

جامعة ميدأوشن

كلية الإدارة

قسم / تخصص ماجستير إدارة المخاطر



عنوان البحث

أثر تطبيق معايير ISO 27001 على الحد من مخاطر تسرب وفقدان الوثائق المرقمنة والرقمية في تجمع الطائف الصحي

The Impact of Implementing ISO 27001 Standards on Mitigating the Risks of Leakage and Loss of Digitized and Digital Documents in Taif Health Cluster.

إعداد الطالب/فهد بن رجاء الله الثبيتي

[2021202249](#)

ماجستير إدارة المخاطر

إشراف/

د.الفیصل عبد الحمید

د.فايز جراد

العام الدراسي:

٢٠٢٥

مقدمة:

يعد أمن المعلومات وإدارة الوثائق الرقمية أحد الركائز الرئيسية في المؤسسات الحديثة، لا سيما في القطاعات الصحية التي تتعامل مع كميات هائلة من البيانات الحساسة. ومع التوسع في التحول الرقمي، أصبحت المؤسسات الصحية أكثر اعتمادًا على الأنظمة الإلكترونية لحفظ وتخزين الوثائق، مما جعلها عرضة لمخاطر متعددة مثل التسرب غير المصرح به، الفقدان، والاختراقات الأمنية. ومن هنا برزت الحاجة إلى تطبيق معايير ISO 27001، التي تعد من أهم المعايير الدولية لضمان أمن المعلومات وإدارة المخاطر المرتبطة بها.

يهدف هذا البحث إلى دراسة أثر تطبيق معايير ISO 27001 على الحد من مخاطر تسرب وفقدان الوثائق الرقمية والمرقمنة في تجمع الطائف الصحي. حيث يعتبر تطبيق هذه المعايير أداة إستراتيجية لضمان سرية، سلامة، وتوافر المعلومات، مما يعزز من كفاءة العمليات الإدارية ويحسن مستوى الأمان الرقمي. ويركز البحث على تحليل مدى تأثير الامتثال لهذه المعايير على أمن الوثائق الصحية ومعلوماتها، من خلال تقييم الأنظمة التقنية، السياسات التنظيمية، وإجراءات الحماية المعتمدة داخل التجمع الصحي.

تأتي أهمية هذه الدراسة من الحاجة الماسة إلى حماية الوثائق الصحية، التي تتضمن معلومات حساسة عن المرضى، التقارير الطبية، وسجلات المعاملات المالية والإدارية. ففقدان أو تسرب هذه الوثائق يمكن أن يؤدي إلى مخاطر جسيمة مثل انتهاك خصوصية المرضى، الإضرار بسمعة المؤسسة، والتعرض للمساءلة القانونية. لذا، فإن هذه الدراسة تسهم في سد الفجوة المعرفية من خلال تقديم تحليل شامل لتأثير تطبيق ISO 27001 على إدارة مخاطر الوثائق الرقمية في المؤسسات الصحية، مما يساعد في تحسين الأمن السيبراني وتعزيز الامتثال التنظيمي.

وعليه، فإن هذه الدراسة تقدم إضافة نوعية في مجال إدارة المخاطر وأمن المعلومات الصحية، حيث توفر نتائجها دليلاً عملياً للمؤسسات الصحية الراغبة في تبني استراتيجيات متقدمة لحماية وثائقها الرقمية من المخاطر المحتملة.

مشكلة الدراسة:

مع التطور السريع في التحول الرقمي واعتماد المؤسسات الصحية على الأنظمة الإلكترونية في إدارة الوثائق والمحفوظات، أصبحت البيانات الرقمية والمرقمنة عرضة لمخاطر أمنية متزايدة، أبرزها تسرب المعلومات، فقدان الوثائق، والاختراقات السيبرانية .

في تجمع الطائف الصحي، يتم التعامل مع كميات ضخمة من الوثائق الرقمية التي تشمل السجلات الطبية للمرضى، البيانات الإدارية، العقود، التقارير المالية، والمراسلات الرسمية، مما يجعلها هدفًا محتملاً للتهديدات الأمنية في ظل غياب سياسات فعالة لضبط وحماية هذه المعلومات.

على الرغم من أن معايير ISO 27001 تُعتبر إطارًا عالميًا لإدارة أمن المعلومات والحد من المخاطر المرتبطة بها، إلا أن مستوى تطبيق هذه المعايير في المؤسسات الصحية قد يواجه تحديات تتعلق بالبنية التحتية التقنية، الوعي الأمني، الامتثال التنظيمي، وتطوير السياسات والإجراءات المناسبة .

عدم تطبيق هذه المعايير بشكل صحيح قد يؤدي إلى ثغرات أمنية خطيرة، مما يزيد من احتمالية تسرب الوثائق الحساسة أو فقدانها، وبالتالي التأثير على كفاءة العمل، الامتثال القانوني، وثقة المرضى والمؤسسات الشريكة.

رغم الجهود المبذولة لتطبيق معايير أمن المعلومات، لا تزال هناك فجوات واضحة في إدارة الوثائق الرقمية والمرقمنة، مما يجعل المؤسسة عرضة لمخاطر تسرب أو فقدان البيانات. ومن هنا تبرز مشكلة البحث الرئيسية: هل يؤدي تطبيق معايير ISO 27001 إلى الحد من مخاطر تسرب وفقدان الوثائق الرقمية والمرقمنة في تجمع الطائف الصحي؟

يمكن تصنيف مشكلة الدراسة إلى المحاور التالية:

١. مشكلة أمنية: ضعف أنظمة الحماية المطبقة على الوثائق الرقمية والمرقمنة، مما يزيد من احتمالية تعرضها للاختراق أو التسرب غير المصرح به، الأمر الذي قد يؤثر على سرية المعلومات المخزنة وسلامتها.
٢. مشكلة تشغيلية: غياب سياسات واضحة وآليات تنفيذ فعالة لإدارة أمن الوثائق الرقمية وفقًا لمتطلبات ISO 27001، مما يؤدي إلى عدم كفاءة في التعامل مع المخاطر المحتملة.
٣. مشكلة قانونية وأخلاقية: احتمالية تعرض الوثائق الحساسة، مثل بيانات المرضى والسجلات الطبية، للاختراق، مما قد يتسبب في انتهاكات قانونية وأخلاقية تتعلق بخصوصية الأفراد وحماية المعلومات الشخصية.
٤. مشكلة إدارية وتقنية: نقص التكامل بين الأنظمة الرقمية المستخدمة في إدارة الوثائق، مما يحد من قدرة المؤسسات الصحية على تطبيق معايير الأمان بالشكل الأمثل، ويؤثر على موثوقية أنظمة الأرشفة واسترجاع البيانات.
٥. مشكلة بحثية وعلمية: وجود فجوة بحثية تتعلق بمدى فاعلية تطبيق ISO 27001 في المؤسسات الصحية، حيث تفتقر الدراسات المحلية إلى تقييم شامل لكيفية الحد من مخاطر تسرب وفقدان الوثائق الرقمية في هذا السياق.

إشكالية الدراسة:

بناءً على التحديات السابقة، تتمحور إشكالية البحث حول التساؤل التالي: "ما مدى تأثير تطبيق معايير ISO 27001 على الحد من مخاطر تسرب وفقدان الوثائق الرقمية والمقرمنة في تجمع الطائف الصحي؟"

أسئلة الدراسة الرئيسية والفرعية:

للإجابة على إشكالية الدراسة، سيتم استكشاف المحاور التالية:

١. ما مدى الالتزام الحالي بتطبيق معايير ISO 27001 في تجمع الطائف الصحي؟
٢. إلى أي مدى يساهم تطبيق هذه المعايير في تحسين أمن الوثائق الرقمية وتقليل مخاطر الفقدان والتسرب؟
٣. ما هي أبرز التحديات التي تواجه المؤسسات الصحية عند تطبيق معايير ISO 27001؟
٤. كيف يمكن تعزيز السياسات والإجراءات لضمان حماية الوثائق والمحفوظات وفقاً لمتطلبات ISO 27001؟
٥. ما مدى تأثير التوعية والتدريب في تحسين الامتثال لمعايير الأمن السيبراني وإدارة الوثائق الرقمية؟

أسئلة الدراسة التفصيلية:

١. ما هي المخاطر الرئيسية المرتبطة بتسرب وفقدان الوثائق الرقمية والمقرمنة في تجمع الطائف الصحي؟
٢. إلى أي مدى يمكن أن تساهم معايير ISO 27001 في الحد من هذه المخاطر وتعزيز أمن الوثائق الرقمية؟
٣. ما هي الفجوات الحالية في أنظمة إدارة الوثائق الرقمية في تجمع الطائف الصحي، وما سبل معالجتها؟
٤. كيف يمكن تحسين استراتيجيات تطبيق معايير ISO 27001 لتقليل مخاطر تسرب وفقدان الوثائق الرقمية والمقرمنة؟
٥. ما هو الدور الذي تلعبه البنية التحتية التقنية والسياسات التنظيمية في دعم تطبيق معايير أمن المعلومات ISO 27001؟

أهمية الدراسة:

تأتي هذه الدراسة استجابة للحاجة المتزايدة إلى تعزيز أمن الوثائق الرقمية في المؤسسات الصحية، حيث يشكل تسرب البيانات وفقدانها تهديدًا خطيرًا على الأمن المعلوماتي وسلامة السجلات الصحية والوثائق الرسمية. ومع التطور المستمر للأنظمة الرقمية، أصبح تطبيق معايير ISO 27001 ضرورة ملحة لضمان حماية الوثائق الرقمية والحد من المخاطر المرتبطة بها، مثل الاختراقات السيبرانية، الأخطاء البشرية، وفقدان البيانات نتيجة أعطال تقنية أو هجمات إلكترونية. يهدف البحث إلى تقييم دور هذه المعايير في تعزيز أمن الوثائق الرقمية في تجمع الطائف الصحي، مما يعزز القدرة على الحد من المخاطر وضمان الامتثال لأفضل الممارسات في إدارة أمن المعلومات.

مكانة الدراسة بين الدراسات السابقة

سلّطت العديد من الدراسات السابقة الضوء على أهمية إدارة الوثائق الرقمية وحمايتها، حيث تناولت دراسة علام (2023) استخدام الأنظمة الآلية في إدارة الوثائق والأرشيف الرقمي، مؤكدةً ضرورة تطوير أنظمة متخصصة تتماشى مع المعايير الأرشيفية بدلاً من الاعتماد على حلول برمجية غير مخصصة. بالإضافة إلى ذلك، ركزت دراسات أخرى على تأمين الوثائق الإلكترونية ضد التهديدات السيبرانية، وضمان الامتثال لمعايير أمن المعلومات. ومع ذلك، تفتقر معظم الأبحاث إلى دراسة معمقة لتطبيق معايير ISO 27001 داخل المؤسسات الصحية، وخاصة في بيئة مثل تجمع الطائف الصحي. ومن هنا تأتي أهمية هذه الدراسة في سد هذه الفجوة البحثية، من خلال تحليل مدى فاعلية تطبيق معايير ISO 27001 وتأثيرها المباشر على تقليل مخاطر تسرب وفقدان الوثائق الرقمية.

الجديد الذي تقدمه الدراسة

تهدف هذه الدراسة إلى تقديم رؤية تحليلية متكاملة حول تأثير تطبيق معايير ISO 27001 على أمن الوثائق الرقمية والمركمنة في المؤسسات الصحية، وذلك من خلال:

١. تحليل الفجوات الأمنية الحالية في أنظمة الأرشيف الرقمية وأمن المعلومات داخل تجمع الطائف الصحي.
 ٢. تقييم فاعلية تطبيق معايير ISO 27001 في تقليل المخاطر المرتبطة بتسرب وفقدان الوثائق الرقمية، بناءً على بيانات ميدانية وتحليلية.
 ٣. تقديم حلول وتوصيات عملية لمواءمة سياسات الأرشيف الرقمية مع أفضل الممارسات العالمية في أمن المعلومات، بما يساهم في تحسين كفاءة العمل المؤسسي وحماية البيانات الحساسة.
- وبذلك، تقدم الدراسة نموذجًا إرشاديًا يمكن اعتماده في المؤسسات الصحية الأخرى التي تسعى إلى تعزيز أمن وثائقها الرقمية وتطوير سياسات فعالة لحمايتها من المخاطر المحتملة، مما يساهم في تحسين استمرارية الأعمال وحماية بيانات المرضى والمستندات الإدارية الحيوية.

أهداف الدراسة:

تهدف هذه الدراسة إلى تحليل أثر تطبيق معايير ISO 27001 على الحد من مخاطر تسرب وفقدان الوثائق المرقمنة والرقمية في تجمع الطائف الصحي، وذلك من خلال تحقيق الأهداف التالية:

١. تقييم مدى فعالية تطبيق معايير ISO 27001 في تقييم وتحليل المخاطر الأمنية المتعلقة بتسرب وفقدان الوثائق الرقمية، وذلك من خلال دراسة الإجراءات الأمنية المتبعة ومدى توافقها مع المعايير الدولية.
 ٢. تحليل تأثير ضوابط التحكم في الوصول وفق معايير ISO 27001 على تقليل احتمالية الوصول غير المصرح به للوثائق الرقمية، وتحديد مدى كفاءة آليات المصادقة والتوثيق الأمني المطبقة.
 ٣. قياس مدى مساهمة تقنيات التشفير وحماية البيانات في تحسين أمان الوثائق الرقمية في تجمع الطائف الصحي، من خلال دراسة فاعلية أنظمة التشفير وأدوات الحماية الرقمية المطبقة.
 ٤. دراسة تأثير خطط استمرارية الأعمال والتعافي من الكوارث وفق معايير ISO 27001 على حماية الوثائق الرقمية من الفقدان، ومدى جاهزية المؤسسات الصحية لاستعادة البيانات بعد حدوث أي أعطال أو تهديدات أمنية.
 ٥. تحليل أثر التدقيق الأمني المستمر وفق معايير ISO 27001 على تحسين أمن الوثائق الرقمية وتقليل نقاط الضعف الأمنية، وتحديد دور عمليات المراجعة الدورية في تحقيق الامتثال للمعايير.
 ٦. تقييم دور معايير ISO 27001 في الحد من تسرب الوثائق الرقمية من خلال تقنيات الحماية والرصد المستمر، وقياس مدى كفاءة إجراءات الحماية المطبقة في تجمع الطائف الصحي.
 ٧. تحليل مدى تأثير تطبيق معايير ISO 27001 على تحسين أداء وموثوقية أنظمة الأرشفة الرقمية، وتقليل فقدان الوثائق الرقمية من خلال تعزيز الأمن السيبراني لنظم الأرشفة.
 ٨. دراسة كيف يمكن لاستراتيجيات إدارة الوثائق وفق معايير ISO 27001 أن تعزز من أمن الوثائق الرقمية وتقليل فقدانها من خلال توظيف السياسات الأمنية الفعالة في الأرشفة الإلكترونية.
 ٩. تحليل مدى تأثير ضوابط الوصول المطبقة وفق ISO 27001 على تحسين التحكم في إدارة الوثائق الرقمية ومنع فقدانها، من خلال تطبيق مبادئ التحكم في الصلاحيات والتوثيق الأمني.
 ١٠. قياس أثر تدريب الموظفين على معايير ISO 27001 في تعزيز أمن الوثائق الرقمية وتقليل الأخطاء البشرية التي قد تؤدي إلى فقدانها أو تسريبها، عبر تعزيز وعي المستخدمين بأفضل ممارسات الحماية الرقمية.
- يتمثل الهدف الرئيسي لهذا البحث في تطوير نموذج متكامل لتطبيق معايير ISO 27001 داخل المؤسسات الصحية، بما يساهم في تعزيز حماية الوثائق المرقمنة والرقمية، والحد من المخاطر المرتبطة بتسريبها أو فقدانها. كما تسعى الدراسة إلى تقديم توصيات عملية لتحسين إجراءات الأمان، وتعزيز كفاءة أنظمة الأرشفة الرقمية، وتحقيق أعلى مستويات الامتثال للمعايير الدولية في مجال أمن المعلومات داخل تجمع الطائف الصحي.

تساؤلات الدراسة

تهدف هذه الدراسة إلى استكشاف وتحليل أثر تطبيق معايير ISO 27001 على الحد من مخاطر تسرب وفقدان الوثائق المرقمنة والرقمية في تجمع الطائف الصحي، وذلك من خلال الإجابة على التساؤلات البحثية التالية:

١. ما مدى فعالية تطبيق معايير ISO 27001 في تقييم وتحليل المخاطر الأمنية المتعلقة بتسرب وفقدان الوثائق الرقمية؟
٢. كيف يؤثر تطبيق ضوابط التحكم في الوصول وفق معايير ISO 27001 على تقليل احتمالية الوصول غير المصرح به للوثائق الرقمية؟
٣. إلى أي مدى يساهم استخدام تقنيات التشفير وحماية البيانات في تحسين أمان الوثائق الرقمية في تجمع الطائف الصحي؟
٤. ما مدى تأثير خطط استمرارية الأعمال والتعافي من الكوارث وفق معايير ISO 27001 على حماية الوثائق الرقمية من الفقدان؟
٥. كيف يؤثر إجراء التدقيق الأمني المستمر وفق معايير ISO 27001 على تحسين أمن الوثائق الرقمية؟
٦. كيف يساهم تطبيق معايير ISO 27001 في الحد من تسرب الوثائق الرقمية من خلال تقنيات الحماية والرصد المستمر؟
٧. إلى أي مدى يساهم تطبيق معايير ISO 27001 في تحسين أداء وموثوقية أنظمة الأرشفة الرقمية وتقليل فقدان الوثائق؟
٨. كيف يمكن لاستراتيجيات إدارة الوثائق وفق معايير ISO 27001 أن تعزز من أمن الوثائق الرقمية وتقليل فقدانها؟
٩. ما مدى تأثير ضوابط الوصول المطبقة وفق ISO 27001 على تحسين التحكم في إدارة الوثائق الرقمية ومنع فقدانها؟
١٠. كيف يؤثر تدريب الموظفين على معايير ISO 27001 في تعزيز أمن الوثائق الرقمية وتقليل الأخطاء البشرية التي قد تؤدي إلى فقدانها أو تسريبها؟

تسعى هذه الأسئلة إلى استكشاف جميع الجوانب المتعلقة بتطبيق معايير ISO 27001 في بيئة المؤسسات الصحية، مع التركيز على التحديات، الفوائد، وأثر تنفيذ هذه المعايير على أمن الوثائق المرقمنة والرقمية داخل تجمع الطائف الصحي.

السؤال الرئيسي للدراسة

إلى أي مدى يسهم تطبيق معايير ISO 27001 في الحد من مخاطر تسرب وفقدان الوثائق المرقمنة والرقمية في تجمع الطائف الصحي؟

تسهم هذه الأسئلة في بناء إطار تحليلي شامل يساعد في فهم تأثير معايير الأمان المعلوماتي على إدارة الوثائق المرقمنة والرقمية، وتقديم حلول عملية لتعزيز أمنها داخل المؤسسات الصحية.

1. المتغير الرئيسي (المستقل):

تطبيق معايير ISO 27001

- التعريف الإجرائي: يقصد به تنفيذ السياسات والإجراءات الأمنية المستندة إلى معايير ISO 27001 داخل تجمع الطائف الصحي، بهدف تعزيز أمن المعلومات وتقليل مخاطر تسرب وفقدان الوثائق الرقمية والرقمنة.

أبعاد المتغير الرئيسي تطبيق معايير: (ISO 27001)

١. إدارة المخاطر الأمنية: (Risk Management)

- تقييم وتحليل المخاطر المحتملة لتسرب أو فقدان الوثائق.
- وضع خطط للحد من المخاطر الأمنية المرتبطة بالوثائق الرقمية.

٢. التحكم في الوصول إلى المعلومات: (Access Control)

- تحديد مستويات الصلاحيات بناءً على مبدأ "الحد الأدنى من الامتيازات".
- تنفيذ التوثيق المتعدد العوامل (MFA) لضمان أمن الوصول.

٣. التشفير وحماية البيانات: (Data Encryption & Protection)

- تطبيق أنظمة التشفير لحماية الوثائق أثناء التخزين والنقل.
- تنفيذ أنظمة إدارة مفاتيح التشفير (KMS) لضمان أمن البيانات.

٤. إدارة استمرارية الأعمال والتعافي من الكوارث: (BCP & DRP)

- تطوير خطط طوارئ تضمن استرجاع الوثائق الرقمية عند حدوث أعطال.
- اختبار استراتيجيات النسخ الاحتياطي لضمان سلامة الوثائق.

٥. الامتثال والتدقيق الأمني: (Compliance & Security Audits)

- إجراء مراجعات دورية لضمان التزام الأنظمة بمعايير ISO 27001.
- تقييم مدى تطبيق الإجراءات الأمنية لحماية الوثائق الرقمية.

2. المتغير التابع:

الحد من مخاطر تسرب وفقدان الوثائق المرقمنة والرقمية

- التعريف الإجرائي: يقصد به قدرة المنظمة على تقليل احتمالات تسرب الوثائق أو فقدانها من خلال تطبيق ضوابط أمنية وإدارية وتقنية، وتحقيق بيئة أكثر أماناً لإدارة الوثائق.

أبعاد المتغير التابع (الحد من مخاطر تسرب وفقدان الوثائق):

١. تقليل معدل التسرب الأمني للوثائق: (Data Breach Reduction)

- مراقبة وتتبع عمليات الوصول غير المصرح بها إلى الوثائق.
- استخدام حلول أمنية تقلل من احتمالية حدوث خروقات أمنية.

٢. زيادة موثوقية أنظمة الأرشيف الرقمية: (Reliability of Digital Archiving Systems)

- تعزيز أمان منصات الأرشيف من خلال استخدام أنظمة مقاومة للاختراق.
- تحسين إجراءات النسخ الاحتياطي لضمان استعادة الوثائق عند الحاجة.

٣. تحسين استراتيجيات إدارة الوثائق: (Document Management Strategies)

- تعزيز آليات التحقق من صحة الوثائق وسلامتها.
- تطبيق سياسات لحماية البيانات من الفقدان العرضي أو المتعمد.

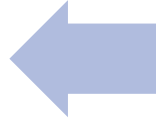
٤. التحكم في الوصول إلى الوثائق: (Document Access Control)

- تطبيق تقنيات التحقق من الهوية والمصادقة الثنائية لمنع الوصول غير المصرح به.
- تسجيل جميع العمليات على الوثائق الرقمية لضمان الشفافية والمراقبة.

٥. تحسين وعي الموظفين بالمخاطر الأمنية: (Security Awareness & Training)

- تنفيذ برامج تدريبية حول مخاطر أمن المعلومات الخاصة بالوثائق الرقمية.
- قياس مدى التزام الموظفين بإجراءات حماية الوثائق الرقمية وتقليل الأخطاء البشرية.

أبعاد المتغير الرئيسي (تطبيق معايير ISO 27001):



أبعاد المتغير التابع (الحد من مخاطر تسرب وفقدان الوثائق):

• إدارة المخاطر الأمنية (Risk Management)

• التحكم في الوصول إلى المعلومات (Access Control)

• التشفير وحماية البيانات (Data Encryption & Protection)

• إدارة استمرارية الأعمال والتعافي من الكوارث (BCP & DRP)

• الامتثال والتدقيق الأمني (Compliance & Security Audits)

• تقليل معدل التسرب الأمني للوثائق (Data Breach Reduction)

• زيادة موثوقية أنظمة الأرشيف الرقمية (Reliability of Digital Archiving Systems)

• تحسين استراتيجيات إدارة الوثائق (Document Management Strategies)

• التحكم في الوصول إلى الوثائق (Document Access Control)

• تحسين وعي الموظفين بالمخاطر الأمنية (Security Awareness & Training)

فروض الدراسة:

بناءً على مشكلة البحث وأهدافه، تم صياغة الفرضيات التالية لاختبار العلاقة بين تطبيق معايير ISO 27001 والحد من مخاطر تسرب وفقدان الوثائق المرقمنة والرقمية في تجمع الطائف الصحي.

الفرضية الرئيسية (H0)

لا يوجد تأثير ذو دلالة إحصائية لتطبيق معايير ISO 27001 على الحد من مخاطر تسرب وفقدان الوثائق المرقمنة والرقمية في تجمع الطائف الصحي.

الفرضية البديلة (H1)

يوجد تأثير ذو دلالة إحصائية لتطبيق معايير ISO 27001 على الحد من مخاطر تسرب وفقدان الوثائق المرقمنة والرقمية في تجمع الطائف الصحي.

ستتم اختبار هذه الفرضيات باستخدام التحليل الإحصائي عبر أسلوب الانحدار الخطي والمتعدد لقياس العلاقة بين تطبيق المعايير الأمنية وتأثيرها على الحد من المخاطر المتعلقة بالوثائق الرقمية في تجمع الطائف الصحي. فيما يلي نموذج جدولي يوضح العلاقة بين المتغير الرئيسي وأبعاده، مع التساؤل المقابل لكل بعد والفرضية المرتبطة به، بالإضافة إلى نموذج مماثل للمتغير التابع.

النموذج الجدولي للمتغير الرئيسي (تطبيق معايير ISO 27001)

المتغير الرئيسي (تطبيق معايير ISO 27001)	الأبعاد	التساؤل البحثي المقابل	الفرضية المقابلة
إدارة المخاطر الأمنية (Risk Management)	تقييم وتحليل المخاطر المحتملة لتسرب أو فقدان الوثائق	ما مدى فعالية تطبيق معايير ISO 27001 في تقييم وتحليل المخاطر الأمنية المتعلقة بتسرب وفقدان الوثائق الرقمية؟	H1: يوجد تأثير ذو دلالة إحصائية بين تطبيق معايير ISO 27001 وتحسين إدارة المخاطر الأمنية وتقليل احتمالية تسرب أو فقدان الوثائق الرقمية.
التحكم في الوصول إلى المعلومات (Access Control)	ضبط صلاحيات المستخدمين وفق مبدأ "الحد الأدنى من الامتيازات"	كيف يؤثر تطبيق ضوابط التحكم في الوصول وفق معايير ISO 27001 على تقليل احتمالية الوصول غير المصرح به للوثائق الرقمية؟	H2: يوجد تأثير ذو دلالة إحصائية بين تطبيق ضوابط التحكم في الوصول وفق معايير ISO 27001 والحد من الوصول غير المصرح به للوثائق الرقمية.
التشفير وحماية البيانات (Data Encryption & Protection)	استخدام تقنيات التشفير لتأمين الوثائق الرقمية	إلى أي مدى يساهم استخدام تقنيات التشفير وحماية البيانات في تحسين أمان الوثائق الرقمية في تجمع الطائف الصحي؟	H3: يوجد تأثير ذو دلالة إحصائية بين تطبيق تقنيات التشفير وفق معايير ISO 27001 وتقليل مخاطر تسرب وفقدان الوثائق الرقمية.

إدارة استمرارية الأعمال والتعافي من الكوارث (BCP & DRP)	تطوير خطط طوارئ لضمان استعادة الوثائق الرقمية في حالات الطوارئ	ما مدى تأثير خطط استمرارية الأعمال والتعافي من الكوارث وفق معايير ISO 27001 على حماية الوثائق الرقمية من فقدان؟	H4: يوجد تأثير ذو دلالة إحصائية بين تطبيق خطط استمرارية الأعمال والتعافي من الكوارث وفق معايير ISO 27001 وتقليل احتمالية فقدان الوثائق الرقمية.
الامتثال والتدقيق الأمني (Compliance & Security Audits)	إجراء مراجعات دورية لضمان تطبيق الإجراءات الأمنية	كيف يؤثر إجراء التدقيق الأمني المستمر وفق معايير ISO 27001 على تحسين أمن الوثائق الرقمية؟	H5: يوجد تأثير ذو دلالة إحصائية بين التدقيق الأمني المستمر وفق معايير ISO 27001 وتحسين مستوى أمان الوثائق الرقمية في المؤسسات الصحية.

النموذج الجدولي للمتغير التابع (الحد من مخاطر تسرب وفقدان الوثائق)

المتغير التابع (الحد من مخاطر تسرب وفقدان الوثائق)	الأبعاد	التساؤل البحثي المقابل	الفرضية المقابلة
تقليل معدل التسرب الأمني للوثائق (Data Breach Reduction)	تنفيذ أنظمة مراقبة متقدمة لرصد أي وصول غير مصرح به	كيف يساهم تطبيق معايير ISO 27001 في الحد من تسرب الوثائق الرقمية من خلال تقنيات الحماية والرصد المستمر؟	H6: يوجد تأثير ذو دلالة إحصائية بين تطبيق معايير ISO 27001 وتقليل مخاطر تسرب الوثائق الرقمية من خلال أنظمة المراقبة الأمنية.
زيادة موثوقية أنظمة الأرشفة الرقمية (Reliability of Digital Archiving Systems)	تحسين أمان منصات الأرشفة من خلال استخدام تقنيات متقدمة	إلى أي مدى يساهم تطبيق معايير ISO 27001 في تحسين أداء وموثوقية أنظمة الأرشفة الرقمية وتقليل فقدان الوثائق؟	H7: يوجد تأثير ذو دلالة إحصائية بين تطبيق معايير ISO 27001 وتعزيز موثوقية أنظمة الأرشفة الرقمية وتقليل احتمالات فقدان الوثائق.
تحسين استراتيجيات إدارة الوثائق (Document Management Strategies)	تطبيق سياسات صارمة لحماية الوثائق من الضياع أو التلف	كيف يمكن لاستراتيجيات إدارة الوثائق وفق معايير ISO 27001 أن تعزز من أمن الوثائق الرقمية وتقليل فقدانها؟	H8: يوجد تأثير ذو دلالة إحصائية بين استراتيجيات إدارة الوثائق وفق معايير ISO 27001 وتقليل مخاطر فقدان الوثائق الرقمية.
التحكم في الوصول إلى الوثائق (Document Access Control)	استخدام أنظمة تحقق من الهوية لمنع الوصول غير المصرح به	ما مدى تأثير ضوابط الوصول المطبقة وفق ISO 27001 على تحسين التحكم في إدارة الوثائق الرقمية ومنع فقدانها؟	H9: يوجد تأثير ذو دلالة إحصائية بين تطبيق ضوابط الوصول وفق ISO 27001 وتقليل احتمالية فقدان الوثائق الرقمية بسبب الوصول غير المصرح به.

تحسين وعي الموظفين بالمخاطر الأمنية (Security Awareness & Training)	تنفيذ برامج تدريبية لتعزيز أمن المعلومات	كيف يؤثر تدريب الموظفين على معايير ISO 27001 في تعزيز أمن الوثائق الرقمية وتقليل الأخطاء البشرية التي قد تؤدي إلى فقدانها أو تسريبها؟	H10: يوجد تأثير ذو دلالة إحصائية بين تدريب الموظفين على معايير ISO 27001 وتقليل فقدان الوثائق الرقمية الناتج عن الأخطاء البشرية.
--	---	---	---

تساعد هذه الفرضيات في اختبار العلاقة بين تطبيق معايير ISO 27001 وتأثيرها على الحد من مخاطر تسرب وفقدان الوثائق الرقمية في تجمع الطائف الصحي، مما يسهم في تقديم نتائج واضحة تدعم التوصيات المستقبلية.

الدراسات السابقة:

تعتبر معايير ISO 27001 من أهم المعايير المعتمدة عالميًا لإدارة أمن المعلومات، وهي تلعب دورًا محوريًا في حماية الوثائق والمحفوظات الرقمية من التسرب أو الفقدان. العديد من الدراسات تناولت هذه المعايير وتأثيرها على الأمن السيبراني وإدارة المخاطر، ومن بين هذه الدراسات:

دراسة (ميلاد، ٢٠١٢) تناولت الدراسة مفهوم المعلوماتية في الوثائق الجارية والتاريخية وأهمية المعيار لتحقيق الجودة الشاملة، وقدمت ترجمة لجزءي المعيار وشروحًا وأمثلة على كيفية التطبيق، وأخيرًا دراسة لأهم الأنشطة الأرشيفية الأساسية وفي مقدمتها خطة التصنيف واستبعاد الوثائق وتحديد مدد الحفظ والأمن والإتاحة، وقد تحقق الهدف من الدراسة وظهرت مجموعة من الدراسات التي تناولت جوانب تطبيق المعيار في أكثر من مؤسسة، منها على سبيل المثال دراسة (البصري، ٢٠١٤) بعنوان: "السياسة الوطنية لإدارة الوثائق والمحفوظات بسلطنة عمان في ضوء المعايير الدولية في المجال" واستعرضت مدى تطبيق مبادئ المعيار (ISO ١٥٤٨٩) من قبل الهيئة الوطنية للوثائق والمحفوظات بصفقتها المستولة عن نظام إدارة الوثائق في كافة مؤسسات السلطنة، وكان أحدثها دراسة (خليفة و هندي، ٢٠٢٠) بعنوان: "مدى مطابقة الأرشيف الإلكتروني بمشيخة الأزهر الشريف لمعيار ISO ١٥٤٨٩: دراسة حالة" حيث سعت الدراسة إلى قياس مدى إمكانية تطبيق المعيار (ISO ١٤٥٨٩) على نظام إدارة الوثائق الإلكترونية بالمشيخة، وخلصت إلى وجود أرضية جيدة من الممارسات الأرشيفية والعناصر التي يتضمنها النظام الإلكتروني يمكن من خلالها الشروع في تطبيق المعيار.

أوضحت دراسة Meissonnier & Roques (٢٠١٥) أن نظم إدارة المحتوى التي تتبنى معايير ISO تحقق مستوى أمان أعلى، مما يساهم في تحسين إدارة الوثائق وتقليل الفقدان والتسرب. تشير الدراسات السابقة إلى أن تطبيق معايير ISO 27001 يلعب دورًا أساسيًا في تعزيز أمن الوثائق الرقمية وتقليل المخاطر المرتبطة بها. كما أن الالتزام بهذه المعايير يساعد المؤسسات على تحقيق بيئة آمنة وموثوقة، مما يساهم في تسهيل الوصول إلى الوثائق وحمايتها من الفقدان أو الاختراقات الأمنية.

يمكن للدراسة الحالية أن تبني على هذه النتائج من خلال تحليل تطبيق معايير ISO 27001 في تجمع الطائف الصحي، وقياس مدى تأثيرها على تقليل المخاطر الأمنية وتحسين إدارة الوثائق المرقمنة والرقمية.

المنطلقات النظرية للدراسة:

تمثل المنطلقات النظرية الإطار العلمي والمفاهيمي الذي تستند إليه هذه الدراسة لفهم وتحليل أثر تطبيق معايير ISO 27001 على الحد من مخاطر تسرب وفقدان الوثائق المرقمنة والرقمية في تجمع الطائف الصحي. وتشمل هذه المنطلقات مجموعة من المفاهيم والنظريات التي توضح أسس إدارة أمن المعلومات، وإدارة المخاطر، وأنظمة الأرشفة الرقمية، وحوكمة البيانات، ودور التكنولوجيا الحديثة في تأمين الوثائق.

1. مفهوم أمن المعلومات وإدارة المخاطر

يُعد أمن المعلومات من أهم المجالات التي تهتم بها المؤسسات في العصر الرقمي، ويهدف إلى حماية البيانات من الوصول غير المصرح به، أو التعديل، أو التلف، أو الفقدان. وفقًا لمنظمة المعايير الدولية (ISO)، يعتمد أمن المعلومات على ثلاثة محاور رئيسية، تعرف بمثلث CIA:

- **السرية (Confidentiality):** ضمان عدم وصول المعلومات إلا للأشخاص المصرح لهم.
- **التكاملية (Integrity):** الحفاظ على دقة المعلومات وعدم تعديلها بشكل غير مصرح به.
- **التوافر (Availability):** التأكد من أن المعلومات متاحة عند الحاجة إليها.

من ناحية أخرى، تهدف إدارة المخاطر إلى تحديد وتحليل وتقييم المخاطر التي قد تؤثر على الوثائق الرقمية، ثم اتخاذ الإجراءات اللازمة للحد من تأثيرها. تشمل المخاطر المحتملة:

- **المخاطر التقنية:** مثل الهجمات السيبرانية وفقدان البيانات بسبب أعطال النظام.
- **المخاطر البشرية:** مثل الأخطاء البشرية أو سوء الاستخدام للأنظمة.
- **المخاطر البيئية:** مثل الحرائق أو الكوارث الطبيعية التي قد تؤثر على التخزين الرقمي.

2. معايير ISO 27001 وإدارة أمن المعلومات

تمثل ISO 27001 أحد أهم المعايير الدولية المعتمدة لإدارة أمن المعلومات، حيث توفر إطارًا متكاملًا لتحديد وتنفيذ وإدارة وتحسين سياسات أمن المعلومات داخل المؤسسات. يهدف هذا المعيار إلى:

- **تقييم المخاطر الأمنية المتعلقة بالوثائق الرقمية والمحفوظات الإلكترونية.**
- **تنفيذ سياسات وإجراءات أمنية لحماية الوثائق الرقمية.**
- **ضمان استمرارية الأعمال من خلال استراتيجيات النسخ الاحتياطي واستعادة البيانات.**
- **إجراء تدقيق دوري لأنظمة الأمن والتأكد من فعاليتها.**

وفقًا لمنظمة ISO، فإن تطبيق هذا المعيار يساعد المؤسسات الصحية على تعزيز حماية الوثائق الطبية والإدارية من التسرب أو الفقدان، وبالتالي تحسين مستوى الأمان الرقمي.

3. العلاقة بين تطبيق معايير ISO 27001 والحد من مخاطر تسرب وفقدان الوثائق

يؤثر تطبيق ISO 27001 بشكل مباشر على تقليل المخاطر المتعلقة بالوثائق الرقمية من خلال:

- تقنيات التشفير: لضمان حماية البيانات أثناء التخزين والنقل.
- إجراءات التحكم في الوصول: لمنع أي تعديلات أو اختراقات غير مصرح بها.
- إدارة استمرارية الأعمال: لتقليل أثر الكوارث على فقدان الوثائق الرقمية.
- رفع وعي الموظفين: عبر برامج التدريب المستمرة حول الأمن السيبراني.

تشير الدراسات إلى أن تطبيق ISO 27001 يقلل من معدل التسريبات الرقمية بنسبة 40-60% في المؤسسات التي تتبع سياسات أمنية صارمة.

4. أنظمة الأرشيف الرقمية وإدارة الوثائق

تعتمد المؤسسات الحديثة على أنظمة الأرشيف الرقمية كوسيلة لتحسين تخزين الوثائق واسترجاعها بأمان. ومن بين أهم التقنيات المستخدمة:

- أنظمة إدارة المحتوى المؤسسي (ECM) التي تسمح بأتمة تخزين الوثائق وأرشفتها وفقاً لمعايير الأمان.
 - أنظمة التوقيع الرقمي: التي توفر طبقة إضافية من الحماية ضد التلاعب بالمستندات.
 - تقنيات الذكاء الاصطناعي: التي تساعد في تصنيف الوثائق واكتشاف التهديدات الأمنية المحتملة.
- يعد تطبيق معايير ISO 27001 في هذه الأنظمة أمراً بالغ الأهمية لضمان أمن الوثائق والحفاظ على سرية المعلومات.

5. حوكمة البيانات ودورها في تعزيز أمن الوثائق الرقمية

حوكمة البيانات تعني وضع إطار تنظيمي يحدد كيفية إدارة البيانات داخل المؤسسة. تشمل أهداف حوكمة البيانات:

وضع سياسات موحدة لحماية الوثائق الرقمية.

تحديد صلاحيات الوصول ومسؤوليات الأفراد عن البيانات الرقمية.

الامتثال للمتطلبات القانونية والتنظيمية الدولية والمحلية.

تساعد حوكمة البيانات في تحقيق التوافق مع معايير ISO 27001 من خلال تحديد الضوابط الأمنية والإجراءات اللازمة لحماية الوثائق.

6. التحديات التي تواجه تطبيق معايير ISO 27001 في المؤسسات الصحية

على الرغم من الفوائد الكبيرة لتطبيق ISO 27001، إلا أن هناك بعض التحديات التي قد تعيق التنفيذ الفعال لهذه المعايير، مثل:

١. ارتفاع تكلفة التنفيذ: حيث تتطلب معايير الأمان الحديثة استثمارات مالية كبيرة في الأنظمة التكنولوجية والتدريب.

٢. مقاومة التغيير من قبل الموظفين: بعض العاملين يواجهون صعوبة في التكيف مع الأنظمة الأمنية الصارمة.

٣. تعقيد أنظمة الحماية: قد يكون تنفيذ معايير ISO 27001 معقدًا عند دمجها مع الأنظمة القائمة في المؤسسات الصحية.

٤. نقص الكفاءات المتخصصة: يتطلب تطبيق ISO 27001 وجود كوادر مدربة في إدارة أمن المعلومات والأرشفة الرقمية.

7. دور الإدارة العليا في دعم تطبيق معايير ISO 27001

يلعب دعم الإدارة العليا دورًا حاسمًا في نجاح تطبيق ISO 27001 من خلال:

- وضع استراتيجية واضحة لحماية الوثائق الرقمية.
- توفير الموارد المالية والتقنية المطلوبة لتنفيذ أنظمة الأمان.
- تدريب الموظفين ورفع مستوى الوعي حول أهمية أمن المعلومات.
- إجراء تقييم دوري لمدى التزام المؤسسة بمعايير الأمن السيبراني.

أظهرت الدراسات أن دعم الإدارة العليا يزيد من معدل الامتثال لمعايير الأمان بنسبة ٧٠% في المؤسسات التي تطبق سياسات صارمة.

8. أهمية التشفير والنسخ الاحتياطي في حماية الوثائق الرقمية

تعد تقنيات التشفير والنسخ الاحتياطي من أهم الأساليب المستخدمة لحماية الوثائق الرقمية، وتشمل:

- التشفير المتماثل وغير المتماثل: لضمان عدم قدرة الأطراف غير المصرح بها على قراءة البيانات.
- التوقيع الإلكتروني: للتحقق من صحة الوثائق وسلامتها من التعديل.
- النسخ الاحتياطي الدوري: لضمان استعادة البيانات في حالات الطوارئ مثل الهجمات الإلكترونية.

تشير الدراسات إلى أن المؤسسات التي تعتمد على تقنيات التشفير والنسخ الاحتياطي تقلل من احتمالات فقدان الوثائق بنسبة ٨٠% مقارنة بالمؤسسات التي لا تستخدم هذه التقنيات.

المنهجية وطرق البحث:

تعتمد الدراسة على المنهج الوصفي التحليلي (Descriptive-Analytical Approach) ، حيث تم استخدام الأساليب الكمية لجمع وتحليل البيانات، وذلك لدراسة العلاقة بين تطبيق معايير ISO 27001 ومدى تأثيرها على أمن الوثائق الرقمية في بيئة الرعاية الصحية.

يُعد المنهج الوصفي مناسباً لهذه الدراسة، حيث يسمح بوصف الوضع الحالي لتطبيق معايير ISO 27001 ، بينما يساعد التحليل الإحصائي على اختبار الفرضيات وتحديد العلاقات بين المتغيرات.

طرق جمع البيانات (Data Collection Methods)

تم الاعتماد على المصادر الأولية والثانوية لجمع البيانات:

المصادر الأولية (Primary Data):

تمثلت في تطوير استبيان بحثي موجه إلى موظفي تجمع الطائف الصحي الذين يتعاملون مع الوثائق الرقمية والإجراءات الأمنية المتعلقة بها.

المصادر الثانوية (Secondary Data):

جمع بيانات من أدبيات بحثية، دراسات سابقة، تقارير رسمية، معايير ISO 27001، ووثائق داخلية من تجمع الطائف الصحي لتعزيز دقة وتكامل الدراسة.

أدوات الدراسة :

تعتمد هذه الدراسة على مجموعة من الأدوات البحثية التي تهدف إلى جمع البيانات وتحليلها بدقة من أجل قياس أثر تطبيق معايير ISO 27001 على الحد من مخاطر تسرب وفقدان الوثائق المرقمنة والرقمية في تجمع الطائف الصحي. تم اختيار الأدوات البحثية بعناية لضمان موثوقية النتائج ودقتها، وقد تم تقسيمها إلى أدوات لجمع البيانات وأخرى لتحليلها، كما يلي:

أولاً: أدوات جمع البيانات

تعتمد الدراسة على النهج الكمي باستخدام الاستبيان كأداة رئيسية لجمع البيانات، حيث يوفر معلومات كمية قابلة للمقاييس حول مدى تطبيق معايير ISO 27001 ومدى تأثيرها على أمن الوثائق الرقمية. وتم تصميم الاستبيان استناداً إلى الأدبيات السابقة والممارسات المعتمدة في مجال إدارة أمن المعلومات والأرشفة الرقمية.

الاستبيان (Questionnaire)

تم تصميم الاستبيان وفق مقياس ليكرت الخماسي لقياس آراء المشاركين حول تأثير تطبيق معايير ISO 27001 على أمن الوثائق الرقمية، ويشمل الأسئلة التالية:

الجزء الأول: البيانات الديموغرافية

- تهدف إلى تحديد خصائص العينة (المسمى الوظيفي، الخبرة، المؤهل العلمي، وغيرها).

الجزء الثاني: قياس المتغير الرئيسي (تطبيق معايير ISO 27001)

- يحتوي على أسئلة تقيس مدى تطبيق معايير الأمن السيبراني مثل إدارة المخاطر الأمنية، التحكم في الوصول، التشفير، خطط استمرارية الأعمال، والتدقيق الأمني.

الجزء الثالث: قياس المتغير التابع (الحد من مخاطر تسرب وفقدان الوثائق الرقمية)

- يشمل أسئلة تقيس مدى تأثير تطبيق معايير ISO 27001 على تقليل تسرب الوثائق الرقمية، زيادة موثوقية أنظمة الأرشفة، تحسين سياسات إدارة الوثائق، تعزيز ضوابط الوصول، ورفع وعي الموظفين بالمخاطر الأمنية.

تم توزيع الاستبيان إلكترونياً على موظفي تجمع الطائف الصحي، وتم التأكد من صلاحية وموثوقية الأسئلة قبل التوزيع من خلال مراجعات الخبراء.

ثانياً: أدوات تحليل البيانات

بعد جمع البيانات، تم استخدام التحليل الإحصائي لاختبار فرضيات الدراسة وقياس العلاقة بين تطبيق معايير ISO 27001 والحد من مخاطر تسرب وفقدان الوثائق الرقمية.

البرنامج الإحصائي (SPSS (Statistical Package for the Social Sciences)

تم الاستعانة ببرنامج SPSS لإجراء التحليلات الإحصائية التالية:

♦ التحليل الوصفي: (Descriptive Analysis)

- تحليل التوزيع التكراري والنسب المئوية لعينة الدراسة لفهم خصائص المستجيبين.
- وصف المتغيرات البحثية والتأكد من مستوى تطبيق معايير ISO 27001.

♦ اختبارات الصدق والثبات: (Validity & Reliability Tests)

- اختبار ألفا كرونباخ (Cronbach's Alpha) لقياس ثبات الاستبيان وموثوقية الأسئلة.
- تم التأكد من أن معاملات الثبات أكبر من 0.7 مما يشير إلى موثوقية الأداة البحثية.

♦ تحليل الارتباط: (Correlation Analysis)

- قياس العلاقة بين تطبيق معايير ISO 27001 والمتغيرات التابعة، لمعرفة قوة واتجاه العلاقة بين المتغيرات.

♦ تحليل الانحدار الخطي البسيط والمتعدد: (Simple & Multiple Linear Regression)

- تم استخدام الانحدار الخطي البسيط لاختبار تأثير ISO 27001 على أمن الوثائق الرقمية.
- تم استخدام الانحدار الخطي المتعدد لقياس مدى تأثير كل بُعد من أبعاد ISO 27001 على أمن الوثائق الرقمية.

♦ اختبار الدلالة الإحصائية: (Significance Tests)

- اختبار القيمة الاحتمالية (p-value) لتحديد ما إذا كان التأثير دال إحصائياً أم لا.

ثالثاً: مراجعة الأدبيات السابقة والمصادر الثانوية

إلى جانب الاستبيان والتحليل الإحصائي، اعتمدت الدراسة على المصادر الثانوية لدعم الإطار النظري، وشملت: الدراسات السابقة: تم الاطلاع على أبحاث تناولت أمن المعلومات، معايير ISO 27001، وأثرها على حماية الوثائق الرقمية.

المعايير والتقارير الرسمية: مراجعة تقارير ومعايير ISO 27001 الصادرة عن المنظمة الدولية للمعايير (ISO).
المراجع الأكاديمية: الاستعانة بمصادر علمية حول إدارة المخاطر وأمن الوثائق الرقمية.
الأنظمة والتشريعات: الاطلاع على التشريعات والسياسات المحلية والدولية المتعلقة بأمن الوثائق الرقمية في القطاع الصحي.

رابعاً: مقابلات شبه منظمة (Semi-Structured Interviews) (اختياري)

في بعض الحالات، تم دعم البيانات الكمية من خلال مقابلات مع متخصصين في إدارة أمن المعلومات والأرشفة الرقمية داخل تجمع الطائف الصحي. تهدف هذه المقابلات إلى فهم التحديات الواقعية التي تواجه تطبيق معايير ISO 27001 والحلول المحتملة لتعزيز أمن الوثائق الرقمية.

ملخص أدوات الدراسة

الأداة	الوصف	الهدف
الاستبيان (Questionnaire)	استبيان مكون من 3 أقسام لتقييم تطبيق معايير ISO 27001 وأثرها على أمن الوثائق الرقمية	جمع بيانات كمية من عينة الدراسة حول مستوى تطبيق المعايير والتحديات المرتبطة بها
التحليل الإحصائي (SPSS)	تحليل البيانات من خلال التحليل الوصفي، اختبار الصدق والثبات، تحليل الارتباط والانحدار الخطي	اختبار الفرضيات وقياس قوة العلاقة بين المتغيرات
مراجعة الأدبيات السابقة	الاطلاع على الدراسات السابقة، المعايير الدولية، والمصادر الأكاديمية حول أمن المعلومات	بناء الإطار النظري وتعزيز تفسير النتائج
المقابلات (اختياري)	مقابلات مع متخصصين في أمن المعلومات	فهم التحديات الفعلية والتوصيات العملية

ساهمت أدوات الدراسة المختارة في تحقيق تكامل بين الأساليب الكمية والنوعية لضمان تقديم نتائج دقيقة وموثوقة حول أثر تطبيق معايير ISO 27001 على أمن الوثائق الرقمية في تجمع الطائف الصحي. ومن خلال التحليل الإحصائي المتقدم باستخدام SPSS، تمكنت الدراسة من اختبار الفرضيات المطروحة وتحديد نقاط القوة والضعف في تطبيق المعايير، مما يعزز من إمكانية تعميم نتائج البحث على مؤسسات صحية أخرى تواجه تحديات مشابهة في مجال أمن الوثائق الرقمية.

حدود الدراسة :

تمثل حدود الدراسة مجموعة من العوامل التي تحد من تعميم النتائج المستخلصة من البحث، وتحدد نطاق تطبيق هذه النتائج. وتكمن أهمية توضيح هذه الحدود في إعطاء صورة واقعية عن قدرات الدراسة في تمثيل الظاهرة المدروسة، وكذلك في تمهيد الطريق لدراسات مستقبلية أكثر شمولية وتوسعاً. وبناءً على طبيعة الدراسة الحالية حول أثر تطبيق معايير ISO 27001 على الحد من مخاطر تسرب وفقدان الوثائق المرقمنة والرقمية في تجمع الطائف الصحي، يمكن تلخيص هذه الحدود فيما يلي:

أولاً: الحدود الموضوعية:

تتعلق الحدود الموضوعية بالتركيز على دراسة أثر تطبيق معايير أمن المعلومات ISO 27001 في القطاع الصحي، وتحديدًا تجمع الطائف الصحي، وعلى مخاطر تسرب أو فقدان الوثائق الرقمية والمرقمنة. وبالتالي، لم تشمل هذه الدراسة قطاعات أخرى قد تختلف في احتياجاتها الأمنية أو معايير التطبيق المتبعة لديها. إن نتائج هذه الدراسة قد لا تكون قابلة للتعميم بشكل كامل على المؤسسات التي تختلف بشكل جوهري في أنشطتها وطبيعة البيانات التي تتعامل معها.

ثانيًا: الحدود المكانية:

تقتصر هذه الدراسة على تجمع الطائف الصحي بوصفه المجال المكاني المحدد لها. حيث أن تجمع الطائف الصحي يتمتع بخصائص إدارية وتنظيمية وتقنية خاصة به، ما يجعل النتائج مرتبطة بسياقه الخاص، وبالتالي قد تختلف النتائج إذا طبقت الدراسة على تجمعات صحية أو مستشفيات أخرى في مناطق جغرافية مختلفة، نظرًا لاختلاف الموارد، والبنى التحتية التكنولوجية، والسياسات المتبعة.

ثالثًا: الحدود الزمنية:

تمت الدراسة خلال عام ٢٠٢٥، مما يعني أن النتائج تعكس الوضع الراهن لتطبيق معايير ISO 27001 خلال هذه الفترة.

مع التطورات المستمرة في مجال الأمن السيبراني وتقنيات إدارة الوثائق الرقمية، قد تتغير نتائج البحث إذا تم إجراؤه في فترة مستقبلية مختلفة، حيث يمكن أن تظهر تقنيات جديدة تؤثر على إدارة الوثائق الرقمية.

رابعًا: الحدود البشرية (العينة المدروسة):

تمثل الحدود البشرية أحد الجوانب الأساسية التي يجب مراعاتها، حيث اعتمدت هذه الدراسة على عينة من الموظفين في تجمع الطائف الصحي، والتي تشمل العاملين في الإدارات التقنية، والإدارية، والطبية، وغيرها من الإدارات ذات العلاقة المباشرة بإدارة الوثائق الرقمية. ونظرًا لأن حجم العينة وطبيعة اختيارها يؤثر بشكل كبير على دقة النتائج وإمكانية تعميمها، فإن نتائج هذه الدراسة قد لا تعكس بالضرورة آراء جميع موظفي التجمع أو موظفي المؤسسات الصحية الأخرى بشكل كامل.

خامسًا: الحدود المنهجية:

اعتمدت الدراسة على المنهج الكمي من خلال استخدام الاستبيانات والتحليل الإحصائي كأداة أساسية لجمع البيانات

وتحليلها. وبالرغم من دقة هذا المنهج وقدرته على تقديم نتائج كمية واضحة، إلا أنه قد لا يوفر تفاصيل كافية حول الأسباب النوعية أو الظروف التي أدت إلى نتائج معينة. وقد تكون هناك حاجة لاستخدام مناهج أخرى (مثل المقابلات المعمقة أو دراسات الحالة) مستقبلاً للحصول على فهم أكثر عمقاً لأبعاد المشكلة.

سادساً: حدود الأدوات المستخدمة:

استخدمت الدراسة أداة الاستبيان كوسيلة أساسية لجمع البيانات، وهي أداة تعتمد بشكل كبير على دقة استجابة المشاركين وصدق إجاباتهم. ومن الممكن أن تتأثر الإجابات بالتحيز الشخصي، أو عدم فهم الأسئلة بشكل كامل، أو قلة وعي المشاركين ببعض الجوانب التقنية والتخصصية، مما قد يؤدي إلى تباين في النتائج. كما أن الدراسة لم تستخدم أدوات بحثية نوعية، مثل المقابلات المفتوحة، التي قد توفر معلومات إضافية تفسر النتائج.

سابعاً: حدود التمويل والموارد المتاحة:

قد تواجه الدراسة حدوداً مرتبطة بالموارد المالية والبشرية والتقنية المتاحة، مما قد يؤثر على إمكانية استخدام تقنيات أكثر تطوراً أو إجراء تحليل أكثر عمقاً. وفي هذه الدراسة تحديداً، قد يؤثر عدم توفر الموارد الكافية على قدرة الباحث على توسيع نطاق العينة أو إجراء اختبارات إضافية.

في ضوء هذه الحدود، توصي الدراسة بإجراء مزيد من البحوث المستقبلية لتجاوز هذه الحدود من خلال توسيع النطاق الزمني، وزيادة حجم وتنوع العينة، واستخدام أدوات بحثية إضافية، مما يساهم في تعزيز إمكانية تعميم النتائج وتوفير فهم أعمق لظاهرة أمن الوثائق الرقمية وفقاً لمعايير ISO 27001 في القطاع الصحي.

المراجع:

- علام & ناهد علام. (٢٠٢٣). البرامج الآلية لإدارة الوثائق والأرشيف: مفاهيم وقضايا. *المجلة العلمية للمكتبات و الوثائق و المعلومات*, 5(13.2), 202-226.
- د/بوفاس الشريف, & أ/طلحي فاطمة الزهراء. (٢٠١٤). نحو بناء نظم لإدارة حماية المعلومات ISO27001 في المؤسسات الجزائرية. In *الملتقى الدولي الثاني حول اليقظة الإستراتيجية و نظم المعلومات في المؤسسة الإقتصادية*.
- Meissonnier, A., & Roques, R. (2015). L'archiviste, les normes et le droit. *La Gazette des archives*, 240(4), 135-151.
- بسمة بصير. (٢٠١٩). السياسة الوطنية لإدارة والمحفوظات الوثائق بسلطنة عمان في ضوء المعايير الدولية في المجال. *Revue maghrébine de documentation et d'information*, (٢٧), ٢٢-٧.
- أسامة محسن هندي, & بهاء فتحي خليفة. (٢٠٢٠). ISO مدى مطابقة الأرشيف الإلكتروني بمشيخة الأزهر الشريف لمعيار ١٥٤٨٩ دراسة حالة. *Information (AJADI) & Arab Journal for Archives, Documentation*, ٤٧.
- ميلاد, & سلوى على. (٢٠١٢). الجودة الشاملة في الأرشيف لماذا؟ وكيف؟. *بحوث في علم المكتبات و المعلومات*, ٩ (سبتمبر), ٨٥-٥١.

-Meissonnier, A., & Roques, R. (2015). L'archiviste, les normes et le droit. *La Gazette des archives*, 240(4), 135-151.