل الطبعة القديمة ISO/IEC 27001:2005.

ويعتبر هذا الإصدار الدولي من أحدث المواصفات القياسية لنظام إدارة أمن المعلومات، وهو محايد ومستقل عن التكنولوجيا، فهو نظام إداري وليس مواصفة تقنية وهذا يظهر من خلال عنوانه، وهو مصمم للاستخدام في المؤسسات من جميع الأحجام وفي كل القطاعات وفي أي مكان في العالم. (Vasudevan, 2015, p. 13)

هذا المعيار عبارة عن 30 صفحة طويلة، ويرد جوهر هذا المعيار في الصفحات التسع التي تحدد مواصفات تصميم وتنفيذ إدارة أمن المعلومات، وأيضا في الصفحات B من الملحق A والتي تحوي 114 عناصر فردية تحت المعيار، والتي يجب أخذها بعين الاعتبار عند التطبيق.(Calder, 2013, p. 25)

- **ISO/IEC 27001:2017**: تم اعتماده سنة 2017 من قبل هيئة القياس الأروبية (EN) التي قامت بنشره، معيار 2013 ومعيار2017 نفس الشيء غير أن الغلاف مختلف، وعليه يمكن شراء ISO/IEC27001 :2013 من موقع ISO، ويمكن شراء ISO/IEC 27001:2017 من موقع EN. (Gallotti, 2019, p. 231)

●**معيار ISO/IEC 27002**:هناك طبعتين :

- **ISO/IEC 27002:2005**: عبارة عن وثائق للتطبيقات الجيدة لإدارة أمن المعلومات، هو معيار توصيات محتواه مطابق تماما لإيزو 17799 ويغطي 11 فئة.

- **ISO/IEC 27002 :2013**: العنوان الرسمي لهذا المعيار هو تكنولوجيا المعلومات – التقنيات الأمنية – مدوّنة قواعد الممارسة لإدارة أمن المعلومات، نشر في أكتوبر 2013، حل محلّ الطبعة القديمة ISO/CEI 27002 :2005، هو مدونة قواعد الممارسة وليس مواصفة، يستعمل كلمات مثل "يجب"، "قد"، يمكن اعتباره نقطة انطلاق لتطوير مبادئ توجيهية محددة ومنظمة، وهو أطول مرتين من ISO/IEC 27001، حوالي 90 صفحة، 8 منها مواد تمهيدية، 78 صفحة تتعامل بالتفصيل مع الضوابط الأمنية.(Calder, 2013, p. 27)

●**معيار ISO/IEC 27003**: يقدم نهج عملي من أجل النجاح في عملية وضع نظام إدارة أمن المعلومات مطابقة لإيزو27001، يصف عملية إدارة أمن نظم المعلومات ومواصفات التصميم منذ البداية إلى غاية إنتاج مخططات تنفيذ المشروع، مغطيا التحضير والتخطيط للأنشطة التي تسبق التنفيذ الفعلي. (Calder, 2009, p. 29)

●**معيار ISO/IEC 27004**: هذا المعيار العالمي يقدم نصائح حول تطوير واستعمال المعايير من أجل تقييم فعالية نظام إدارة أمن المعلومات الموضوع كما هو مقرر في معيار ايزو27001. (Librairietechnique, 2016)

●**معيار ISO/IEC 27005**:عملية تسيير المخاطر المتعلقة بأمن المعلومة ، يقترح منهجية تقييم ومعالجة المخاطر(Berteau et al, 2013, p. 10) .

- **معيار ISO/IEC 27006**::دليل يشرح المتطلبات الأساسية ويوفر الإرشادات لهيئات التدقيق وإصدار الشهادات الخاصة بنظام إدارة أمن المعلومات.(Carpentier, 2012, p. 33)
- **معيار ISO/IEC 27007**:دليل لفحص أنظمة إدارة أمن المعلومات.
- **معيار ISO/IEC 27008**: هذا المعيار يقترح دليل حول ضوابط أمن مراجعة المعلومة.

هذه هي معايير الإيزو الخاصة بأمن المعلومات عموما، وهناك معايير أمنية خاصة بقطاعات معينة مثل:(Carpentier, 2012, p. 34)

- **ISO/IEC 27010**: متعدد الأجزاء، يقترح دليل حول إدارة أمن المعلومة لقطاع الاتصالات.
- **ISO/IEC 27011**: دليل لتسيير أمن المعلومات في قطاع الاتصال عن بعد(معروفة أيضا ب(ITUX.1051).
- **ISO/IEC 27013**:نظام إدارة أمن المعلومات لقطاع الصناعة.
- **ISO/IEC 27014**: هذا المعيار يغطي حوكمة أمن المعلومة.
- **ISO/IEC 27015**: سيكون دليل نظام إدارة أمن المعلومات للخدمات المالية في المنظمات .
- **ISO/IEC 27031**: هذا المعيار يرتكز على استمرارية النشاط في أنظمة المعلومات.
- **ISO/IEC 27032**: هذا المعيار يقترح دليل حول أمن الانترنت.

إضافة إلى: (Gallotti, 2019, PP 228.229)

- **ISO/IEC 27017**: لمقدمي ومستخدمي الخدمات السحابية.
- **ISO/IEC 27018**: موجه لمقدمي الخدمات السحابية، و مخصص لحماية البيانات الشخصية.
- **ISO/IEC 27019**: لصناعة مرافق الطاقة.
- **ISO/IEC 27799**: لقطاع الصحة.
- **ISO/IEC 29151**: لوحدة التحكم في البيانات الشخصية.

3. نظام إدارة أمن المعلومات وعلاقته بالمواصفة القياسية ISO/IEC 27001

نظام إدارة أمن المعلومات هو نظام ككل الأنظمة الموجودة في المؤسسة، وأصبح اليوم متعلقا بمعيار ISO/IEC 27001، تماما كعلاقة نظام إدارة الجودة الشاملة بمعيار ISO9001.

1.3 تعريف نظام إدارة أمن المعلومات:

أنظمة إدارة أمن المعلومات هي قبل كل شيء أنظمة إدارة، بمعنى أنها تطبق على الأمن المعلوماتي الوصفات المجرّبة من قبل على ميادين أخرى خاصة الجودة.

معيار إيزو 9001 في الركن المعنون ب"نظام الإدارة "يعرّف نظام الإدارة على أنه نظام يسمح ب:

- وضع سياسة، – وضع أهداف، – تحقيق هذه الأهداف.

وعليه فإن نظام الإدارة هو مجموعة معايير تنظيمية وتقنية تهدف لتحقيق هدف، وبمجرد تحقيقه تسعى لتجاوزه.(Fernandez-Toro, 2016, p. 6)

نظام الإدارة أيضا يرتكز على مرجع مكتوب، والذي يخضع للفحص بوسيلة تدقيق التي تعمل على مقارنة المرجع مع الواقع من أجل استخراج الاختلافات المسماة بالفجوات أو عدم التطابق، وبدون مرجع المدقق سيكون له عدة صعوبات في اتمام مهمته.(Bloch & Wolfhugel, 2011, p. 22)

أما بالنسبة لأمن المعلومات فنحن لا نتكلم فقط عن الأمن المعلوماتي، بل يهمنا الكلام عن المعلومة في كل أشكالها بعيدا عن كل تحاميلها: برامج، أجهزة، وحتى العنصر البشري، أوراق، مهارات،..إلخ، مهما كان التحميل الذي يميز المعلومة، المعلوماتية تأخذ حيزا مهما ولكن حصر نظام إدارة أمن المعلومات في الجهة المعلوماتية فهذا خطأ.(Fernandez-Toro, 2016, p. 13)

تم تعريف الأصل في إيزو 27000 بأنه"كل شيء له قيمة للمؤسسة"، إذ تخضع أصول المعلومات لمجموعة واسعة من التهديدات الخارجية والداخلية على حد سواء، انطلاقا من العشوائية إلى المحددة بدقة، فتشمل المخاطر تهديدات الطبيعة، الاحتيال والأنشطة الإجرامية، خطأ المستخدم، فشل النظام، ويمكن أن تؤثر مخاطر المعلومات على واحد أو أكثر من السمات الأساسية الثلاث لأصل المعلومات وهي: السرية، التوافر، التكامل، والتي تعرف باسم"ثالوث الأمان".(Vasudevan, 2015, pp 15.16)

وعليه يعرف إيزو27000 أمن المعلومات على أنه:"الحفاظ على سرية، تكامل، وتوافر المعلومات، إضافة إلى خصائص أخرى مثل الأصالة، المساءلة، عدم التنصل والموثوقية".(Calder, 2013, p. 23)

من خلال تعريف نظام الإدارة وأمن المعلومات نتوصل إلى تعريف نظام إدارة أمن المعلومات بصفة عامة، وهناك عدة تعريفات في هذا المجال نذكرها كالتالي :

لعل أشهر تعريف لنظام إدارة أمن المعلومات هو تعريف المنظمة العالمية للتقييس (ISO) والتي تعرفه على أنه "جزء من نظام الإدارة الشاملة معتمدة على نهج مخاطر الأعمال لتأسيس وتنفيذ وتشغيل ومراقبة وصيانة وتحسين أمن المعلومات"(Arnason & Willett, 2008, p. 98)

وهو نهج إداري منظم خاص بأمن المعلومات، يهدف إلى ضمان التفاعل الفعّال للمكونات الرئيسية الثلاثة لتنفيذ سياسة أمن المعلومات: العمليات، التكنولوجيا، سلوك المستخدم. (Calder, 2013, p. 24)

ويعرف نظام إدارة أمن المعلومات على أنه مجموع الموارد المستعملة من أجل التنظيم والتسيير اليومي لأمن المعلومة، أكثر دقة هو يضم مجموع الوثائق التي تعرف قواعد وعمليات الأمن، المنظومة المشاركة (مسؤول أمن المعلومات، المراسلين الأمنيين، المستخدمين، هيئات القرار....) إضافة إلى البنيات التحتية التقنية للأمن، وبالتالي هو جهاز أو آلية عامة لحوكمة أمن المعلومة.(Bellefin, 2008, p. 5)

2.3 علاقة ISO/IEC 27001 بنظام إدارة أمن المعلومات

المعيار الذي يعالج نظام إدارة أمن المعلومات هو ISO/IEC 27001، هذا الأخير يرتكز على مفاهيم السرية، السلامة والتوافر، والهدف الأساسي لنظام إدارة أمن المعلومات هو العمل على حماية هذه الخصائص الثلاثة بالنسبة للمعلومات الحساسة للمؤسسة، إضافة إلى عناصر أخرى مثل: التحقق من الهوية، متابعة الطلب وامكانية التعقب، المرجعية، عدم التخلي والعديد من الميكانيزمات الأخرى. (Fernandez-Toro, 2016, p. 14)

المعيار ISO/IEC 27001 يحدد الطريقة الواجب اتباعها من أجل اعداد ووضع نظام إدارة أمن المعلومات وهو كالتالي :

- تعريف نطاق نظام إدارة أمن المعلومات: إذ أن إيزو27001 ليست ذو حجم واحد يناسب جميع الأنظمة، وليس كيان ثابت باعتباره يتداخل مع نمو وتطور الأعمال التجارية، والمعيار يعترف صراحة بأنه سيتم تحجيم نظام إدارة أمن المعلومات وفقا لاحتياجات المنظمة. (Calder, 2013, p. 24)

- تكوين سياسة الإدارة.

- تحديد طرق تحليل المخاطر المستعملة: إيزو27001 يفرض تحليل مخاطر ولكن لا يقترح أي طريقة من أجل تحقيقها، صاحب نظام إدارة أمن المعلومات حر في اختيار الطريقة المناسبة بشرط أن تكون موثقة، إيزو يقترح مع ذلك طريقته في التحليل وهي إيزو27005، وهناك طريقة أخرى لتحليل المخاطر مستعملة في إطار إيزو27001 وهي طريقة EBIOS التي تسمح بتقييم ومعالجة المخاطر المتعلقة بأمن أنظمة المعلومات.(Bloch & Wolfhugel, 2011, p. 23)

- تعريف، تحليل وتقييم المخاطر، وتحديد المعالجات المطبقة على مختلف المخاطر، فمعيار إيزو27001 يفرض قيادة تحليل المخاطر ثم تعريف مخطط معالجة هذه المخاطر التي يكون تطبيقها مراقب بصفة مستمرة. تحليل المخاطر يمثل نقطة انطلاق إيزو27001، فهوتطبيق معقد وحساس يتطلب ارتكاز قوي على الإدارة وأيضا منهجية ومخطط تواصل محضر جيدا.

- اثبات التزام إدارة المنظمة في طريقة نظام إدارة أمن المعلومات.

3.3 شروط (طريقة) تبني شهادة الإيزو27001

من أجل الحصول على المصادقة، من الضروري القيام بتدقيق في نظام إدارة أمن المعلومات من طرف منظمة مصادقة خارجية، فشهادة نظام إدارة أمن المعلومات ايزو27001 تتبع نفس العملية في أنظمة الإدارة الأخرى مثل ايزو9001 وايزو14001، إذ يكون العمل بين ثلاثة أعوان: (Del Duca & Planche, 2012, p. 113)

* المؤسسة التي تسعى للشهادة. * مكتب التحضير للمصادقة. * المكتب المصادق.

المنظمة التي تسعى للحصول على الشهادة يجب أولا أن تتعاقد مع منظمة تصديق، هذا العقد لمدة سنوات سيؤطر مجموع دورات المصادقة، منظمة التصديق ستفوض مدققين مصادقين أو مفوضين لتحقيق

الرقابات، هناك العديد من التدقيقات، التدقيق الإبتدائي يغطي مجموع النطاق، تدقيقات مراقبة على مستوى محيط أكثر تقييد، وتدقيق التجديد. مدة الفحص والتدقيق محددة من قبل إيزو27006 وتختلف تبعا لعدد وحجم المواقع، عدد الأشخاص في النطاق.(Bellefin, 2008, p. 15) لكن عملية التدقيق لا تقتصر على المدققين المفوضين بل تكون بمشاركة 3 أطراف، تدقيق الطرف الأول هو مراجعة الممارسات الخاصة التي تقوم بها المؤسسة والتي تتم من قبل تلك المؤسسة، تتم مراجعة الطرف الثاني من قبل منظمة شريكة عادة عملها العلاقات التجارية لبعض المواصفات، ويتم تدقيق الطرف الثالث من قبل طرف ثالث مستقل مثل هيئة اصدار الشهادات أو مدقق الحسابات الخارجي.(Calder, 2013, p. 19)

المنظمة تحصل على الشهادة بعد ضمان قدرتها على العمل في الداخل والحفاظ على نظام إدارة أمن المعلومات.

والبند 4-8 من إيزو27001 إلزامية من أجل الحصول على الشهادة، ويتطلب الإيزو تنفيذ نظام إدارة أمن المعلومات ليكون على نفس نهج إدارات أنظمة الإيزو الأخرى وهي نموذج PDCA.

المصادقة ليست شهادة مكتسبة إلى الأبد، بل يتم فحص نظام إدارة أمن المعلومات وتحديثه وتحسينه بانتظام وفقا لمبدأ PDCA.

تبني "إيزو27001" لا يعطي فعاليته التامة إلا بتفعيل مبادئه الأساسية المقترحة بفعالية، فمشروع تبني"ايزو27001" يجب أن يأخذ مكانته في قلب إدارة أمن المعلومات، أو يكون متبنى من قبل مسؤول أمن نظم المعلومات بمساعدة جماعات الجودة وتسيير المخاطر، ولكن يجب أن يدعم من قبل الإدارة.

4.3 أهمية تبني إيزو 27001

من وراء ارتفاع التبادلات الرقمية، أنظمة المعلومات هي اليوم موصولة داخليا مع كل المخاطر الممكنة، ومصادقة إيزو27001 هي ضمان ثقة بين الشركاء ويمكن أن يصبح في عدة حالات ضرورة (Boulet, 2007, p. 64)، فأكثر من 5000 مؤسسة صادقت على أنظمة إدارة أمن المعلومات بالامتثال لإيزو27001، والعديد منها في طريقها لفعل ذلك نظرا لفعاليتها الواسعة للمساعدة في حماية تجهيزات ومعلومات المؤسسة، فالتفعيل التدريجي لنظام إدارة أمن المعلومات يسمح للمؤسسات بتحقيق

ودون جهد كبير مستوى حماية قاعدي، اقتصادي أكثر، فبإتباع خطوتين أو ثلاث خطوات اضافية، المنظمة يمكنها الحصول على نظام إدارة أمن المعلومات مطابق تماما لإيزو27001 ومناسب جدا للمؤسسة، الأمر الذي يدعم ثقة الإدارة في المنهجية المتبعة من قبل مسؤول أمن نظم المعلومات ومصداقيته، إذ تهدي له دعم جد فعال من أجل الحصول على الوسائل التي يحتاجها لإتمام نشاطاته.

وبهذا الخصوص، صرّح "جوران" الرئيس التنفيذي لمركز البيانات المستقل في "زغرب" كرواتيا والذي عمل لمدة 12 سنة في الصناعة المالية، ويعمل في أمان مدفوعات بطاقات الائتمان، أن حصولهم على شهادة ايزو27001 كان أمرا يستحق العناء، فالعملاء اليوم يتوقعون أصلا حصول المنظمة التي يتعاملون معها على ايزو 27001 وإلا فإنهم ليسوا على استعداد للتحدث معها أصلا، فهو لا يجلب العملاء فقط بل يتيح الدخول إلى أسواق لم يكن ممكنا الدخول إليها لولا هذا المعيار، وبالنسبة لهم فإن تبنّي المعيار ضروري ولكن ليس كافيا.(Al-Zahawi, 2019, p. 74)

4. تطبيق الإيزو27001 حسب نموذج PDCA

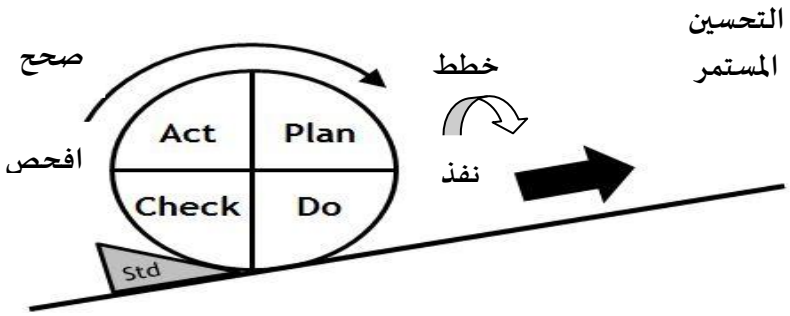
1.4 تعريف دورة التحسين المستمر PDCA

نموذج PDCA هو عبارة عن دورة نشاطات تم تصميمه من أجل الحث على التحسينات المستمرة، من طرف"Walter Shewarts"الاحصائي الأمريكي مخترع دورة دمينغ في كتابه " Statistical Method for the viewpoint of quality control"، هذا النموذج أصبح أكثر شعبية من خلال "Edward Deming" الإحصائي والفيلسوف الأمريكي، مخترع مبادئ الجودة عندما شجع المراحل الأربع لنموذج PDCA للتحسين المستمر، وعليه فان دورة PDCA الناتجة عن إيزو9000 تسمى أيضا دورة التحسين، أو دورة دمينغ نسبة لادوارد دمينغ.

تم تقديم مفهوم التحسين المستمر في الثمانينات في اليابان كجزء من إدارة الجودة الشاملة، فالمبدأ الذي تقوم عليه الجودة الشاملة هو أن كل عملية تساهم في جودة المنتجات والخدمات المقدمة، لذلك هناك حاجة لتحسين جميع عمليات المنظمة. (Gallotti, 2019, p. 233)

نموذج أو دورة PDCA اليوم لم يعد مقتصرا على الجودة الشاملة، بل أصبح نموذج يطبق على كل المعايير المتعلقة بأنظمة الإدارة، مبدأها التحكم في العملية وتحسينها باستعمال دورة مستمرة من أربع مراحل تهدف لتخفيض الحاجة إلى التصحيح، وايزو 27001 الموجه للاهتمام بنظام إدارة أمن المعلومات كغيره من المعايير المتعلقة بأنظمة الإدارة، يرتكز على مقاربة عملية وأكثر دقة على نموذج PDCA، وسمي بهذا الاسم اختصارا لمبادئه الأربعة: خطط (plan)، نفذ (do)، افحص(check)، صحح (act).

الشكل 1:دورة ديمنغ (التحسين المستمر)



Source: (Chardonnet & Thibaudon, 2003, p. 62)

يتسم هذا النموذج بطابعه الدوري، فدورة PDCA تسمح بالوصول إلى الأهداف المسطرة من قبل الإدارة، لكن ماذا يحصل في حال تحقيق الأهداف؟ هنا يجب اتخاذ دورة أخرى لهذا يوجد سهم بين مرحلة Act وPlan فنظام الإدارة عملية تدور بدون توقف(Fernandez-Toro, 2016, p. 12) .

هذا النموذج يطبق على نظام الإدارة في مجموعه كما يطبق على كل مرحلة من مراحله، فمثلا مرحلة خطط لوحدها يمكن تنفيذها عن طريق نموذج PDCA آخر.

2.4 مراحل دورة PDCA: المراحل الأربعة لدورة PDCA هي مراحل مستمرة، فبمجرد الوصول إلى المرحلة الأخيرة يتم اتخاذ دورة أخرى جديدة وتكون المراحل كالتالي :

1.2.4 مرحلة خطط: تتمثل هذه المرحلة في وضع أساسيات نظام إدارة أمن المعلومات، فيتم تعريف الهدف الأساسي، والقيام بجرد لكل الوسائل الضرورية لتحقيقه، وتحديد تكلفة تحقيقه، ووضع الخطة للوصول إليه. وتضم هذه المرحلة عدة خطوات أساسية:(Arnason & Willett, 2008, p. 99)

- تعريف نطاق وسياسة نظام إدارة أمن المعلومات.
- تعريف وتقييم المخاطر.
- تحديد أهداف الرقابة وضوابط علاج المخاطر.
- صياغة مخطط معالجة المخاطر.
- تحضير بيان قابلية التطبيق.

2.2.4 مرحلة نفذ: هذه المرحلة هي المرحلة العملياتية للطريقة، وتضم :

- **مخطط المعالجة:** هذه المرحلة ترتكز على مخطط معالجة المخاطر، بمعنى مخطط الأعمال المفصل الناتج عن تحليل المخاطر الذي يعرف المسؤول عن كل نشاط، الميزانية، المخططات، الوقت اللازم، الأولويات...إلخ

- **اختيار المؤشرات:** هذه المرحلة تكمن في وضع مؤشرات الأداء للتحقق من فعالية معايير الأمن إضافة إلى مؤشرات الامتثال لمراقبة نظام ادراة أمن المعلومات. ايجاد أحسن المؤشرات ليس هيّنا، المعيار لا يدعو إلى مؤشرات معيّنة ولكن إيزو27004 يقترح إجراءات مساعدة.(Boileau, 2010, p. 42)

- **تحسيس وتكوين المستخدمين:** من الضروري أن تتحقق لدى المستخدم ثقافة أمنية تحسّن من تصرفاته وترفع من قدراته في مجال أمن المعلومات، ولا يتم ذلك إلا برفع الوعي والتحسيس وتكثيف التكوين، والتحسيس لا يكون بإلقاء المواعظ ونشر القواعد، وإنما بالتطبيق وإعطاء الأمثلة التي يفهمها المستخدم البسيط، أما التكوين فيجب أن يتكيف مع السياسة الأمنية ومستوى الموظفين، فلكل مستوى تكوين خاص يتلاءم مع وظيفته ونوعية المعلومات التي يمكنه الاطلاع عليها، ويكون بصفة دورية.

- **إجراءات تسيير نظام إدارة أمن المعلومات:** كتحرير الوثائق الضرورية، تسيير موارد النظام، تسيير المخاطر، صيانة نظام إدارة أمن المعلومات عن طريق ضمان العمل الجيد لكل مراحله، تنفيذ المهام،...إلخ.

3.2.4 مرحلة إفحص: تكمن هذه المرحلة في مراجعة عمل نظام إدارة أمن المعلومات بتحديد العناصر غير المتماثلة ونقاط الضعف فيه والقيام بالتحسينات الملائمة، وأيضا التحقق من أن العمليات المتخذة

موافقة للاحتياجات المرجوة حسب الوقت والتكلفة المحدد في المرحلة الأولى..(Carpentier, 2012, p.9)وتكون عملية الفحص من خلال الاجراءات التالية :(Boileau, 2010, p. 44)

- **التدقيق الداخلي**: يمكن أن ينظّم من طرف عمال المنظمة أو يكون تحت إشراف شركة إستشارات، والهدف منه مراقبة امتثال وفعالية نظام إدارة أمن المعلومات بالبحث عن الثغرات بين توثيق النظام ونشاطات المنظمة، المعيار يفرض أن تكون الطريقة المستخدمة في التدقيق موثقة في إجراءات، والتقارير محفوظة من أجل أن تكون مستخدمة من قبل مراجعات الإدارة.

- **المراقبات الداخلية**: هدفها ضمان أن المساهمين يطبقون بطريقة صحيحة الإجراءات يوميا، على عكس التدقيقات الداخلية التي تكون مخططة بمدة مسبقة.

- **مراجعات الإدارة**: المراجعة هي اجتماع سنوي يسمح لمسيري المنظمة بتحليل الأحداث التي جرت في تلك السنة، النقاط المدروسة غالبا هي: نتائج التدقيق، عودة أصحاب المصلحة، حالة النشاطات الوقائية والتصحيحية، التهديدات المفهومة بطريقة سيئة من خلال تقدير المخاطر.

مرحلة افحص عبارة عن مراجعة إدارية لنظام إدارة امن المعلومات تسمح بإعادة تموقع النظام حسب أهداف والتزامات المؤسسة، وفي حالة الضرورة يتم طلب تحديث تحليل المخاطر ومخطط معالجة المخاطر.

4.2.4 مرحلة صحح: في هذه المرحلة يتم الأخذ بعين الإعتبار الفجوات والمشاكل المكتشفة خلال مرحلة إفحص، واقتراح النشاطات الضرورية لتصحيحها واستباق المشاكل المستقبلية، هذه المرحلة تسمح أيضا بإنهاء دورة ديمنغ تحضيرا للدورة المقبلة .

المعيار يؤكد على ضرورة تحضير مخطط للنشاطات التصحيحية موجّه لتصحيح الضعف أو الإختلال الوظيفي الظاهر في نظام إدارة أمن المعلومات والذي يعود إما لعيوب في نظام إدارة أمن المعلومات نفسه أو لعدم فعالية معايير الأمن، وفي إطار نموذج التحسين المستمر PDCA يجب أيضا اقتراح مخطط النشاطات الوقائية، الهدف منه منع الاختلالات المستقبلية (وضع رقابات إضافية مستقبلية). (Bellefin, 2008, p. 7)

5. خاتمة:

إن نظام إدارة أمن المعلومات نظام متكامل يعمل على ضمان أمن المعلومات من خلال ضمان سريتها فلا تُقدم إلا لمن يحتاجها، واتاحتها عند الحاجة إليها دون عراقيل، وتكاملها أي توفيرها على شكلها الأساسي دون حذف أو تعديل، وهذا الأمر يحتاج إلى موارد وكفاءات وسياسات وهياكل..أي تحتاج إلى نظام متكامل، ولتقييم فعالية أنظمة إدارة أمن المعلومات في المؤسسات تم العمل من طرف منظمات دولية مثل:ISO, BSI, IEC على إصدار معيار الإيزو27001. من خلال هذا البحث قمنا بدراسة إشكالية مدى مساهمة معيار ISO/IEC27001 في إرساء قواعد نظام إدارة أمن المعلومات في المؤسسة ودوره في الرفع من مصداقيته، وتم التوصل إلى **النتائج** التالية:

- معيار ISO/IEC27001 عبارة عن مواصفة أو معيار تصديق يحدد المتطلبات والمعايير الواجب الالتزام بها من أجل الحصول على الشهادة، يرافقه معيار ISO/IEC27002 الذي يعتبر معيار توصية من أجل تقديم أفضل الممارسات والتطبيقات في مجال الأمن والحماية.

- يساهم معيار ISO/IEC27001 في إرساء قواعد نظام إدارة أمن المعلومات ويرفع من مصداقيته من خلال الشروط التي يضعها لحصول المنظمة على الشهادة، حيث تقوم المؤسسة التي تسعى للحصول على الشهادة برفع مستوى أمن المعلومات لديها، ويساعد في ذلك الممارسات والتطبيقات الجيدة التي يقدمها معيار ISO/IEC27002 من أجل الاستئناس بها، وهذا ما يؤكد صحة الفرضية الأولى.

- معيار ISO/IEC 27001 يحدد الطريقة الواجب اتباعها من أجل إعداد ووضع النظام، لكن ايزو27001 ليس ذو حجم واحد يناسب جميع الأنظمة، فالمعيار يعترف صراحة بأنه سيتم تحجيم نظام إدارة أمن المعلومات وفقا لاحتياجات المنظمة.

- معيار الايزو 27001 الخاص بأمن نظم المعلومات يعتبر كدليل لأفضل الممارسات في مجال الأمن، يقدم للمؤسسة خطوات مجربة و فعالة في التطبيق، ويساعدها في تقييم وضعيتها الأمنية، خصوصا أنه يطبق عن طريق دورة التحسين المستمر الفعالة.

- دورة التحسين المستمر الخاصة بنظام إدارة الجودة الشاملة PDCA أثبتت فعاليتها أيضا على نظام إدارة أمن المعلومات، حيث تطبيق الدورة من خلال مراحلها الأربعة: خطط، نفذ، افحص، صحح يبين ويكشف لنا دائما عن الثغرات سواء التي تكون في النظام أو في تطبيقة والعمل على تداركها وتحسينها، وهذا ما يؤكد صحة الفرضية الثانية.

التوصيات:

- على المؤسسات الإعتماد على سياسات أمنية مكتوبة، لتسهيل عملية تطبيق أمن المعلومات والمراقبة والمحاسبة ضد أي تجاوز.
- على المؤسسات تهيئة بيئة أنظمة المعلومات من خلال توفير أحدث الأنظمة وبرمجيات الحماية، وتطوير قواعد البيانات وتصميمها بطريقة تسهل الوصول إليها وتوفر لها الحماية من أي اعتداء.
- الاستثمار في الجانب البشري أكثر منه في الجانب المادي، واختيار أحسن الكفاءات للتعامل مع أنظمة المعلومات، وابتكار طرق تسيير حديثة تتلاءم مع بيئة المؤسسة والبيئة الخارجية في نفس الوقت.
- على المؤسسات السعي للحصول على مواصفة إيزو27001، للإرتقاء بمستوى أنظمة معلوماتها وسياساتها الأمنية، ورفع ميزتها التنافسية.

المراجع:

Al-Zahawi, O. (2019). *Information Security"Handbook for ISO27001 controls"*. UR Expert Solutions Ltd.

Arnason, S. T., & Willett, K. (2008). *How to achieve 27001 certification " an example of applied compliance management"*. New York, London: AUerbach publications.

Bellefin, L. (2008). *l'ISO 27000 nouveau nirvana de la sécurité?* France: Solucum Group.

Berteau, Michel, Doyen, et Eric. (2013). *Benchmark des outils SMSI, club 27001*. Livre Blanc.

Bloch, L., & Wolfhugel, C. (2011). *Securité Informatique: principes et méthodes*. Paris: ed Eyrolles.

Boileau, T. (2010). *Mise en oeuvre de la SSI de SUSS Micro Optics par l'approche processus ISO/IEC 27001*. Lyon: Archives ouvertes Hal.
Boulet, P. (2007). *Management de la sécurité de systéme d'information.* Paris: Lavoisier.
Calder, A. (2009). *Information Security based on ISO 27001/ISO 27002 "A Management Guide"*. London: Van Haren.
Calder, A. (2013). *ISO27001/ISO27002 "A pocket guide"*. IT Gouvrnance Publishing.
Carpentier, J. F. (2012). *la sécurité informatique dans la petite entreprise " état de l'art et bonnes pratiques"*. France: ed ENI.
Chardonnet, A., & Thibaudon, D. (2003). *Le Guide du PDCA de Deming " progrés continu et management"*. Editions d'Organization.
Del Duca, J., & Planche, A. (2012). *la Sécurité Informatique"organisez la sécurité du SI de votre entreprise"*. France: ED: ENI.
Fernandez-Toro, A. (2016). *Sécurité Opérationnelle " conseil pratique pour sécuriser le systéme d'information"*. Eyrolles.
Gallotti, C. (2019). *Information Security" Risk Assessment, Management Systems, The ISO/IEC27001 Standard"*. Lulu.
Librairietechnique, s. e. (2016). *ISO 27001 management de la sécurité de l'information.* Paris: Normadoc.
Linlaud, D. (2003). *Sécurité de l'Information"Elaboration et gestion de la politique de l'entreprise suivant l'ISO 17799"*. France: AFNOR.
Vasudevan, V. a. (2015). *Application Security in the 27001:2013 Environment.* United Kingdom: IT Governance Publishing.