IRAQI Academic Scientific Journals
العراقية المجلات الأكاديمية العلمية
مجلة جامعة الكوت
ISSN (E): 2616 - 7808 II ISSN (P): 2414 - 7419
www.kutcollegejournal.alkutcollege.edu.iq
k.u.c.j.sci@alkutcollege.edu.iq
عدد خاص - المؤتمر العلمي الثامن للعلوم الإدارية والاقتصادية - 28-29 يونيو / حزيران 2025

تقييم مدى تطبيق معيار ISO 27001 ودوره في تعزيز التحول الرقمي وأمن المعلومات: دراسة حالة في جامعة الكوت

أ. م. د. صالح مهدي العامري [1] ، م. د علي سعد علوان [2] ، أ. م كمال علوان محيسن [3]

انتساب الباحثين
[1، 2] جامعة الكوت ، العراق ، الكوت ، 52001

[3] جامعة واسط، العراق، الكوت، 52001

[1] salih.alameri@alkutcollege.edu.iq
[2] ali.s.almusawi@alkutcollege.edu.iq
[3] kalwan@uowasit.edu.iq

[2] المؤلف المراسل

معلومات البحث
تاريخ النشر: آب 2025

المستخلص

تواجه المؤسسات الأكاديمية في العراق تحديًا متزايدًا في تعزيز التحول الرقمي وحماية البنية التحتية المعلوماتية في ظل تزايد التهديدات السيبرانية، وتباين الالتزام المؤسسي بمعايير الأمن المعلوماتي. ومن هنا، تنطلق هذه الدراسة لمعالجة الفجوة القائمة بين متطلبات التحول الرقمي ومستوى تطبيق معيار ISO 27001 لنظام إدارة أمن المعلومات، من خلال دراسة حالة في جامعة الكوت.

تهدف الدراسة إلى تشخيص مدى جاهزية الجامعة في تبني متطلبات ISO 27001 وتقييم أثر ذلك في دعم أمن المعلومات وتعزيز الثقة في العمليات الرقمية. وقد اعتمدت الدراسة على منهج دراسة الحالة التحليلية، من خلال استخدام قائمة فحص مكونة من (21 بندًا) موزعة على المحاور الرئيسة للمعيار، إلى جانب مقابلات ميدانية مع أصحاب العلاقة، وتحليل الوثائق الإدارية والتقنية ذات الصلة.

أظهرت النتائج أن مستوى التطبيق الكلي لمتطلبات ISO 27001 بلغ (62.70%)، في حين بلغت الفجوة (37.30%)، مما يشير إلى وجود جهود مؤسسية قائمة لكنها غير مكتملة، خاصة في مجالات التوثيق، تدريب الكوادر، وتحليل مؤشرات الأداء الأمني.

وتوصي الدراسة بضرورة تبني نموذج مؤسسي متكامل لإدارة أمن المعلومات، مع وضع سياسات داخلية واضحة قابلة للقياس، وتوسيع نطاق التدريب والتوثيق، بما يُسهم في تقليل الفجوات وتعزيز الأمن السيبراني في البيئة الجامعية.

الكلمات المفتاحية: التحول الرقمي، أمن المعلومات، الإدارة المؤسسية، ISO 27001، جامعة الكوت

Evaluating the Implementation of ISO 27001 and Its Role in Enhancing Digital Transformation and Information Security: A Case Study at University of Kut

Saleh Mahdi Al-Amiri [1] , Ali Saad Alwan [2] , Kamal Alwan Muheisen [3]

Authors Affiliations
[1, 2] University of Kut, Iraq, wasit, 52001

[3]Wasit University, Iraq, Kut, 52001

[1] salih.alameri@alkutcollege.edu.iq
[2] ali.s.almusawi@alkutcollege.edu.iq
[3] kalwan@uowasit.edu.iq

[2] **Corresponding Author**

Paper Info.
Published: Aug. 2025

Abstract

Academic institutions in Iraq are increasingly challenged to align their digital transformation efforts with international standards for information security, particularly in light of growing cybersecurity threats and inconsistent institutional compliance. This study addresses the gap between the strategic need for digital advancement and the practical implementation of ISO 27001, the international standard for Information Security Management Systems (ISMS), through a case study conducted at Kut University.

The aim of the study is to assess the university's level of adherence to ISO 27001 requirements and evaluate its role in strengthening information security and institutional trust in digital operations. The study adopts an analytical case study approach, utilizing a checklist composed of 21 items mapped to the core components of ISO 27001. It also incorporates qualitative interviews with key stakeholders and analysis of administrative and technical documentation.

The findings reveal that the overall implementation level of ISO 27001 reached 62.70%, with a recorded gap of 37.30%. This reflects an ongoing institutional commitment to security practices, albeit with significant shortfalls, particularly in documentation, staff training, and performance indicator analysis.

The study recommends adopting a comprehensive and integrated institutional model for information security management, supported by measurable internal policies, expanded training programs, and robust documentation. Such measures would help close existing gaps and enhance cybersecurity resilience across the university

environment.

Keywords: Digital Transformation, Information Security, Institutional Management, ISO 27001, University of Kut

المقدمة

أصبحت حماية المعلومات والبيانات الحساسة ركيزة أساسية لنجاح المؤسسات الأكاديمية، لا سيما في ظل تسارع التحول الرقمي وتزايد التهديدات السيبرانية. وفي هذا السياق، يُعد معيار ISO 27001إطارًا عالميًا لإدارة أمن المعلومات، حيث يوفّر نظامًا شاملًا يساعد المؤسسات على تقييم المخاطر، وتعزيز السياسات الأمنية، وتطبيق ضوابط تقنية وتنظيمية فعالة. ويكتسب هذا الموضوع أهمية مضاعفة في بيئات التعليم العالي، مثل جامعة الكوت، التي تعتمد بشكل متزايد على الأنظمة الرقمية لإدارة شؤونها الإدارية والأكاديمية، مما يجعل أمن المعلومات أمرًا لا غنى عنه لضمان الاستقرار المؤسسي والثقة المجتمعية.

تشير الأبحاث الحديثة إلى أن تطبيق ISO 27001 لا يقتصر على تقليل مخاطر الاختراقات، بل يسهم في تحسين كفاءة العمليات وتسهيل التحول الرقمي المستدام. كما يساعد في تحقيق الامتثال لمتطلبات الحوكمة الرشيدة وتعزيز الشفافية والموثوقية في التعامل مع البيانات. وتبرز أهمية هذا التطبيق في ظل تطور التهديدات الرقمية وتعقيد البنية التحتية التقنية، ما يستدعي وجود نظام إدارة أمن معلومات مرن وقابل للتطوير. وتُعد دراسة حالة جامعة الكوت خطوة نحو تقييم واقعي لمدى التزام المؤسسة بتطبيق هذا المعيار، وتحليل نقاط القوة والضعف في سياساتها الرقمية.

ومن خلال هذا التقييم، يمكن التعرف على المعوقات المؤسسية والتقنية التي قد تؤثر على فعالية أمن المعلومات، وتقديم توصيات استراتيجية تدعم بيئة جامعية رقمية وآمنة. وبالتالي، فإن هذا البحث يسعى لتسليط الضوء على العلاقة بين تطبيق معيار ISO 27001والتحول الرقمي بوصفهما محركين رئيسيين للتطوير المؤسسي المستدام في التعليم العالي.

اولاً: مشكلة الدراسة

رغم التوجهات المتزايدة نحو تبني التحول الرقمي في المؤسسات الأكاديمية وتعزيز البنى التحتية التكنولوجية، لا تزال العديد من الجامعات، بما فيها جامعة الكوت، تواجه تحديات في تطبيق معايير متكاملة لأمن المعلومات تواكب هذا التحول. وتتمثل هذه الإشكالية في غياب تطبيق منهجي لمعيارISO 27001 ، ما يؤدي إلى وجود ثغرات أمنية محتملة تؤثر على سلامة البيانات وحوكمة المعلومات داخل البيئة الجامعية. وتزداد أهمية هذه المسألة في ظل توسع الاعتماد على الأنظمة الإلكترونية في إدارة شؤون الطلبة والموظفين، دون وجود إطار موحد لضبط وحماية المعلومات.

وفي هذا السياق، تبرز الحاجة إلى دراسة مدى التزام جامعة الكوت بتطبيق معيارISO 27001 ، وتحليل أثره في دعم التحول الرقمي الآمن والفعّال. وتكمن إشكالية البحث في التساؤل المحوري التالي:

1. إلى أي مدى يسهم تطبيق معيار ISO 27001 في تعزيز التحول الرقمي وأمن المعلومات في جامعة الكوت؟

ثانيًا: أهمية الدراسة

تنبع أهمية هذه الدراسة من تركيزها على أحد المحاور الحيوية في بيئة التعليم العالي المعاصر، وهو أمن المعلومات في ظل التحول الرقمي، وما يرتبط به من مخاطر وتحديات تقنية وتنظيمية. وتكمن الأهمية الجوهرية لهذه الدراسة في سعيها إلى تحليل وتقييم مدى تطبيق معيار ISO 27001 في جامعة الكوت، بوصفه إطارًا دوليًا لإدارة أمن المعلومات يعزز من حماية البيانات ويدعم فعالية التحول الرقمي المؤسسي. في ظل تصاعد الاعتماد على المنصات الرقمية والأنظمة الإلكترونية في إدارة الخدمات الأكاديمية والإدارية، تبرز الحاجة إلى آليات منهجية تضمن حماية هذه البيانات من التهديدات السيبرانية.

وتُعد هذه الدراسة مساهمة نوعية في ردم فجوة معرفية واضحة في الأدبيات العربية التي غالبًا ما تتناول التحول الرقمي بمعزل عن الجوانب الأمنية والمعيارية. كما أنها تسعى إلى تقديم نموذج عملي قابل للتطبيق المؤسسي في بيئة الجامعات العراقية، يسهم في رفع كفاءة الأداء وضمان استمرارية العمل ضمن بيئة رقمية آمنة وموثوقة. من خلال التركيز على معيار ISO 27001، تؤكد الدراسة على أن أمن المعلومات ليس مجرد إجراء تقني، بل هو عنصر استراتيجي ضمن منظومة الحوكمة المؤسسية الشاملة.

1. تعالج إحدى القضايا المحورية في التعليم العالي، وهي أمن المعلومات، ضمن إطار مؤسسي وقياسي.
2. تربط بين التحول الرقمي والامتثال لمعيار ISO 27001، ما يمنح الدراسة بعدًا معياريًا قابلًا للتطبيق.
3. تُسهم في بناء نموذج قياس لتقييم فعالية نظم إدارة أمن المعلومات في البيئة الجامعية.

4. تدعم التوجه نحو حوكمة مؤسسية رقمية قائمة على الكفاءة والامتثال وليس فقط على التطوير التقني.
5. تعزز من قدرة الجامعات على حماية بيانات الطلبة والعاملين وضمان استمرارية الخدمات الأكاديمية.
6. تسهم في إثراء الأدبيات العربية في مجال التحول الرقمي من منظور أمني ومعياري.
7. توفر توصيات عملية تدعم صناعة القرار في مؤسسات التعليم العالي في مجال الأمن السيبراني والتحول الرقمي.

ثالثًا: اهداف الدراسة

تهدف هذه الدراسة إلى تحليل وتقييم مدى التزام جامعة الكوت بتطبيق معيار ISO 27001، ومدى فاعلية هذا التطبيق في دعم التحول الرقمي وتعزيز أمن المعلومات في البيئة الجامعية. وتسعى إلى تقديم نموذج علمي وتطبيقي يمكن أن يسهم في تطوير السياسات الجامعية لضمان بيئة معلوماتية آمنة وموثوقة ومستدامة. إذ تهدف هذه الدراسة إلى تحقيق مجموعة من الأهداف الرئيسة، وهي كما يلي:

1. تحليل مدى توافق ممارسات أمن المعلومات في جامعة الكوت مع متطلبات معيار ISO 27001.
2. تقييم أثر تطبيق نظم إدارة أمن المعلومات على فاعلية التحول الرقمي المؤسسي داخل الجامعة.
3. استكشاف دور الجامعة كمؤسسة تعليمية في تعزيز ثقافة الأمان الرقمي ضمن بيئتها الأكاديمية والإدارية.
4. قياس العلاقة بين تطبيق معيار ISO 27001 ومستوى حماية البيانات والأنظمة الإلكترونية المستخدمة.
5. اقتراح آليات تقنية وإدارية لتعزيز كفاءة نظام إدارة أمن المعلومات بما يواكب التحول الرقمي المتسارع.
6. تسليط الضوء على معيار ISO 27001 كأداة استراتيجية لتقوية الحوكمة الرقمية وضمان الاستدامة المعلوماتية في التعليم العالي.

رابعًا: نموذج الدراسة

يوضح الشكل (1) نموذج الدراسة.

الشكل (1) نموذج الدراسة

خامسًا: مجتمع وعينة الدراسة

يتكون مجتمع الدراسة من العاملين في جامعة الكوت من الملاكات الأكاديمية والإدارية والفنية، ممن لهم علاقة مباشرة بتطبيق نظم

المعلومات أو استخدام المنصات الرقمية، باعتبارهم المعنيين بفعالية نظام إدارة أمن المعلومات والتحول الرقمي داخل الجامعة.

سادسًا: حدود الدراسة

تتحدد هذه الدراسة بالحدود الآتية:

1. الحدود المكانية: جامعة الكوت.
2. الحدود الزمانية: المدة من (2025/2/20) إلى (2025/4/1).
3. الحدود الموضوعية: دراسة مدى تطبيق معيار ISO 27001 في جامعة الكوت، وتحليل دوره في تعزيز التحول الرقمي وأمن المعلومات في البيئة الجامعية.

سابعًا: أداة الدراسة

اعتمدت الدراسة على منهج دراسة الحالة(Case Study) ، بوصفه أحد المناهج النوعية التي تتيح للباحث التعمق في تحليل ظاهرة محددة داخل سياقها الواقعي. وقد تم اختيار جامعة الكوت كحالة للدراسة، لكونها تمثل مؤسسة أكاديمية تسعى نحو التحول الرقمي وتعزيز أمن المعلومات، مما يجعلها بيئة مناسبة لفحص مدى تطبيق معيار ISO 27001 ، وتحليل تأثير هذا التطبيق في دعم البنية الرقمية الآمنة وتعزيز الحوكمة المعلوماتية .وتم استخدام استبانة موجهة لجمع البيانات من الفئات المستهدفة ذات الصلة بالموضوع، مثل كوادر تقنية المعلومات والإداريين والأكاديميين ذوي العلاقة.

ثامنًا: الأساليب الإحصائية المعتمدة

اعتمدت الدراسة على قائمة فحص (Check List) تم إعدادها بالاستناد إلى بنود ومعايير ISO 27001 الخاصة بنظام إدارة أمن المعلومات، بهدف تقييم مدى التزام جامعة الكوت بتطبيق هذه المعايير ضمن بيئة التحول الرقمي. ولتحليل البيانات، تم استخدام الأساليب الإحصائية الوصفية مثل التكرارات، النسب المئوية، والمتوسطات الحسابية، وذلك لقياس درجة الالتزام في المحاور المختلفة. كما تم استخدام تحليل الفجوات (Gap Analysis) لتحديد المسافة بين الوضع التطبيقي الفعلي في الجامعة ومتطلبات معيار ISO 27001 ، بما يساعد في الكشف عن أوجه القصور وتقديم مقترحات تطويرية.

تاسعًا: مصطلحات إجرائية

1. تطبيق معيار ISO 27001: هو مدى التزام جامعة الكوت بتطبيق المتطلبات المنصوص عليها في معيار ISO 27001 لنظام إدارة أمن المعلومات (ISMS)، ويُقاس من خلال فقرات قائمة الفحص المصممة استنادًا إلى بنود المعيار، مثل: سياسة أمن المعلومات، إدارة المخاطر، ضوابط الوصول، واستمرارية الأعمال.
2. التحول الرقمي: هو استخدام التكنولوجيا الرقمية لتحسين العمليات الأكاديمية والإدارية داخل الجامعة، ويُقاس من خلال مدى استخدام الأنظمة الإلكترونية في الإدارة، الخدمات الذكية، وتكامل البنية التحتية الرقمية.
3. أمن المعلومات: يُقصد به في هذه الدراسة حماية بيانات الجامعة من التهديدات السيبرانية، وضمان سريتها وسلامتها وتوافرها، ويُقاس من خلال مؤشرات تتعلق بفعالية الضوابط التقنية والإدارية، والتعامل مع الحوادث الأمنية.
4. قائمة الفحص (Check List): هي أداة بحثية أُعدت استنادًا إلى معيار ISO 27001، بهدف قياس مدى تطبيق البنود الأساسية للمعيار في جامعة الكوت وتحليل الفجوات بين الواقع والتطبيق الأمثل.

عاشرًا: الإطار المفاهيمي لمتغيرات الدراسة

من أجل تعميق الإطار المفاهيمي المتعلق بتقييم تطبيق معيار ISO 27001ودوره في تعزيز التحول الرقمي وأمن المعلومات في جامعة الكوت، مثل تحديات التطبيق، فوائد الحصول على الشهادة، والتوجهات المستقبلية .سيتم دعم كل محور منها بأدبيات علمية ذات صلة، بما يسهم في توسيع الفهم للعلاقة التفاعلية بين ISO 27001والأهداف الأوسع لأمن المعلومات والتحول الرقمي.

1. تطبيق معيار ISO 27001

يوفر معيار ISO 27001 نهجًا منظمًا لإنشاء نظام إدارة أمن المعلومات .(ISMS) تبدأ عملية تطبيقه بتقييم شامل للممارسات الأمنية القائمة، يتبعها تطوير سياسات وإجراءات تتماشى مع متطلبات المعيار [1]. كما يؤكد على أن فهم انتشار معيار ISO 27001 ومعدلات تبنيه يُعد أمرًا جوهريًا للمنظمات الساعية إلى تعزيز أطرها الأمنية [2]. يساهم هذا الفهم في اتخاذ قرارات مدروسة بشأن عملية الحصول على الشهادة، مما يعزز بيئة تنظيمية مواتية لإدارة المخاطر بشكل منهجي.

ولا يقتصر تطبيق ISO 27001 على إرساء بنية أمنية قوية، بل يُظهر أيضًا التزامًا بأفضل الممارسات في حماية البيانات، وهو أمر بات ضروريًا في عالمنا الرقمي. كما يعزز هذا المعيار الميزة التنافسية للمؤسسات من خلال بناء الثقة مع الأطراف المعنية والعملاء عبر الامتثال لمعايير أمنية دولية معترف بها.

2. الدور في أمن المعلومات

يؤدي معيار ISO 27001 دورًا محوريًا في تعزيز قدرات المؤسسات على إدارة أمن المعلومات. إذ يُقدّم إطارًا واضحًا لتحديد وتقييم ومعالجة المخاطر الأمنية، ما يُمكّن المؤسسات من حماية بياناتها الحساسة بفعالية [3]. ويذهب إلى أن دمج ISO 27001 ضمن عمليات إدارة المخاطر المؤسسية يعزز قدرة المؤسسات على كشف الثغرات والتعامل مع المخاطر بشكل فعّال [4].

يُتيح هذا التوافق للمؤسسات التعامل استباقيًا مع التهديدات السيبرانية، من خلال تبني الضوابط والإجراءات المناسبة للحيلولة دون وقوع الاختراقات وفقدان البيانات. كما أن الحصول على الشهادة يُظهر للجهات الخارجية التزام المؤسسة بمعايير عالية من الأمان، ما يعزز مصداقيتها وسمعتها. ويؤكد المعيار على أهمية المراجعة الدورية والتقييم المستمر، بما يضمن التطوير المستدام وتكيّف المؤسسة مع المتغيرات التنظيمية والتقنية.

3. الأثر على التحول الرقمي

يلعب معيار ISO 27001 دورًا أساسيًا في إنجاح مبادرات التحول الرقمي من خلال توفير بيئة آمنة تنطلق منها المؤسسات نحو تبني الحلول التكنولوجية الحديثة. وبحسب ووسيل ودي فريس، فإن الحصول على الشهادة يرسّخ ثقافة الامتثال والوعي الأمني، وهي ثقافة ضرورية في ظل تعقيدات البيئة الرقمية [5]. ومن خلال إدماج ممارسات الأمان في النسيج التشغيلي للمؤسسة، يُسهّل ISO 27001 تبني التقنيات الحديثة دون المساس بأمن المعلومات.

وتُعزز هذه البيئة الآمنة ثقة المستفيدين وأصحاب العلاقة، مما يُمكّن المؤسسات، ومن بينها جامعة الكوت، من تنفيذ مبادرات رقمية نوعية بثقة أكبر. كما يتيح التكامل بين ISO 27001 والرؤية الاستراتيجية للتحول الرقمي الفرصة ليس فقط لتحسين الكفاءة التشغيلية، بل أيضًا للابتكار والاستجابة لمتطلبات السوق والمنافسة.

4. تحديات التطبيق

رغم الفوائد الكبيرة لتطبيقISO 27001 ، إلا أن العديد من المؤسسات تواجه تحديات حقيقية أثناء التنفيذ. وتشمل هذه التحديات: محدودية الموارد، مقاومة التغيير، وقلة الكوادر المؤهلة في مجال إدارة أمن المعلومات. أن المؤسسات غالبًا ما تجد صعوبة في مواءمة المعايير مع العمليات التشغيلية القائمة، وضمان تدريب الموظفين على السياسات والإجراءات الجديدة [6]. كما أن إجراء تقييمات دقيقة للمخاطر، وهو عنصر أساسي في إطار ISO 27001، قد يكون معقدًا بسبب تشعب بيئات تكنولوجيا المعلومات الحديثة. الأمر الذي يتطلب استثمارًا في التدريب والتوعية المستمرة لتمكين جميع الموظفين من فهم مسؤولياتهم في الحفاظ على أمان المعلومات.

5. فوائد الحصول على شهادة ISO 27001

لا تقتصر شهادة ISO 27001 على الامتثال، بل تتيح العديد من المزايا الاستراتيجية للمؤسسات. من أبرز هذه المزايا: تعزيز الثقة والمصداقية لدى العملاء وأصحاب المصلحة. كما تميز الشهادة المؤسسة عن منافسيها من خلال إظهار التزامها بمعايير أمان عالية، وهو ما يُعد نقطة جذب مهمة في قطاعات مثل التمويل والرعاية الصحية. بالإضافة إلى ذلك، تسهم الشهادة في تحسين الكفاءة التشغيلية من خلال تنظيم العمليات وتوفير إطار واضح لإدارة أمن المعلومات [1].

وتتيح الشهادة للمؤسسات الوصول إلى الأسواق العالمية التي تتطلب الالتزام بمعايير الأمان. كما أن تطبيق المعيار بفعالية يقلل من وقت الاستجابة للحوادث الأمنية، ويحد من آثارها التشغيلية والمالية.

6. التوجهات المستقبلية

مع استمرار المؤسسات، ومنها الجامعات مثل جامعة الكوت، في التوسع الرقمي، فإن مستقبل ISO 27001 يبدو واعدًا. هناك توجه متنامٍ نحو دمج ISO 27001 مع معايير إدارية أخرى، مثل اللائحة العامة لحماية البيانات (GDPR) وISO 9001، لتكوين إطار شامل للحوكمة والامتثال[2] . كما أن صعود تقنيات الذكاء الاصطناعي والتعلم الآلي يدفع إلى إعادة تقييم آليات تقييم المخاطر التقليدية المعتمدة في .ISO 27001 إذ بدأت المؤسسات في استكشاف إمكانية توظيف هذه التقنيات لأتمتة عمليات التدقيق وتحسين الاستجابة للتهديدات الأمنية. وقد تركز الأبحاث المستقبلية على تطوير مناهج مبتكرة ترفع من كفاءة تطبيق المعيار، وتضمن استمرارية ملاءمته في بيئة رقمية متسارعة التغير.

الحادي عشر: الجانب العلمي

تهدف هذه الدراسة إلى تحليل وتشخيص واقع تطبيق معيار ISO 27001في جامعة الكوت، باعتباره الإطار المعياري الدولي لإدارة أمن المعلومات، وذلك ضمن السياق الأوسع لتعزيز التحول الرقمي في المؤسسات الأكاديمية. وقد اعتمد الباحثون الثلاثة على منهج دراسة الحالة كمدخل نوعي وعملي لتقويم الأداء المؤسسي من منظور أمني ورقمي، بهدف الكشف عن مدى التزام الجامعة

بمتطلبات ISO 27001 ، وتحليل أثر ذلك في تمكين التحول الرقمي وحماية البنية التحتية المعلوماتية.

ولتحقيق هذا الهدف، تم اعتماد قائمة فحص (Checklist) تم إعدادها بالاستناد إلى المحاور الأساسية للمعيار، إلى جانب توظيف تحليل الفجوات (Gap Analysis) لتحديد مستوى التباين بين الواقع الفعلي والتطبيق المعياري المطلوب.

وقد نُفذت الدراسة ميدانيًا من خلال زيارات ميدانية مباشرة ومعايشة واقعية لبيئة العمل داخل الجامعة، شملت مقابلات شبه مهيكلة مع الكوادر التقنية والإدارية، بالإضافة إلى ملاحظات منظمة، بهدف جمع بيانات وصفية وكمّية موثوقة.

وقد تم قياس مؤشرات الأداء باستخدام مقياس سباعي التدريج كما هو موضح في الجدول (1)، حيث يُمنح الوزن (0) في حال غياب المؤشر تمامًا، ويُمنح الوزن (6) عند تحقيقه بشكل متكامل ومتوافق مع متطلبات ISO 27001.

يسهم هذا التحليل في تشخيص الفجوات البنيوية والتنظيمية، وفهم الأسباب المؤدية إليها، وتحديد إمكانية معالجتها عبر تدخلات مؤسسية محسوبة، الأمر الذي من شأنه أن يُعزز من فاعلية نظام إدارة أمن المعلومات، ويدعم رؤية الجامعة في التحول الرقمي المستدام.

جدول (1) المقياس السباعي

التسلسل	فقرات المقياس السباعي	الوزن (الدرجة)
1	مطبق كلياً وموثق كلياً	6
2	مطبق كلياً وموثق جزئياً	5
3	مطبق كلياً وغير موثق	4
4	مطبق جزئياً وموثق كلياً	3
5	مطبق جزئياً وموثق جزئياً	2
6	مطبق جزئياً وغير موثق	1
7	غير مطبق وغير موثق	0

1. تحليل بيانات قائمة الفحص الخاصة بالمتطلبات

اعتمد الباحثون في إعداد قائمة الفحص (Checklist) الخاصة بجامعة الكوت على زيارات ميدانية مباشرة، ولقاءات نوعية مع رؤساء الأقسام، والشُعب، والوحدات الإدارية، والمراكز التقنية في الجامعة، بالإضافة إلى توثيق ملاحظات تفصيلية ومناقشات متخصصة تتعلق بمجالات تطبيق نظام إدارة أمن المعلومات والتحول الرقمي.

وقد جاءت هذه المنهجية بهدف جمع البيانات والمعلومات بشكل منظم ومنهجي، وتقييم مدى تحقق متطلبات معيار ISO 27001 ، لا سيما ما يتعلق بالمخاطر، الضوابط الأمنية، إدارة الأصول، والتحكم بالوصول، من أجل الوقوف على واقع الممارسات المؤسسية في مجال أمن المعلومات وتعزيز الجاهزية الرقمية .

سعى الباحثون من خلال هذه العملية إلى فهم شامل للعوامل المؤثرة في بناء بيئة معلوماتية مؤمنة ومستدامة، عبر توثيق التحديات المحتملة، وتحديد نقاط الضعف والفرص التحسينية، بما يمكّن من رسم خارطة طريق واضحة لتطوير نظام أمن المعلومات وتحديث البنية الرقمية.

وسيتم لاحقًا تحليل الفجوات بين الواقع الفعلي والتطبيق المعياري المطلوب، باستخدام معادلات تحليلية كمية لقياس مستوى التباين، بهدف تفسير أسباب ظهور هذه الفجوات وقياس أثرها على فاعلية نظام إدارة أمن المعلومات، وصولًا إلى اقتراح حلول عملية قابلة للتطبيق تساعد في تقليص الفجوات وتحقيق الأهداف الأمنية والتنظيمية المرجوة، وذلك وفق المعادلات التالية:

معادلة (1) الوسط الحسابي = مجموع (الأوزان * تكراراتها) / مجموع التكرارات

معادلة (2) النسبة المئوية لمدى المطابقة = (الوسط الحسابي المرجح) / قيمة أعلى وزن في المقياس

معادلة (3) حجم الفجوة لكل قائمة فحص = 1 – النسبة المئوية لمدى المطابقة

2. قائمة فحص المسؤولية الاجتماعية وفق معيارISO 26000

تُعد قائمة الفحص (Checklist) من الأدوات الأساسية التي اعتمد عليها الباحثون الثلاثة في هذه الدراسة لتقييم واقع تطبيق متطلبات معيار ISO 27001 في جامعة الكوت، وذلك بهدف تشخيص

مستوى الالتزام المؤسسي ببناء نظام متكامل لإدارة أمن المعلومات (ISMS)، وتعزيز التحول الرقمي في بيئة أكاديمية معقدة ومترابطة.

ويهدف هذا التقييم إلى قياس مدى توافر الضوابط الإدارية والفنية المتعلقة بأمن المعلومات، والكشف عن الفجوات بين الواقع الفعلي ومتطلبات المعيار، بما يمكّن من تحسين استجابة الجامعة للتهديدات السيبرانية، وضمان حماية البيانات والخدمات الرقمية.

تضمنت قائمة الفحص مجموعة من المحاور الجوهرية التي يعالجها معيارISO 27001 ، تشمل تحديد نطاق نظام أمن المعلومات داخل الجامعة، والرجوع إلى المراجع المعيارية ذات العلاقة، وتحديد المصطلحات والتعاريف المعتمدة لضمان وضوح المفاهيم. كما تناولت القائمة تحليل سياق المؤسسة والبيئة التي تعمل ضمنها، ودور القيادة العليا في توجيه ودعم نظام أمن المعلومات. وقد تم تضمين بنود تتعلق بالتخطيط وتقييم المخاطر وتحديد الأهداف الأمنية، إضافة إلى عناصر الدعم التي تشمل الموارد والتدريب والتوثيق.

كما شملت القائمة تقييم الجوانب التشغيلية للنظام من حيث التنفيذ الفعلي للإجراءات والضوابط الأمنية، وقياس الأداء من خلال عمليات المراجعة والتدقيق الداخلي، وأخيرًا تقييم مدى التزام المؤسسة بإجراءات التحسين المستمر لتطوير كفاءة النظام ومعالجة نقاط الضعف.

تم إعداد هذه البنود بالاستناد إلى زيارات ميدانية مباشرة، ومقابلات نوعية مع مسؤولي الأقسام والوحدات الفنية والإدارية، فضلًا عن تحليل الوثائق الرسمية والملاحظات الميدانية التي جُمعت أثناء مراحل التنفيذ. وتعرض تفاصيل قائمة الفحص في الجدول (2) ، الذي يُبيّن مؤشرات التقييم المستخدمة، وأدوات قياس مدى الالتزام المؤسسي بمعيار ISO 27001.

جدول (2) قائمة فحص تطبيق معيار ISO 27001

ت	1. قائمة فحص تطبيق معيار ISO 27001	مستوى التطبيق والتوثيق						
		مطبق كلياً وموثق كلياً	مطبق كلياً وموثق جزئياً	مطبق كلياً وغير موثق	مطبق جزئياً وموثق كلياً	مطبق جزئياً وموثق جزئياً	مطبق جزئياً وغير موثق	غير مطبق وغير موثق
أولًا: السياق المؤسسي								
1.1	قامت الجامعة بتحليل البيئة الداخلية والخارجية التي تؤثر في نظام إدارة أمن المعلومات؟				✓			
2.1	تم تحديد احتياجات وتوقعات الأطراف المعنية المتعلقة بأمن المعلومات؟			✓				
3.1	تم تحديد نطاق واضح ومعتمد لنظام إدارة أمن المعلومات داخل الجامعة؟			✓				
ثانيًا: القيادة								
4.1	تلتزم الإدارة العليا بتوفير الموارد اللازمة ودعم تطبيق نظام أمن المعلومات؟	✓						
5.1	توجد سياسة أمن معلومات			✓				

	موثقة، معتمدة، ومعلنة لجميع الموظفين؟							
6.1	تُراجع الإدارة العليا هذه السياسة الأمنية بشكل دوري للتأكد من ملاءمتها؟			✓				
ثالثًا: التخطيط								
7.1	تم تحديد وتقييم مخاطر أمن المعلومات بطريقة منهجية؟					✓		
8.1	تم وضع أهداف أمنية واضحة تتماشى مع سياسات الجامعة؟		✓					
9.1	توجد خطة معالجة للمخاطر تتضمن مسؤوليات وإجراءات وموارد واضحة؟			✓				
رابعًا: الدعم								
10.1	تمتلك الجامعة الموارد البشرية والتقنية الكافية لتطبيق النظام؟	✓						
11.1	يتم تدريب الموظفين على السياسات والإجراءات الأمنية بشكل دوري؟							✓
12.1	تتم إدارة الوثائق والمعلومات الأمنية بصورة منظمة وسهلة الوصول؟	✓						
خامسًا: التشغيل								
13.1	تُطبق الجامعة الإجراءات والضوابط الأمنية على جميع الأنظمة والمعلومات؟			✓				
14.1	يتم مراقبة العمليات المهمة، والتعامل مع الحوادث الأمنية وفق إجراءات محددة؟			✓				
15.1	توجد خطط تشغيلية تضمن استمرارية الأمن المعلوماتي؟			✓				
سادسًا: تقييم الأداء								
16.1	يتم إجراء عمليات تدقيق داخلي بشكل منتظم لمراجعة تطبيق النظام؟				✓			

17.1	تُستخدم نتائج التدقيق لاتخاذ قرارات تصحيحية أو تطويرية؟				✓			
18.1	يتم تحليل مؤشرات الأداء الأمني بصورة دورية لتحديد اتجاهات المخاطر؟							✓
	سابعًا: التحسين							
19.1	توجد إجراءات معتمدة للتحسين المستمر ومعالجة أوجه القصور؟				✓			
20.1	يتم توثيق نتائج التحسينات الأمنية وتقييم فعاليتها بعد التنفيذ؟				✓			
21.1	تُراجع التحسينات ضمن الاجتماعات الإدارية لضمان التوافق مع الأهداف الاستراتيجية؟				✓			
	الأوزان	**6**	**5**	**4**	**3**	**2**	**1**	**0**
	التكرارات	3	1	12	2	1	0	2
	الوزن (ناتج x عدد التكرارات)	18	5	48	6	2	0	0
	المعدل الموزون (الوسط الحسابي المرجح)	**3.76**						
	النسبة المئوية للتطبيق	**% 62.70**						
	حجم الفجوة للمتطلب	**% 37.30**						

المصدر: من إعداد الباحثون

من خلال نتائج قائمة الفحص تبين الآتي:

أولاً: نقاط القوة

1. التزام الإدارة العليا بتوفير الموارد اللازمة لنظام إدارة أمن المعلومات، وهو ما يعكس دعمًا مؤسسيًا واضحًا.
2. توفر السياسات الأساسية لأمن المعلومات، مثل وجود سياسة موثقة ومعلنة، ووجود خطة معالجة للمخاطر.
3. إدارة الوثائق والمعلومات الأمنية بطريقة منظمة وسهلة الوصول، ما يدل على وجود نظام توثيق فعّال.
4. تطبيق الإجراءات والضوابط الأمنية على الأنظمة والبيانات، وهو مؤشر على وجود بنية تحتية رقمية محمية.
5. وجود خطط لتقييم الأداء من خلال تنفيذ عمليات تدقيق داخلي بشكل منتظم.
6. توفر آلية للتحسين المستمر من خلال مراجعة التحسينات وتوثيق نتائجها بعد التنفيذ.

ثانيًا: نقاط الضعف

1. ضعف توثيق بعض الممارسات؛ حيث لوحظ أن العديد من الإجراءات تُطبق دون دعم كافٍ بالتوثيق الرسمي.
2. غياب التدريب المستمر للموظفين على السياسات والإجراءات الأمنية، ما قد يؤثر على فاعلية التنفيذ.

3. تحليل مؤشرات الأداء الأمني لم يُطبق بالشكل الكافي، مما يحد من القدرة على الكشف المبكر عن المخاطر.
4. تفاوت في التزام بعض الوحدات بتطبيق السياسات أو مراقبة العمليات الأمنية.
5. عدم اكتمال دمج تقييم المخاطر مع الأهداف الاستراتيجية في بعض الحالات، ما قد يؤثر على التكامل المؤسسي بين الجوانب الأمنية والتنموية.
6. وجود بنود غير مطبقة أو غير موثقة كليًا (كما في 2 من أصل 21)، وهو ما يؤكد الحاجة إلى مزيد من المراجعة والتطوير التنظيمي.

الاستنتاجات والتوصيات

اولاً: الاستنتاجات

1. يتضح أن جامعة الكوت حققت مستوى متوسطًا من الالتزام بمتطلبات معيار ISO 27001، مما يعكس وجود وعي مؤسسي مبدئي بأهمية إدارة أمن المعلومات، إلا أن التطبيق لا يزال بحاجة إلى مزيد من التعزيز المؤسسي.
2. أظهرت البيانات وجود دعم إداري فعلي من القيادة العليا، خصوصًا في ما يتعلق بتوفير الموارد الأساسية ووضع السياسات الأمنية، إلا أن عملية التوثيق لم تكن متكاملة في عدد من المؤشرات الأساسية.
3. تعاني بعض المحاور، مثل تدريب الكوادر وتحليل مؤشرات الأداء الأمني، من ضعف واضح في التطبيق، وهو ما يحدّ من فاعلية النظام على المدى الطويل ويعرض البيانات الجامعية للمخاطر المحتملة.
4. تُظهر الفجوة البالغة 37.30% أن هناك مجالات حرجة لم تُعالج بعد بالشكل المطلوب، وخصوصًا ما يتعلق بالتكامل بين الخطة الأمنية وأهداف التحول الرقمي.
5. إن عدم انتظام التدقيق الداخلي والتحسين التفاعلي المستند إلى البيانات يشكل أحد أبرز أسباب اتساع الفجوة بين الواقع والمتطلبات القياسية للمواصفة.

ثانياً: التوصيات

استنادًا إلى ما سبق، نوصي بما يلي:

1. ضرورة إطلاق خطة مؤسسية شاملة لتعزيز تطبيق معيار ISO 27001، تشمل تحديث السياسات، وضبط التوثيق، وتوسيع التدريب ليشمل كافة العاملين ذوي العلاقة.
2. إنشاء وحدة مختصة بإدارة أمن المعلومات داخل الجامعة تتولى التنسيق بين الأقسام الفنية والإدارية لضمان التنفيذ الفعلي لمتطلبات النظام.
3. اعتماد برامج تدريبية دورية لرفع وعي الموظفين بسياسات أمن المعلومات، وتحديث معارفهم حول إدارة المخاطر والاستجابة للحوادث.
4. تعزيز عملية التدقيق الداخلي المنتظم، ومتابعة نتائج المراجعات لاتخاذ قرارات تصحيحية فعالة ومبنية على مؤشرات أداء واقعية.
5. تحسين آليات جمع البيانات وتحليل مؤشرات الأداء الأمني بشكل دوري، من أجل اكتشاف الثغرات بشكل استباقي قبل تحوّلها إلى تهديدات فعلية.
6. تطوير خطة تحسين مستمر مؤسسية تعالج أوجه القصور المكتشفة، وتُدمج ضمن الخطط الاستراتيجية للتحول الرقمي، مع التأكيد على أن أمن المعلومات ركيزة أساسية في حوكمة الأنظمة الجامعية.

المصادر

[1] Disterer, G. (2013). Iso/iec 27000, 27001 and 27002 for information security management. Journal of Information Security, 04(02), 92-100. https://doi.org/10.4236/jis.2013.42011.

[2] Podrecca, M. and Sartor, M. (2023). Forecasting the diffusion of iso/iec 27001: a grey model approach. The TQM Journal, 35(9), 123-151. https://doi.org/10.1108/tqm-07-2022-0220.

[3] Jevelin, J. and Faza, A. (2023). Evaluation the information security management system: a path towards iso 27001 certification. Journal of Information Systems and Informatics, 5(4), 1240-1256. https://doi.org/10.51519/journalisi.v5i4.572.

[4] Olaniyi, O. O., Omogoroye, O. O., Olaniyi, F. G., Alao, A. I., & Oladoyinbo, T. O. (2024). Cyberfusion protocols: strategic integration of enterprise risk management, iso 27001, and mobile forensics for advanced digital security in the modern business ecosystem. Journal of

Engineering Research and Reports, 26(6), 31-49. https://doi.org/10.9734/jerr/2024/v26i61160.

[5] Wessel, R. v. and Vries, H. d. (2018). Business impacts of international standards for information security management. lessons from case companies. Journal of ICT Standardization, 1(1), 25-40. https://doi.org/10.13052/jicts2245-800x.112.

[6] Kamariotou, M., & Kitsios, F. (2022). Hackathons for driving service innovation strategies: The evolution of a digital platform-based ecosystem. Journal of Open Innovation: Technology, Market, and Complexity, 8(3), 111.

[7] Alwan, A. S., Esmail, B. S., & Al-khattawi, A. A. (2023). The Quality of Educational Laboratories According to the International Standard ISO 15189-A Case Study at Kut University College. Al-Kut University College Journal, (Special issue).