

عنوان الدراسة

"أثر تطبيق معايير ISO 27001 على الحد من مخاطر تسرب وفقدان الوثائق الرقمية: دراسة تطبيقية على
تجمع الطائف الصحي في المملكة العربية السعودية"

The Impact of Implementing ISO 27001 Standards on Mitigating the Risks of "
Digital Document Leakage and Loss: A Case Study of the Taif Health Cluster in
"Saudi Arabia

إعداد الطالب/فهد بن رجاء الله الثبيتي

2021202249

ماجستير إدارة المخاطر

إشراف/

د. الفصيل عبد الحميد

د. فايز جراد

العام الدراسي:

٢٠٢٥

حقوق الطباعة – Copyright notice

جميع حقوق الطبع والنشر المتعلقة بهذه الرسالة محفوظة لجامعة ميدأوشن، ولا يجوز نسخها، أو إعادة طباعتها، أو نشرها بأي وسيلة دون الحصول على إذن خطي مسبق من الجامعة.

المستخلص

الهدف:

سعت هذه الدراسة إلى استقصاء مدى إسهام تطبيق معايير ISO 27001 في الحد من مخاطر تسرب وفقدان الوثائق الرقمية والمقرنة في بيئة تجمع الطائف الصحي، وذلك من خلال تحليل العلاقة بين ممارسات أمن المعلومات المعتمدة وفقاً لهذه المعايير، وبين فعالية الأنظمة والإجراءات المؤسسية في حماية الوثائق.

المنهجية:

اعتمدت الدراسة على المنهج الوصفي التحليلي بهدف قياس العلاقة بين تطبيق معايير ISO 27001 ومستوى الحد من مخاطر تسرب وفقدان الوثائق. وقد تم استخدام الاستبانة كأداة رئيسية لجمع البيانات من عينة مكونة من (٦٤) موظفاً وموظفة من مختلف قطاعات تجمع الطائف الصحي.

النتائج:

أظهرت نتائج الدراسة وجود علاقة ارتباط إيجابية ذات دلالة إحصائية بين تطبيق معايير ISO 27001 والحد من مخاطر تسرب وفقدان الوثائق الرقمية والمقرنة، حيث بلغ معامل الارتباط (٠.٦١٢) عند مستوى دلالة (٠.٠١). كما بينت التحليلات الإحصائية أن هناك اتجاهاً إيجابياً لدى المشاركين نحو تطبيق تلك المعايير في بيئة عملهم، وخاصة في مجالات التحكم في الوصول، واستمرارية الأعمال، والتشفير، والامتثال الأمني. ووفقاً لتحليل الفرضيات، فإن تطبيق المعايير يسهم بشكل فعال في تقليل الحوادث الأمنية وتعزيز موثوقية الأرشفة ورفع وعي الموظفين بسياسات أمن المعلومات.

التوصيات:

أوصت الدراسة بضرورة تعزيز تطبيق معايير ISO 27001 بشكل مؤسسي ومنهجي في جميع أقسام تجمع الطائف الصحي، وتكثيف برامج التوعية والتدريب الأمني للموظفين، خاصة في الجوانب المتعلقة بحماية الوثائق الرقمية. كما دعت إلى تطوير البنية التحتية التقنية وتعزيز أدوات التشفير والتحكم في الوصول، بالإضافة إلى مراجعة وتحديث السياسات الأمنية بشكل دوري لضمان استمرارية حماية الوثائق وتقليل احتمالات التسرب أو الفقدان.

الكلمات المفتاحية:

ISO 27001، أمن المعلومات، الوثائق الرقمية، تسرب الوثائق، فقدان الوثائق، الحوكمة الرقمية، تجمع الطائف الصحي، إدارة الوثائق والمحفوظات.

Abstract

Purpose:

This study aimed to examine the extent to which the application of ISO 27001 standards contributes to reducing the risks of digital and digitized document leakage and loss within the Taif Health Cluster. The objective was to assess the relationship between information security practices aligned with ISO 27001 and the institutional effectiveness in protecting documents.

Methodology:

The study employed a **descriptive analytical approach**, using a structured questionnaire to collect data from a purposive sample of 64 employees. Data were analyzed using SPSS software, applying reliability and validity tests, descriptive statistics, correlation coefficients, and hypothesis testing to determine the statistical significance of the relationships between variables.

Findings:

The results revealed a **statistically significant positive correlation** between the implementation of ISO 27001 standards and the reduction of document leakage and loss risks (correlation coefficient = 0.612, $p < 0.01$). Participants demonstrated a positive attitude toward the application of these standards, particularly in areas such as access control, disaster recovery, encryption, and compliance. The analysis confirmed that applying these standards enhances security reliability, reduces security incidents, and improves employee awareness of data protection policies.

Recommendations:

The study recommends **institutionalizing the implementation of ISO 27001 standards**, strengthening employee training programs on information security, upgrading technical infrastructure, and regularly reviewing security policies to ensure continuous protection of digital documents and minimize the risks of leakage or loss.

Keywords:

ISO 27001, Information Security, Digital Documents, Document Leakage, Document Loss, Digital Governance, Taif Health Cluster, Records and Archives Management

الشكر والتقدير

تحية طيبة،

بدايةً أحمد الله سبحانه وتعالى حمداً كثيراً مباركاً على ما منَّ به عليّ من إتمام هذه الدراسة، راجياً منه سبحانه أن يكون هذا الجهد المتواضع نافعا ومفيداً.

ثم أتقدم بخالص الشكر والتقدير إلى مُشرفيَّ الكريمين، اللذين كان لهما بالغ الأثر في إخراج هذه الدراسة بالصورة التي هو عليها، من خلال توجيهاتهما السديدة، وملاحظاتهما القيمة، ودعمهما المستمر لي خلال كافة مراحل إعداد الدراسة.

كما يسرني أن أتوجه بجزيل الشكر والعرفان إلى جميع من قدم لي المساعدة من الأساتذة الأفاضل والزملاء الأعزاء في تجمع الطائف الصحي، لما قدموه من دعم ومساهمة قيّمة في توفير البيانات والمعلومات اللازمة لإتمام هذه الدراسة.

ولا يفوتني في هذا المقام أن أتقدم بأسمى عبارات الشكر والتقدير إلى أفراد عائلتي الكريمة، الذين وقفوا إلى جانبي بالدعاء والتشجيع والدعم المعنوي خلال فترة الدراسة.

ختاماً، أسأل الله أن يوفقنا جميعاً لما يحب ويرضى، وأن يجعل عملنا هذا خالصاً لوجهه الكريم.
خاص تقديري وأمتناني ،،

فهد بن رجاء الله الشبتي
خريج ماجستير إدارة مخاطر
جامعة الجميع الذكية
٢٠٢٥

الإهداء

إلى من كانوا سبباً في وجودي، وسنداً في رحلتي، ومصدر إلهامي وقوتي، إلى والديّ الغاليين، اللذين زرعاً في نفسي حب العلم والتعلم، وأسهما بكل تضحية وعطاء في بناء مستقبلي.

إلى شريكة حياتي وأبنائي الأعزاء، الذين كانوا دوماً الداعم الأكبر والمحفز الأسمى لأواصل مسيرة العلم والعمل. إلى إخوتي وأخواتي، الذين وقفوا معي قلباً وقالباً، وساندوني بقلوبهم الصادقة ودعائهم المستمر. إلى كل من علمني حرفاً، وكل من وقف إلى جانبي، وشجعني، وكان لي عوناً في تحقيق هذا الإنجاز.

إليكم جميعاً أهدي هذا العمل المتواضع، عرفاناً مني بجميلكم وتقديرًا لدوركم في حياتي.

بكل الحب والامتنان ،،،

فهد بن رجاء الله الشبتي
خريج ماجستير إدارة مخاطر
جامعة الجميع الذكية
٢٠٢٥

جدول المحتويات

٢	حقوق الطباعة- Copyright notice	
٣	المستخلص	
٤	Abstract	
٥	الشكر والتقدير	
٦	الإهداء	
٧	جدول المحتويات	
٩	قائمة الأشكال	
٩	نموذج رقم () خطوات تطبيق نظام إدارة أمن المعلومات ISO 27001	
١٠	خطأ! الإشارة المرجعية غير معروفة.	
١٠	قائمة الجداول	
١١	قائمة المصطلحات:	
١٣	المقدمة:	١,١
١٤	مشكلة الدراسة	١,٢
١٥	أهداف الدراسة:	١,٣
١٧	أهمية الدراسة	١,٤
١٧	أولاً: الأهمية العلمية للدراسة	١,٤,١
١٨	ثانياً: الأهمية العملية للدراسة	١,٤,٢
١٩	تساؤلات الدراسة	١,٥
٢٠	السؤال الرئيسي للدراسة	١,٥,١
٢٢	فرضيات الدراسة	١,٦
٢٦	النظرية المتبعة في إعداد الدراسة (Theoretical Framework)	١,٧
٢٨	نموذج الدراسة	١,٨
٢٩	مخطط المشروع (الفصول)	١,٩
٣٠	الفصل الثاني: الدراسات السابقة	٢
٣١	المقدمة	٢,١
٣٢	التعريفات الإجرائية لمتغيرات الدراسة	٢,٢
٣٢	أولاً: المتغير المستقل – تطبيق معايير ISO 27001	٢,٢,١
٣٤	ثانياً: المتغير التابع – الحد من مخاطر تسرب وفقدان الوثائق المرقمنة والرقمية	٢,٢,٢
٣٧	المراجعة الأدبية والدراسات السابقة	٢,٣
٤٠	عرض وتحليل الدراسات السابقة	٢,٣,١
٤٣	الفجوات البحثية (النظرية والتطبيقية)	٢,٣,٢
٤٧	تميز الدراسة الحالية ومساهماتها العلمية	٢,٣,٣
٤٨	الإطار النظري للدراسة (Theoretical Framework)	٢,٤
٥١	الفصل الثالث: منهجية الدراسة	٣
٥٢	١. المقدمة	٣,١
٥٢	تصميم الدراسة (بصلة البحثي)	٣,٢
٥٥	مجتمع الدراسة وطرق وتقنيات أخذ العينات	٣,٣
٥٥	خصائص عينة الدراسة (Sample Characteristics)	٣,٤
٥٦	تحديد حجم العينة (Sample Size Determination)	٣,٥
٥٧	خطوات جمع البيانات / أداة جمع البيانات	٣,٦
٥٩	حدود زمانية، مكانية وحدود موضوعية	٣,٧
٥٩	المحددات الزمنية:	٣,٧,١
٥٩	المحددات المكانية:	٣,٧,١
٦٠	محددات العينة:	٣,٧,٢
٦٠	محددات القياس:	٣,٧,٣
٦١	المحددات المنهجية:	٣,٧,٤
٦١	محددات الوصول:	٣,٧,٥
٦١	القيود الزمنية:	٣,٧,١
٦٢	قيود التمويل:	٣,٧,١
٦٢	قيود حجم العينة:	٣,٧,١
٦٣	قيود الأدوات المستخدمة:	٣,٧,١

٦٣.....	قيود القياس:	٣,٧,١
٦٤.....	الأداة المستخدمة للتحليل الإحصائي (Method of Analysis)	٣,٨
٦٥.....	الفصل الرابع: الدراسة الميدانية	٤
٦٦.....	مقدمة	٤,١
٦٦.....	تحليل البيانات	٤,٢
٦٦.....	توصيف عينة الدراسة (الإحصائيات الوصفية لعينة الدراسة)	٤,٢,١
٧٠.....	الإحصاء الوصفي لمتغيرات الدراسة (الإجابة على أسئلة الدراسة)	٤,٢,٢
٧٢.....	اختبارات الصدق والثبات للاستبيانات	٤,٢,٣
٧٣.....	تحليل صدق البنية لمتغير "تطبيق معايير ISO 27001"	٤,٢,٤
٧٧.....	نتائج الدراسة ومناقشتها مع نتائج الدراسات السابقة	٤,٣
٧٧.....	اختبار الفرضيات ومناقشة النتائج	٤,٣,١
٧٧.....	نتائج اختبار الفرضية الرئيسية	٤,٣,١
٧٨.....	نتائج اختبار الفروض الفرعية	٤,٣,٢
٨٠.....	معاملات الارتباط الخطي	٤,٣,١
٨٢.....	التوصيات	٤,٤
٨٣.....	الدراسات المستقبلية	٤,٥
٨٤.....	الخاتمة	٤,٦
٨٥.....	المراجع	
٨٥.....	العربية	.a
٨٦.....	الاجنبية	.b
٨٧.....	الملاحق	

قائمة الأشكال

الصفحة	عنوان الشكل	رقم الشكل
٢٨	النموذج المقترح للبحث ، المصدر: الباحث	١-١
٢٩	٢-١ مخطط المشروع	٢-١
٣٩	١-٢ نموذج خطوات تطبيق نظام إدارة أمن المعلومات ISO 27001	١-٢
٥٤	١-٣ تصميم بصلة البحث	١-٣
٦٧	١-٤ رسم بياني جهة العمل	١-٤
٦٧	٢-٤ رسم بياني الجنس	٢-٤
٦٨	٣-٤ رسم بياني المستوى التعليمي	٣-٤
٦٨	٤-٤ رسم بياني المسمى الوظيفي	٤-٤
٦٩	٥-٤ رسم بياني سنوات الخبرة	٥-٤
٦٩	٦-٤ رسم بياني الخبرة العملية في حفظ البيانات	٦-٤

قائمة الجداول

رقم الجدول	عنوان الجدول	الصفحة
١-١	النموذج الجدولي للمتغير الرئيسي (تطبيق معايير ISO 27001)	٢٢
٢-١	١.٢ النموذج الجدولي للمتغير التابع (الحد من مخاطر تسرب وفقدان الوثائق)	٢٣
١-٢	جدول المتغير المستقل والأبعاد وأسئلة الدراسة (17)	٣٢
٢-٢	٢-٢ أسئلة الاستبيان:	٣٣
٣-٢	جدول المتغير التابع والأبعاد وأسئلة الدراسة (16)	٣٤
٤-٢	٢-٤ أسئلة الاستبيان:	٣٥
١-٤	١-٤ دلالة المتوسطات الحسابية	٧٠
٢-٤	٢-٤ للمتوسطات الحسابية والانحرافات المعيارية لمتغيرات الدراسة	٧٠
٣-٤	٣-٤ جدول تحليل النتائج	٧٢
٤-٤	٤-٤ نتائج اختبار الفرضية الرئيسية	٧٧
٥-٤	٥-٤ نتائج اختبار الفروض الفرعية	٧٩
٦-٤	٦-٤ معاملات الارتباط الخطي	٨١

قائمة المصطلحات:

المصطلح بالإنجليزية	المصطلح بالعربية
ISO 27001 Standard	معييار ISO 27001
Information Security	أمن المعلومات
Digital Documents	الوثائق الرقمية
Document Leakage	تسرب الوثائق
Document Loss	فقدان الوثائق
Digital Governance	الحوكمة الرقمية
Records and Archives Center	مركز الوثائق والمحفوظات
Document Management	إدارة الوثائق
Encryption	التشفير
Access Control	التحكم في الوصول
Business Continuity Plan	خطة استمرارية الأعمال
Disaster Recovery Plan	خطة التعافي من الكوارث
Security Compliance	الامتثال الأمني
Risk Assessment	تحليل المخاطر
Health Cluster	التجمع الصحي
Taif Health Cluster	التجمع الصحي بالطائف
Confidentiality	السرية
Integrity	النزاهة
Availability of Information	توفر المعلومات
Information Security Management System (ISMS)	نظام إدارة أمن المعلومات (ISMS)
Self-assessment	التقييم الذاتي

١ الفصل الأول: الاطار العام للدارسة

- (١) المقدمة
- (٢) مشكلة الدارسة
- (٣) أهداف الدارسة
- (٤) أهمية الدارسة
- (٥) أسئلة الدارسة
- (٦) فرضيات الدارسة
- (٧) النظرية المتبعة في إعداد الدارسة
- (٨) نموذج الدارسة
- (٩) مخطط المشروع

١.١ المقدمة:

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.

تهدف هذه الدراسة إلى تقييم أثر تطبيق معايير **ISO 27001** على الحد من مخاطر تسرب وفقدان الوثائق الرقمية والمقرنة 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. وتركز الدراسة 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 تسرب الوثائق المقرنة والرقمية 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 والمقرنة من مخاطر التسرب المحتملة.

١.٢ مشكلة الدراسة

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

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

على الرغم من أن معايير ISO 27001 تُعتبر إطاراً عالمياً 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 والمرفقة، مما يجعل المؤسسة عرضة لمخاطر تسرب أو فقدان البيانات. ومن هنا تبرز مشكلة الدراسة الرئيسية: هل يؤدي تطبيق معايير ISO 27001 إلى الحد من مخاطر تسرب وفقدان الوثائق الرقمية والمرفقة في تجمع الطائف الصحي؟

يمكن تصنيف مشكلة الدراسة إلى المحاور التالية:

١. مشكلة أمنية: ضعف أنظمة الحماية المطبقة على الوثائق الرقمية والمرفقة، 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 وفقاً 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 تقتصر الدراسات المحلية إلى تقييم شامل لكيفية الحد من مخاطر تسرب وفقدان الوثائق الرقمية في هذا السياق.

١.٣ أهداف الدراسة:

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

١. تقييم مدى فاعلية 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 السبراني 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 لهذه الدراسة 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.

١.٤ أهمية الدراسة

١.٤.١ أولاً: الأهمية العلمية للدراسة

تكتسب هذه الدراسة أهمية علمية متزايدة لعدة اعتبارات منهجية ونظرية، إذ تمثل إضافة نوعية إلى الحقول المعرفية المتقاطعة بين أمن المعلومات، وإدارة الوثائق، وحوكمة الأنظمة الرقمية، لا سيما في ظل ندرة الدراسات التطبيقية العربية التي تتناول معيار ISO 27001 في السياق الصحي.

أولاً، تسهم الدراسة في سد فجوة بحثية قائمة تتعلق بتطبيق معايير أمن المعلومات على مستوى المؤسسات الصحية العربية. فرغم اتساع نطاق تطبيق معيار ISO 27001 عالمياً، إلا أن الدراسات التي تناولت أثر هذا التطبيق على حماية الوثائق الرقمية والمرفقة في البيئة الصحية لا تزال محدودة، وتفتقر إلى نماذج تقييم منهجية ترتبط بالواقع المؤسسي المحلي.

ثانياً، تعتمد الدراسة على أطر نظرية متعددة، تشمل: نظرية أمن المعلومات التنظيمي، نظرية إدارة المخاطر، نظرية مثلث أمن المعلومات (CIA Triad)، نظرية الامتثال التنظيمي، ونظرية النظم. هذا التعدد في الزوايا النظرية يضفي ثراءً علمياً ويتيح تحليل الظاهرة البحثية من منظور متكامل، يجمع بين التقنية والإدارة والسلوك البشري.

ثالثاً، تسهم الدراسة في بناء نموذج علمي قابل للاختبار، يربط بين تطبيق معيار ISO 27001 كمكون إداري-تقني وبين النتائج المترتبة عليه في ما يتعلق بتقليل مخاطر تسرب أو فقدان الوثائق الرقمية. هذا النموذج يُمكن للباحثين الآخرين تبنيه أو تطويره في دراسات مقارنة، سواء على مستوى القطاعات أو المناطق الجغرافية.

رابعاً، تُعزز هذه الدراسة من محتوى الأدبيات العلمية المكتوبة باللغة العربية، من خلال معالجة موضوع دقيق وحديث بمنهج كمي وتطبيق ميداني داخل مؤسسة صحية. كما تُسهم نتائجها في إثراء البرامج الأكاديمية في تخصصات مثل: إدارة المخاطر، الإدارة الصحية، الأمن السيبراني، وإدارة الجودة.

وأخيراً، تمثل الدراسة أساساً يمكن الانطلاق منه نحو بناء نظريات محلية أو نماذج تقييم معيارية خاصة بالمؤسسات الصحية في المملكة العربية السعودية، بما يتماشى مع احتياجاتها التنظيمية والتقنية الخاصة، ويواكب تطورات التحول الرقمي الآمن والمستدام.

١.٤.٢. الأهمية العملية للدراسة

من الجانب العملي، تتبع أهمية هذه الدراسة من قدرتها على تقديم حلول واقعية قابلة للتطبيق، تسهم في تحسين الأداء المؤسسي في واحدة من أكثر القضايا الحيوية في زمن التحول الرقمي، وهي: حماية الوثائق الرقمية والمراقبة من التسرب أو الفقدان، خصوصًا في قطاع حيوي كالقطاع الصحي.

أولاً، توفر الدراسة تشخيصًا دقيقًا للواقع الميداني في تجمع الطائف الصحي، من خلال قياس مستوى تطبيق متطلبات معيار ISO 27001، وتحليل أثر ذلك على إدارة المخاطر الأمنية المتعلقة بالوثائق. وبالتالي، تُساعد الجهات المعنية في اتخاذ قرارات مستندة إلى بيانات لتطوير سياساتها وإجراءاتها.

ثانيًا، تقدّم الدراسة أداة تقييم مؤسسية قابلة للاستخدام لاحقًا في رصد مستويات الامتثال بالمعيار وتطورها بمرور الوقت. ويمكن تكييف هذه الأداة داخل التجمع أو تعميمها على مؤسسات صحية أخرى في المملكة.

ثالثًا، تسهم النتائج في تعزيز ثقافة أمن المعلومات داخل بيئة العمل، من خلال تسليط الضوء على أهمية دور الموظفين، ومستوى وعيهم، واستعدادهم للتفاعل مع سياسات الحماية المؤسسية. كما يمكن أن تُستخدم النتائج في تصميم برامج توعية وتدريب تستهدف الفئات التي أظهرت انخفاضًا في معدلات الاتفاق مع ممارسات الأمان.

رابعًا، تُوفر الدراسة مؤشرات أداء عملية يمكن الاستناد إليها في وضع سياسات داخلية أكثر كفاءة، كسياسات التحكم في الوصول، والنسخ الاحتياطي، والاستجابة للحوادث، وضبط الصلاحيات. كما تُعد مخرجاتها مرجعًا لتحديث دليل إجراءات العمل الخاص بإدارة الوثائق الرقمية.

خامسًا، تخدم الدراسة التوجهات الوطنية الكبرى من خلال دعم أهداف التحول الرقمي الآمن ضمن رؤية المملكة ٢٠٣٠، والمساهمة في تحقيق بيئة صحية إلكترونية موثوقة وآمنة، ما يعزز من قدرة المملكة على بناء نظام صحي رقمي يوازن بين الكفاءة التشغيلية وأمن المعلومات.

وباختصار، فإن القيمة العملية لهذه الدراسة لا تقتصر على تشخيص الوضع الحالي، بل تمتد إلى تقديم إطار عمل قابل للتنفيذ، يُمكن صانعي القرار من تطوير منظومة إدارة أمن الوثائق بطرق مستدامة ومبنية على بيانات موثوقة.

١.٥ تساؤلات الدراسة

تهدف هذه الدراسة إلى استكشاف وتحليل أثر تطبيق معايير ISO 27001 على الحد من مخاطر تسرب وفقدان الوثائق المرقمة 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 الأرشيف 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 المرقمة والرقمية داخل تجمع الطائف الصحي.

١.٥.١ السؤال الرئيسي للدراسة

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

١. 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 أمان الوصول.

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

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

٢. 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 أمانًا 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 الأرشفة الرقمية: (Reliability of Digital Archiving Systems)

- تعزيز أمان منصات الأرشفة 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 فقدان 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.

١.٦ فرضيات الدراسة

بناءً على مشكلة الدراسة وأهدافها، 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 البسيط 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.

١.١ - 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	H2: يوجد تأثير ذو دلالة إحصائية بين تطبيق ضوابط التحكم في الوصول وفق معايير ISO 27001 والحد

من الوصول غير المصرح به للوثائق الرقمية.	الوصول غير المصرح به للوثائق الرقمية؟		
H3: يوجد تأثير ذو دلالة إحصائية بين تطبيق تقنيات التشفير وفق معايير ISO 27001 وتقليل مخاطر تسرب وفقدان الوثائق الرقمية.	إلى أي مدى يساهم استخدام تقنيات التشفير وحماية البيانات في تحسين أمان الوثائق الرقمية في تجمع الطائف الصحي؟	استخدام تقنيات التشفير لتأمين الوثائق الرقمية	التشفير وحماية البيانات (Data Encryption & Protection)
H4: يوجد تأثير ذو دلالة إحصائية بين تطبيق خطط استمرارية الأعمال والتعافي من الكوارث وفق معايير ISO 27001 واحتمالية فقدان الوثائق الرقمية.	ما مدى تأثير خطط استمرارية الأعمال والتعافي من الكوارث وفق معايير ISO 27001 على حماية الوثائق الرقمية من الفقدان؟	تطوير خطط طوارئ لضمان استعادة الوثائق الرقمية في حالات الطوارئ	إدارة استمرارية الأعمال والتعافي من الكوارث (BCP & DRP)
H5: يوجد تأثير ذو دلالة إحصائية بين التدقيق الأمني المستمر وفق معايير ISO 27001 وتحسين مستوى أمان الوثائق الرقمية في المؤسسات الصحية.	كيف يؤثر إجراء التدقيق الأمني المستمر وفق معايير ISO 27001 على تحسين أمن الوثائق الرقمية؟	إجراء مراجعات دورية لضمان تطبيق الإجراءات الأمنية	الامتثال والتدقيق الأمني (Compliance & Security Audits)

١.٢ 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	تنفيذ أنظمة مراقبة متقدمة لرصد أي	كيف يساهم تطبيق معايير ISO 27001 في الحد من تسرب الوثائق	H6: يوجد تأثير ذو دلالة إحصائية بين تطبيق

معايير ISO 27001 وتقليل مخاطر تسرب الوثائق الرقمية من خلال أنظمة المراقبة الأمنية.	الرقمية من خلال تقنيات الحماية والرصد المستمر؟	وصول غير مصرح به	(Data Breach Reduction)
H7: يوجد تأثير ذو دلالة إحصائية بين تطبيق معايير ISO 27001 وتعزيز موثوقية أنظمة الأرشفة الرقمية وتقليل احتمالات فقدان الوثائق.	إلى أي مدى يساهم تطبيق معايير ISO 27001 في تحسين أداء وموثوقية أنظمة الأرشفة الرقمية وتقليل فقدان الوثائق؟	تحسين أمان منصات الأرشفة من خلال استخدام تقنيات متقدمة	زيادة موثوقية أنظمة الأرشفة الرقمية (Reliability of Digital Archiving Systems)
H8: يوجد تأثير ذو دلالة إحصائية بين استراتيجيات إدارة الوثائق وفق معايير ISO 27001 وتقليل مخاطر فقدان الوثائق الرقمية.	كيف يمكن لاستراتيجيات إدارة الوثائق وفق معايير ISO 27001 أن تعزز من أمن الوثائق الرقمية وتقليل فقدانها؟	تطبيق سياسات صارمة لحماية الوثائق من الضياع أو التلف	تحسين استراتيجيات إدارة الوثائق (Document Management Strategies)
H9: يوجد تأثير ذو دلالة إحصائية بين تطبيق ضوابط الوصول وفق ISO 27001 واحتمالية فقدان الوثائق الرقمية بسبب الوصول غير المصرح به.	ما مدى تأثير ضوابط الوصول المطبقة وفق ISO 27001 على تحسين التحكم في إدارة الوثائق الرقمية ومنع فقدانها؟	استخدام أنظمة تحقق من الهوية لمنع الوصول غير المصرح به	التحكم في الوصول إلى الوثائق (Document Access Control)
H10: يوجد تأثير ذو دلالة إحصائية بين تدريب الموظفين على أمن الوثائق الرقمية وتقليل الأخطاء	كيف يؤثر تدريب الموظفين على معايير ISO 27001 في تعزيز أمن الوثائق الرقمية وتقليل الأخطاء	تنفيذ برامج تدريبية لتعزيز أمن المعلومات	تحسين وعي الموظفين بالمخاطر الأمنية

ISO 27001 وتقليل فقدان الوثائق الرقمية الناتج عن الأخطاء البشرية.	البشرية التي قد تؤدي إلى فقدانها أو تسريبها؟		(Security Awareness & Training)
---	---	--	---------------------------------------

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 يساهم في تقديم نتائج واضحة تدعم التوصيات المستقبلية.

١.٧ النظرية المتبعة في إعداد الدراسة (Theoretical Framework)

في ظل التحول الرقمي المتسارع، بات أمن المعلومات ركيزة أساسية في استمرارية العمل المؤسسي، لاسيما في القطاع الصحي الذي يتعامل مع بيانات حساسة، مثل السجلات الطبية والوثائق الرقمية للمرضى. وانطلاقاً من هذه الأهمية، تهدف هذه الدراسة إلى استكشاف أثر تطبيق معايير **ISO/IEC 27001** على الحد من مخاطر تسرب وفقدان الوثائق الرقمية والمراقبة داخل تجمع الطائفة الصحي، وذلك من خلال تبني إطار نظري يستند إلى مجموعة من النظريات المعترف بها في حقل أمن المعلومات والإدارة التنظيمية.

أولاً: معيار ISO/IEC 27001

يمثل معيار **ISO 27001** نظاماً عالمياً لإدارة أمن المعلومات (ISMS)، يركز على تحديد المخاطر وتقييمها والتصدي لها عبر مجموعة من الضوابط والسياسات. ويشمل هذا النظام خطوات تنظيمية تشمل:

- تحديد نطاق نظام إدارة أمن المعلومات.
- إعداد سجل الأصول.
- تقييم شامل للمخاطر.
- تطوير السياسات والإجراءات الأمنية.
- التدقيق الداخلي والتحسين المستمر.

تعتبر هذه الخطوات أساساً لبناء بيئة رقمية آمنة وفعالة لحماية الوثائق الحساسة من الفقد أو التسرب.

ثانياً: النظريات العلمية المرتبطة بالدراسة

١. نظرية إدارة المخاطر (Risk Management Theory)

تعد هذه النظرية حجر الزاوية في الدراسة، حيث تؤكد على أهمية تحديد وتقييم وتحليل المخاطر، وتطبيق استراتيجيات للحد منها. وتدعم هذه النظرية الفرضية التي ترى أن تطبيق معيار **ISO 27001** يساهم في خفض المخاطر المرتبطة بالوثائق الرقمية.

٢. مثلث أمن المعلومات (CIA Triad Theory)

تركز هذه النظرية على ثلاث ركائز أساسية: السرية (Confidentiality)، السلامة (Integrity)، والتوافر (Availability). ويتطابق هذا المفهوم مع أهداف **ISO 27001**، حيث تهدف جميع ضوابطه إلى حماية هذه الأبعاد.

٣. نظرية الامتثال التنظيمي (Organizational Compliance Theory)

تشير هذه النظرية إلى أن التزام المؤسسة بالمعايير الدولية، مثل **ISO 27001**، يعزز من موثوقيتها التنظيمية، ويقلل من احتمالية الوقوع في مخالفات قانونية أو تسريبات معلوماتية.

٤. نظرية الانتشار والابتكار (Diffusion of Innovation Theory)

تستخدم هذه النظرية لقياس مدى تبني الموظفين والقيادات داخل المؤسسة لمعيار **ISO 27001** وتعتمد على فهم العوامل التي تسهل أو تعيق تبني الممارسات الجديدة، مثل الوعي، التدريب، والدعم الإداري.

٥. نظرية السلوك التنظيمي (Organizational Behavior Theory)

تتناول هذه النظرية أثر البيئة التنظيمية، والثقافة الداخلية، وسلوك الأفراد على فاعلية تطبيق نظم إدارة أمن المعلومات. وتُبرز أهمية وجود وعي أمني وتعاون بين جميع المستويات الإدارية.

٦. نظرية النظم (Systems Theory)

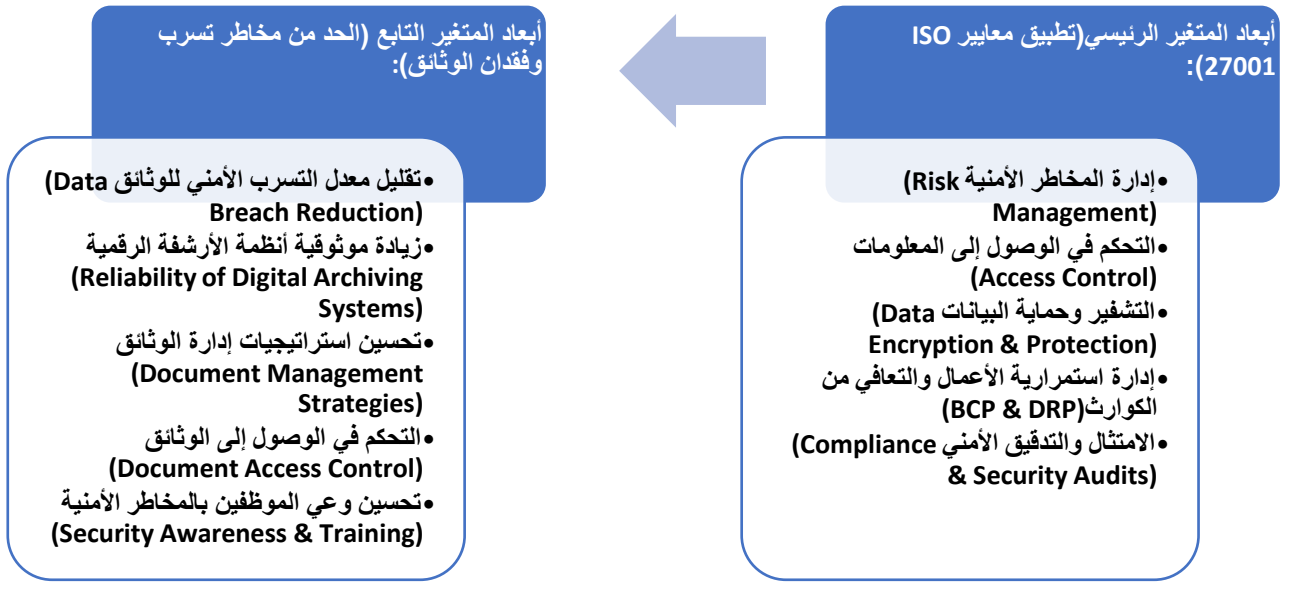
ترى هذه النظرية أن المؤسسة وحدة متكاملة، يتطلب نجاح أي تطبيق - ك - ISO 27001 تنسيقاً وتكاملاً بين جميع المكونات (البشرية، التقنية، التنظيمية).

ثالثاً: العلاقة بين النظرية والتطبيق في الدراسة

يُستخدم هذا الإطار النظري لتفسير وتحليل العلاقة بين تطبيق معيار ISO 27001 (باعتباره المتغير المستقل) ومخاطر تسرب وفقدان الوثائق الرقمية (كمُتغير تابع). وتُسهم النظريات السابقة في بناء فهم معمق للمتغيرات قيد الدراسة، وتساعد على تفسير النتائج المتوقعة في ضوء المفاهيم العلمية والإدارية المعتمدة.

١.٨ نموذج الدراسة

١-١ النموذج المقترح للبحث ، المصدر: الباحث



١.٩ مخطط المشروع (الفصول)

١-٢ مخطط المشروع



٢ الفصل الثاني: الدراسات السابقة

- (١) مقدمة
- (٢) التعريفات الإجرائية لمتغيرات الدراسة
- (٣) المراجعة الأدبية والدراسات السابقة
- (٤) الاطار النظري

٢.١ المقدمة

يهدف هذا الفصل إلى شرح الإطار المنهجي الذي استُخدم في تنفيذ الدراسة، من حيث تصميمها، وطبيعة مجتمعها، وأسلوب اختيار العينة، وأداة جمع البيانات، وآليات تحليلها. كما يُبرز الفصل كيف تم operationalize المتغيرات النظرية وتحويلها إلى مؤشرات قابلة للقياس.

وتكمن أهمية هذا الفصل في كونه يوفّر القواعد المنهجية التي بُنيت عليها النتائج، ويساعد في تقييم مصداقية الدراسة، وإمكانية تكراره أو البناء عليه في دراسات لاحقة. وبذلك، يشكل هذا الفصل الجسر الذي يربط بين الإطارين النظري والتطبيقي، ويُمكن القارئ من فهم منطق الدراسة وتوجهها التحليلي.

في ضوء ذلك، يسعى هذا الفصل إلى توضيح المعايير التي تم الاعتماد عليها في اختيار تصميم الدراسة، وأسباب تفضيل منهجية كمية تستند إلى أدوات قياس معيارية وقابلة للتطبيق على نطاق واسع. ويتناول الفصل تعريفًا دقيقًا بمجتمع الدراسة وخصائصه، إلى جانب مبررات اختيار العينة، سواء من حيث الحجم أو طريقة التوزيع أو طبيعة المشاركين. هذا بالإضافة إلى استعراض خصائص أداة الدراسة، وهي الاستبانة، من حيث محاورها ومقياسها وارتباطها المباشر بأهداف الدراسة وفرضياتها.

كما يتضمن الفصل تحديدًا للتعريفات الإجرائية للمتغيرات الأساسية، بما يشمل المتغير المستقل (تطبيق معايير ISO 27001) والمتغير التابع (مخاطر تسرب وفقدان الوثائق المرقمنة والرقمية)، مع شرح كيفية ترجمة هذه المفاهيم النظرية إلى مؤشرات قابلة للقياس الكمي من خلال فقرات الاستبانة. ويستعرض الفصل كذلك الوسائل الإحصائية المستخدمة في تحليل البيانات، سواء على مستوى التحليل الوصفي أو الاستدلالي، إلى جانب البرامج المستخدمة للتحليل الإحصائي، بما يضمن سلامة الاستنتاجات وموثوقيتها.

ولا يقتصر هذا الفصل على عرض الإجراءات فحسب، بل يعكس أيضًا مدى التزام الباحث بالمعايير الأخلاقية والمنهجية المتعارف عليها في الدراسة العلمي، مثل مراعاة السرية، والحصول على موافقة المشاركين، والتحقق من صدق الأدلة وثباتها. وبذلك، لا يمثل هذا الفصل مجرد وصف فني لإجراءات الدراسة، بل يُعبّر عن فلسفة الدراسة ومنهجيتها، ويُعدّ مكونًا أساسيًا لفهم نتائج الدراسة وتفسيرها في سياقها العلمي الصحيح.

٢.٢ التعريفات الإجرائية لمتغيرات الدراسة

تُعد التعريفات الإجرائية حجر الأساس في الدراسات الكمية، إذ تُترجم المفاهيم النظرية إلى متغيرات قابلة للقياس، وتوضح كيف تم تمثيل كل متغير داخل أداة الدراسة. وبما أن هذه الدراسة تسعى إلى قياس العلاقة بين تطبيق معايير ISO 27001 (المتغير المستقل) والحد من مخاطر تسرب وفقدان الوثائق المرقمنة والرقمية (المتغير التابع)، فقد تم اعتماد التعريفات الإجرائية التالية:

٢.٢.١ أولاً: المتغير المستقل – تطبيق معايير ISO 27001

يشير هذا المتغير إلى مدى التزام المؤسسة الصحية بتطبيق متطلبات معيار ISO 27001 فيما يتعلق بإدارة أمن المعلومات والوثائق الرقمية، وتم قياسه من خلال خمسة أبعاد رئيسية:

١. إدارة المخاطر الأمنية

وتمثل قدرة المؤسسة على تحديد، تقييم، ومعالجة المخاطر التي تهدد أمن الوثائق الرقمية.

٢. التحكم في الوصول

ويقاس مدى وجود ضوابط تقنية وتنظيمية تنظم من يحق له الوصول إلى الوثائق، وكيف.

٣. التشفير وحماية البيانات

ويتعلق بالإجراءات التقنية التي تضمن حماية المعلومات أثناء التخزين أو النقل.

٤. استمرارية الأعمال والتعافي من الكوارث

ويقاس مدى استعداد المؤسسة للتعامل مع الانقطاعات أو الحوادث واستعادة الوثائق الرقمية بسرعة وكفاءة.

٥. الامتثال والتدقيق الأمني

ويعكس قدرة المؤسسة على الالتزام بسياسات أمن المعلومات وإجراء مراجعات دورية للتحقق من التطبيق.

٢-١ جدول المتغير المستقل والأبعاد وأسئلة الدراسة (17)

اسم المتغير	أبعاد المتغير	عدد الفقرات في الاستبيان
تطبيق معايير ISO	SR إدارة المخاطر الأمنية	4
	AC التحكم في الوصول	4
	DP حماية البيانات والتشفير	3
	BC استمرارية الأعمال والتعافي من الكوارث	3

3	الامتثال والتدقيق الأمني	CS	27001 (مستقل)	
---	--------------------------	----	------------------	--

٢-٢ أسئلة الاستبيان:

المتغير	البعد	رقم الفقرة	السؤال	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
Implementation ISO تطبيق معايير 27001	إدارة المخاطر الأمنية	1	تعتمد المؤسسة آلية واضحة لتحديد مخاطر أمن الوثائق الرقمية بانتظام					
	إدارة المخاطر الأمنية	2	يتم تحليل مخاطر فقدان الوثائق ضمن خطط إدارة المعلومات					
	إدارة المخاطر الأمنية	3	تتوفر إجراءات استجابة للحوادث في حال تسرب وثائق رقمية					
	إدارة المخاطر الأمنية	4	يتم تحديث تقييمات المخاطر بشكل دوري					
	التحكم في الوصول	5	توجد صلاحيات محددة للوصول إلى الوثائق الرقمية بناءً على المهام الوظيفية					
	التحكم في الوصول	6	يتم مراقبة سجلات الدخول والخروج من الأنظمة المرتبطة بالوثائق					
	التحكم في الوصول	7	تستخدم كلمات مرور قوية ونظام تحقق مزدوج للوصول إلى الوثائق					
	التحكم في الوصول	8	يتم تقييد الوصول إلى الوثائق الحساسة بناءً على مستويات الصلاحية					
	حماية البيانات والتشفير	9	تستخدم تقنيات تشفير لحماية الوثائق الرقمية أثناء التخزين					
	حماية البيانات والتشفير	10	تُطبق سياسات حماية البيانات عند نقل الوثائق إلكترونياً					
	حماية البيانات والتشفير	11	يتم تحديث بروتوكولات التشفير المستخدمة بشكل دوري					
	استمرارية الأعمال والتعافي	12	تتوفر خطة واضحة لاستمرارية الأعمال في حال حدوث خلل تقني					
	استمرارية الأعمال والتعافي	13	تُحفظ نسخ احتياطية للوثائق الرقمية بشكل دوري					
	استمرارية الأعمال والتعافي	14	تُجرى اختبارات منتظمة لخطة التعافي من الكوارث					
	الامتثال والتدقيق الأمني	15	تخضع المؤسسة لتدقيقات أمنية دورية على أنظمة إدارة الوثائق					
	الامتثال والتدقيق الأمني	16	يتم توثيق جميع السياسات والإجراءات الأمنية الخاصة بالوثائق					
	الامتثال والتدقيق الأمني	17	في إدارة ISO 27001 تلتزم المؤسسة بمتطلبات معيار الوثائق					

٢.٢.٢ ثانياً: المتغير التابع – الحد من مخاطر تسرب وفقدان الوثائق المرقمنة والرقمية

يُقصد بهذا المتغير مدى نجاح المؤسسة في تقليل احتمالات فقدان أو تسرب الوثائق الرقمية بسبب عوامل داخلية أو خارجية. وقد تم تمثيله من خلال الأبعاد التالية:

١. تقليل معدل الحوادث الأمنية المتعلقة بالوثائق

ويقيس عدد وقائع التسرب أو الفقد خلال فترة زمنية معينة.

٢. موثوقية أنظمة الأرشفة الرقمية

ويقيس مدى اعتماد المؤسسة على أنظمة حفظ رقمية آمنة وفعالة.

٣. صرامة الضوابط والإجراءات الداخلية

ويشير إلى مدى وضوح وفعالية السياسات المنظمة لحماية الوثائق.

٤. وعي الموظفين بإجراءات الحماية

ويقيس درجة معرفة الموظفين وتدريبهم على التعامل الآمن مع الوثائق الرقمية.

٥. فعالية السياسات المؤسسية

ويقيس مدى تطبيق سياسات الحوكمة المتعلقة بحماية الوثائق ومدى الالتزام بها.

٢-٣ جدول المتغير التابع والأبعاد وأسئلة الدراسة (16)

اسم المتغير	أبعاد المتغير	عدد الفقرات في الاستبيان
R الحد من مخاطر تسرب وفقدان الوثائق (تابع)	RS تقليل الحوادث الأمنية	3
	RA موثوقية أنظمة الأرشفة	4
	SI صرامة الضوابط الداخلية	3
	EA وعي الموظفين بسياسات الأمان	3
	EC فعالية السياسات المؤسسية	3

٢-٤ أسئلة الاستبيان:

المتغير	البعد	رقم الفقرة	السؤال	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
The Risks of Document Leakage and Loss مخاطر تسرب وفقدان الوثائق	تقليل الحوادث الأمنية	18	انخفاض عدد حوادث تسرب الوثائق الرقمية خلال العامين الماضيين					
	تقليل الحوادث الأمنية	19	توجد آلية واضحة للإبلاغ عن أي حادث أمني يتعلق بالوثائق					
	تقليل الحوادث الأمنية	20	يتم تحليل أسباب الحوادث الأمنية وتوثيقها لمنع تكرارها					
	موثوقية أنظمة الأرشيف	21	تستخدم أنظمة أرشفة رقمية معترف بها وموثوقة					
	موثوقية أنظمة الأرشيف	22	تتوفر صلاحيات وصول مستقلة لكل مستخدم على نظام الأرشيف					
	موثوقية أنظمة الأرشيف	23	يتم الاحتفاظ بنسخ مؤرشفة قابلة للاسترجاع بسهولة					
	موثوقية أنظمة الأرشيف	24	يخضع نظام الأرشيف لصيانة وتحديث منتظم					
	صرامة الضوابط الداخلية	25	توجد سياسات مكتوبة لتنظيم تداول الوثائق الرقمية					
	صرامة الضوابط الداخلية	26	تُطبق عقوبات في حال الإخلال بضوابط حماية الوثائق					
	صرامة الضوابط الداخلية	27	يتم مراجعة السياسات الداخلية بشكل دوري لضمان فعاليتها					
	وعي الموظفين	28	يتم تدريب الموظفين على التعامل الآمن مع الوثائق الرقمية					
	وعي الموظفين	29	تُجرى حملات توعية دورية حول أمن المعلومات					
	وعي الموظفين	30	يتم تقييم التزام الموظفين بإجراءات حماية الوثائق					
	فعالية السياسات المؤسسية	31	تعكس السياسات المؤسسية التزامًا واضحًا بحماية الوثائق الرقمية					
	فعالية السياسات المؤسسية	32	يتم تطبيق السياسات الأمنية بفعالية على جميع الأقسام					
	فعالية السياسات المؤسسية	33	تتم مراجعة وتحديث السياسات الأمنية بناءً على التغيرات التقنية					

تم استخدام هذه التعريفات كأساس لبناء فقرات الاستبانة، بحيث تغطي كل بعد من الأبعاد المحددة بمؤشرات واضحة تُمكن من التحليل الإحصائي الدقيق، وتسهم في الوصول إلى نتائج علمية موثوقة.

نص نشر الاستبيان :

السادة المشاركون الكرام،

تحية طيبة وبعد...

أجري هذا الاستبيان في إطار إعداد رسالة ماجستير بعنوان:

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

تهدف هذه الدراسة إلى قياس مدى فاعلية تطبيق معايير أمن المعلومات (ISO 27001) في حماية الوثائق الرقمية داخل المؤسسات الصحية، وتحديد أثر ذلك على تقليل المخاطر المتعلقة بفقدان أو تسرب تلك الوثائق. ويسعدني أن أوجه إليكم هذه الدعوة للمشاركة باعتباركم من أصحاب الخبرة والمعرفة في هذا المجال، مما يُضفي قيمة علمية وميدانية عالية على نتائج الدراسة.

إن مشاركتكم تمثل جزءاً مهماً من نجاح هذه الدراسة، علماً بأن جميع المعلومات التي ستقدّمونها سيتم التعامل معها بسرية تامة، ولن تُستخدم إلا لأغراض الدراسة العلمي، دون الإشارة إلى أسماء أو جهات. يرجى التكرم بالإجابة بدقة وشفافية على جميع الفقرات، علماً بأن الاستبيان لا يستغرق أكثر من (10-15 دقيقة) من وقتكم الثمين.

شكراً مقدماً على تعاونكم ودعمكم للبحث العلمي.

[رابط الاستبيان](#)

٢.٣ المراجعة الأدبية والدراسات السابقة

شهدت السنوات الأخيرة تزايداً ملحوظاً في الأدبيات التي تتناول قضايا أمن المعلومات في بيئات العمل الرقمية، خاصة في المؤسسات التي تتعامل مع بيانات حساسة كالقطاع الصحي. وقد تركزت أغلب هذه الأدبيات على دراسة المخاطر المرتبطة بتسرب أو فقدان المعلومات، وآليات الحماية الممكنة، وتحديد فعالية المعايير الدولية - وعلى رأسها ISO/IEC 27001 - في تعزيز الضبط الأمني وتحقيق الامتثال المؤسسي.

تشير العديد من الدراسات إلى أن تبني معيار ISO 27001 لا يقتصر على كونه إطاراً تقنياً، بل يمثل نموذجاً إدارياً متكاملًا لإدارة المخاطر وتأمين الأصول المعلوماتية. فقد تناولت دراسة حلمي وعائشة (٢٠٢٣) أثر المعايير الدولية في إدارة الوثائق الحكومية، مؤكدةً أن التقيد بهذه المعايير يسهم في تحقيق الشفافية والموثوقية وتقليل المخاطر التشغيلية. كما أثبتت دراسات أخرى أن ضعف الوعي المؤسسي وعدم وضوح السياسات الداخلية يؤديان إلى فجوات خطيرة في أمن الوثائق.

في السياق الصحي، أظهرت الأدبيات ندرة واضحة في الدراسات العربية التي تُعالج العلاقة بين تطبيق معايير ISO 27001 ومستوى الأمان الوثائقي. ومع ذلك، فإن بعض الدراسات التطبيقية في مستشفيات ومؤسسات صحية دولية كشفت عن وجود تحسن ملحوظ في السيطرة على تسرب البيانات وفقدانها بعد تطبيق هذه المعايير، خصوصاً في جوانب مثل التحكم في الوصول، واستمرارية الأعمال، والتشفير، والتدقيق الأمني.

وتبرز أهمية هذه المراجعة الأدبية في أنها تسلط الضوء على الثغرات المعرفية التي تسعى هذه الدراسة إلى سدّها، من خلال تقييم ميداني لتطبيق ISO 27001 في سياق محلي داخل تجمع الطائف الصحي، وتحليل أثره على تقليل المخاطر المرتبطة بالوثائق الرقمية والمقرنة.

١. تحديد نطاق نظام إدارة أمن المعلومات

تبدأ المؤسسة بتحديد النطاق الذي يشمل البيانات المراد حمايتها، والأنظمة والمواقع والأنشطة المرتبطة بها. ويتم ذلك مع الأخذ في الاعتبار المتطلبات القانونية والتنظيمية والسياقين الداخلي والخارجي للمؤسسة.

٢. إنشاء سجل الأصول

يتطلب المعيار وجود سجل دقيق لجميع الأصول المرتبطة بالمعلومات، مثل البيانات، الأجهزة، البرمجيات، والمستخدمين. ويُعد هذا السجل الأساس لتقييم المخاطر وتوزيع المسؤوليات.

٣. إجراء تقييم شامل للمخاطر

يتم تقييم المخاطر المحتملة التي قد تهدد أصول المعلومات، من خلال تقدير احتمالية حدوثها وتأثيرها، وتحديد درجة الخطورة لكل منها. وتُبنى على هذا التقييم خطط لمعالجة المخاطر والتقليل من آثارها.

٤. تطوير السياسات والإجراءات

يجب أن تنشئ المؤسسة مكتبة سياسات واضحة تغطي جوانب أمن المعلومات كافة، بما في ذلك التحكم في الوصول، حماية البيانات، استمرارية الأعمال، والاستجابة للحوادث. كما يُراعى تحديث هذه السياسات بشكل مستمر.

٥. تنفيذ التدقيق الداخلي

تُعد هذه الخطوة النهائية للتحقق من مدى التزام المؤسسة بتطبيق متطلبات المعيار، قبل الدخول في مرحلة التدقيق الخارجي للحصول على الشهادة الرسمية.

ويُعد اتباع هذه الخطوات أداة فعالة في ترسيخ ممارسات أمن المعلومات المؤسسية، وضمان إدارة المخاطر بطريقة منهجية ومنضبطة. كما ينسجم هذا التوجّه مع أهداف الدراسة الحالية، التي تسعى إلى قياس أثر تطبيق معايير ISO 27001 على الحد من مخاطر تسرب وفقدان الوثائق الرقمية والمقرنة، حيث تمثل هذه الخطوات المعيارية المرجع الذي يُقاس عليه مستوى النضج المؤسسي في مجال أمن الوثائق.

٢-١ نموذج خطوات تطبيق نظام إدارة أمن المعلومات ISO 27001



٢.٣.١ عرض وتحليل الدراسات السابقة

تهدف هذه الدراسة إلى توضيح مفهوم المعيار الدولي ISO 27001 وأهميته في تعزيز أمن المعلومات، وتسليط الضوء على دوره في توفير إطار شامل يسمح للمنظمات بتقييم المخاطر ووضع إجراءات لحماية المعلومات. تشير الدراسة إلى أن تطبيق معايير ISO 27001 يُعتبر مدخلاً مهماً للتحسين المستمر في أنظمة توثيق وإدارة المعلومات في المؤسسات الجزائرية. وخلصت الدراسة إلى أن المؤسسات الجزائرية تعاني نقصاً في تطبيق هذه المعايير وتفتقر للوعي الكافي بأهمية أمن المعلومات، مما يؤكد ضرورة بذل جهود أكبر لتطوير وتطبيق نظم متوافقة مع ISO 27001 للاستفادة من مزاياها المتعددة (الشريف وطلحي، ٢٠١٤، ص. ٣-٥).

سعت دراسة كحيلة سارة (2021) إلى تحليل دور المعايير الدولية ISO 27001 و ISO 27002، بالإضافة إلى القانون الجزائري ١٥-٠٤، في حماية الوثائق الإلكترونية من المخاطر المحتملة، وتسليط الضوء على أهمية التوقيع الإلكتروني كأداة لضمان أصالة وسلامة الوثائق الرقمية، أكدت الدراسة أن المعايير الدولية توفر إطاراً متكاملًا لبناء سياسات أمنية لحماية الوثائق الرقمية، أوضحت أن استخدام هذه المعايير يساعد على تقييم المخاطر، التحكم في الوصول، وتحديد نقاط الضعف في الأنظمة الأمنية، أشارت إلى أن القانون ١٥-٠٤ يمثل دعماً تشريعياً مهماً لحماية الوثائق الإلكترونية من خلال تنظيم التوقيع والتصديق الإلكترونيين.

أجرت ناهد علام (٢٠٢٣) دراسة بعنوان "البرامج الآلية لإدارة الوثائق والأرشيف: مفاهيم وقضايا"، هدفت إلى تسليط الضوء على المفاهيم المرتبطة باستخدام الأنظمة الآلية في إدارة الوثائق والأرشيف، والتحديات التي تواجه المؤسسات عند تبني برامج جاهزة لا تتوافق مع المعايير الأرشيفية المعتمدة. ركزت الدراسة على أهمية تكيف هذه الأنظمة مع احتياجات المؤسسات بدلاً من الاعتماد الكلي على الحلول الجاهزة، مؤكدة على وجود فجوة في التكامل بين الأنظمة التقنية وأمن الوثائق.

أشارت النتائج إلى ضعف تطبيق المعايير الدولية في نظم الأرشيف المعتمدة، وبيّنت الحاجة إلى تبني حلول مؤسسية متوافقة مع المعايير العالمية مثل ISO 15489. كما حذرت من أن غياب معايير الأمان في الأنظمة المستخدمة يؤدي إلى احتمالات مرتفعة لتسرب الوثائق أو فقدانها، خاصة في المؤسسات التي تعتمد على النظم التقنية دون تهيئتها بالشكل الملائم.

تناولت دراسة حلمي وعائشة (2023) معايير **MSR 30300** باعتبارها نموذجاً حديثاً لأنظمة إدارة الوثائق، حيث استعرضت الأسس والمبادئ التي تقوم عليها هذه المعايير وأوجه تميزها مقارنة بالمعايير التقليدية مثل ISO 15489. وركزت الدراسة على دور المعايير في دعم الحوكمة الرشيدة، وضمان التكامل، والحفاظ على أمن الوثائق، كما ناقشت كيفية تبني المنظمات لهذه المعايير لتعزيز الكفاءة وتقليل المخاطر المرتبطة بتسرب أو فقد الوثائق.

وقد أكدت الدراسة أهمية ربط إدارة الوثائق بالاستراتيجية المؤسسية وتكاملها مع نظم إدارة الجودة والأمن والمخاطر. ويمكن الاستفادة من هذه النتائج في دعم الفرضيات المتعلقة بتأثير تطبيق معايير ISO 27001 على تقليل مخاطر تسرب الوثائق الرقمية، مما يعزز موثوقية البحوث التي تبحث في إدارة الوثائق ضمن بيئات صحية أو مؤسساتية معقدة.

أكدت دراسة (Hsu & Shih, 2023) على أن تطبيق معايير ISO 27001 يُسهم بشكل ملحوظ في تحسين أمن المعلومات في المؤسسات الطبية، حيث أثبتت النتائج أن المستشفيات التي تعتمد تدابير أمنية تتوافق مع هذه المعايير تُظهر مستويات أعلى من الحماية ضد المخاطر الأمنية المتنوعة، خاصة تلك المرتبطة بتسرب البيانات وحمايتها من فقدان والاختراقات السيبرانية.

هدفت الدراسة (Hsu & Shih, 2023) إلى تقييم مدى تطبيق معايير ISO 27001 لأمن المعلومات في المؤسسات الطبية، وذلك من خلال مقارنة مستويات حماية أمن المعلومات بين المستشفيات العامة والخاصة، وتحديد مدى الوعي والالتزام بمعايير ISO 27001 وأثرها على تعزيز أمن المعلومات.

اتبعت منهجية دراسة (Hsu & Shih, 2023): استخدم منهج المسح الميداني، وتم تطبيق استبانة مكونة من عدة أجزاء، تقيس الوعي بأمن المعلومات وتقييم المخاطر الأمنية المختلفة (المادية، البشرية، الإدارية، التقنية). ووزعت الاستبانة على عينة قوامها ١٥٠ موظفاً مسؤولاً عن أمن المعلومات في مستشفيات عامة وخاصة ووحدات طبية عسكرية، حيث كانت نسبة الاستجابة مرتفعة (١١٣ استبانة صالحة للتحليل).

أظهرت دراسة (Hsu & Shih, 2023) تفاوتاً واضحاً في مستوى الحماية من المخاطر الأمنية لدى المؤسسات الطبية باختلاف أنواعها، حيث كانت المخاطر المرتبطة بالبيانات هي الأقل حماية، بينما المخاطر المرتبطة بالبرمجيات كانت الأعلى حماية.

أوضحت نتائج دراسة (Hsu & Shih, 2023) أن هناك حاجة ماسة لتعزيز سياسات وإجراءات أمن المعلومات في المستشفيات العامة بشكل خاص، حيث إن مستوى استثمارها في أمن المعلومات ليس أفضل من المؤسسات الخاصة.

أشارت نتائج دراسة (Hsu & Shih, 2023) إلى أهمية التدريب المستمر والتوعية بأمن المعلومات للموظفين، مع تأكيد أن المخاطر البشرية والإدارية كانت ضمن المخاطر التي تحتاج إلى اهتمام أكبر.

وأوصت دراسة (Hsu & Shih, 2023): على ضرورة تعزيز الاستثمار في أنظمة الحماية والتدريب في المستشفيات العامة بشكل خاص، وأهمية وجود نظام تدقيق دوري مستمر لضمان الامتثال الكامل لمعايير ISO 27001، وتطوير سياسات أمن معلومات واضحة تُطبق بشكل فعال للحد من المخاطر البشرية والإدارية.

أكدت دراسة (Moghaddam & Amirsharifi, 2024) على أهمية تطبيق الأطر القانونية والتنظيمية، مثل GDPR وHIPAA، في حماية بيانات المرضى في ظل التوسع الكبير في استخدام التقنيات الصحية الرقمية، وشددت على ضرورة مواكبة هذه الأطر للتطورات التكنولوجية لضمان حماية بيانات المرضى من التهديدات السيبرانية وتسرب البيانات.

أكدت دراسة (Kurdi et al., 2024) على أن تطبيق معايير أمن المعلومات منذ المراحل الأولى من دورة حياة تطوير البرمجيات (SDLC) يساهم بشكل فعال في تقليل المخاطر الأمنية وتحسين جودة البرمجيات المنتجة، وأوضحت الدراسة أهمية التكامل بين ضمان الجودة (Quality Assurance) وعمليات الأمن السيبراني، حيث إن كلاهما يعمل على تقليل المخاطر، الأولى تركز على المخاطر الوظيفية والثانية تركز على المخاطر الأمنية، وأظهرت نتائج الدراسة ضرورة تعزيز الوعي الأمني لدى جميع العاملين في تطوير البرمجيات من خلال برامج تدريبية منتظمة، تشمل الممارسات الآمنة في كتابة الأكواد، ومراجعة أمنية شاملة للبرمجيات.

أجرت دراسة علام (٢٠٢٣) تحليلاً شاملاً لاستخدام الأنظمة الآلية في إدارة الأرشيفات والوثائق الرقمية، وأظهرت أن تبني المؤسسات لمعايير متخصصة في أمن المعلومات مثل ISO 27001 يُساهم بشكل كبير في تقليل حوادث فقدان البيانات. وأكدت الدراسة على أهمية وجود أنظمة أرشفة مخصصة تراعي المعايير الدولية، حيث توصلت إلى أن المؤسسات التي تلتزم بهذه المعايير تمتلك قدرات أكبر في السيطرة على المخاطر الأمنية.

تناولت دراسة سليمان وزكريا (٢٠٢٥) أثر تطبيق معايير حوكمة تكنولوجيا المعلومات، بما في ذلك معايير ISO، على جودة المعلومات المحاسبية في المؤسسات. وأوضحت الدراسة أن معايير الأيزو تساهم في ضمان أمن وسلامة المعلومات من خلال توفير ضوابط وإجراءات أمنية فعالة، وهو ما ينعكس إيجاباً على الخصائص النوعية للمعلومات المحاسبية. كما أظهرت نتائج الدراسة وجود علاقة ذات دلالة إحصائية بين تطبيق هذه المعايير ورفع جودة التقارير المالية، مما يعزز من موثوقية نظم المعلومات المحاسبية، ويدعم الدور التنظيمي والرقابي لتلك النظم في بيئة تعتمد على تكنولوجيا رقمية متقدمة. وتؤكد الدراسة أهمية التكامل بين أمن المعلومات والمعايير المحاسبية لتحقيق الامتثال والجودة معاً.

يُظهر هذا التحليل أن الدراسة الحالية تأتي لتسد فجوة تطبيقية ونظرية مهمة من خلال تقديم نموذج واضح ودقيق لدراسة أثر تطبيق معايير ISO 27001 على مستوى أمن الوثائق الرقمية في تجمع الطائف الصحي، مما يجعلها إضافة نوعية تُعزز الأدبيات الأكاديمية والتطبيقية في مجال أمن المعلومات.

٢.٣.٢ الفجوات البحثية (النظرية والتطبيقية)

٢.٣.٢.١ الفجوات النظرية

من خلال استعراض وتحليل الأدبيات النظرية السابقة التي تناولت موضوع إدارة أمن الوثائق والمعلومات وتطبيق معايير ISO 27001 ، تبين أن هناك فجواتٍ نظريةً متعددة تُبرز الحاجة الملحة إلى إجراء هذه الدراسة لسدها وإثراء القاعدة المعرفية، خصوصاً فيما يتعلق بتطبيق هذه المعايير ضمن القطاعات الصحية في المملكة العربية السعودية وتحديدًا في تجمع الطائفت الصحي. وتتمثل هذه الفجوات بشكل تفصيلي فيما يلي:

أولاً: محدودية الدراسات النظرية المتعلقة بتطبيق معايير ISO 27001 في المؤسسات الصحية: رغم الاهتمام المتزايد عالمياً بمعايير ISO 27001 كنظام شامل لإدارة أمن المعلومات، إلا أن الأدبيات النظرية العربية والعالمية التي تناولت تطبيق هذه المعايير بشكل مفصل ضمن المؤسسات الصحية تعد قليلة ومحدودة جداً. فقد ركزت معظم الدراسات على قطاعات مثل المالية والمصرفية والتكنولوجية، مما يجعل هناك حاجة ماسة لدراسات نظرية تعمق الفهم حول الخصوصيات والتحديات المتعلقة بتطبيق هذه المعايير في المؤسسات الصحية، التي تتميز بحساسية عالية للمعلومات المتداولة.

ثانياً: نقص الدراسات النظرية التي تربط بين تطبيق ISO 27001 وحماية الوثائق الرقمية والمقرنة: على الرغم من أن هناك أدبيات تناولت بشكل عام أهمية معايير ISO 27001 في تعزيز أمن المعلومات، إلا أن هناك نقصاً واضحاً في الأدبيات النظرية التي توضح طبيعة العلاقة بين تطبيق هذه المعايير وتأثيرها على الحد من تسرب وفقدان الوثائق الرقمية، وخاصة فيما يتعلق بالوثائق الصحية ذات الحساسية العالية. ويتجلى ذلك في عدم وجود نماذج نظرية واضحة أو أطر فكرية متخصصة تشرح كيف يمكن لهذه المعايير تحديدًا أن تقلل من هذه المخاطر.

ثالثاً: ضعف الأطر النظرية التي توضح دور الإدارة العليا في نجاح تطبيق ISO 27001: تبين من مراجعة الأدبيات النظرية نقصٌ في التحليلات التي توضح بوضوح العلاقة النظرية بين التزام الإدارة العليا وتقديم الدعم الكافي لتطبيق معايير ISO 27001 وبين نجاح إدارة أمن الوثائق الرقمية. فما زالت أغلب الدراسات تركز بشكل عام على أهمية الإدارة العليا دون تعمق في توضيح الأبعاد النظرية لهذه العلاقة، مثل آليات اتخاذ القرار، أو توفير الموارد، أو قيادة التغيير، وكيف تؤثر هذه العوامل النظرية على نجاح المعايير الأمنية.

رابعاً: غياب الدراسات النظرية حول أثر العوامل التنظيمية والثقافية المحلية في تطبيق ISO 27001: تمثل السياقات الثقافية والتنظيمية عوامل مهمة في نجاح تطبيق معايير أمن المعلومات، ورغم ذلك، لم تُغطِ الأدبيات النظرية هذه الجوانب بشكل معمق، خاصة في السياق المحلي السعودي. فمن خلال مراجعة الأدبيات تبين أن هناك نقصاً في الأبحاث التي توضح تأثير الخصائص التنظيمية والثقافية المحلية على فعالية تطبيق

ISO 27001، لا سيما في مؤسسات الرعاية الصحية السعودية التي قد تواجه تحديات خاصة فيما يتعلق بثقافة الأمن المعلوماتي والامتثال للمعايير الدولية.

خامساً: محدودية الدراسات النظرية في توضيح العلاقة بين التقنيات الحديثة ومعايير ISO 27001 في حماية الوثائق:

رغم الأهمية الكبيرة للتقنيات الحديثة مثل الذكاء الاصطناعي، والحوسبة السحابية، وأنظمة التشفير، في تعزيز أمن الوثائق الرقمية، إلا أن الأدبيات النظرية التي تقدم أطراً واضحة للعلاقة بين استخدام هذه التقنيات وتطبيق معايير ISO 27001 لا تزال محدودة. ويبرز هذا النقص في عدم توفر دراسات نظرية توضح بعمق كيف يمكن دمج هذه التقنيات ضمن منظومة ISO 27001 لتعزيز الحماية وتقليل مخاطر التسرب أو فقدان في بيئة القطاع الصحي.

سادساً: النقص النظري في تحديد التحديات التي تواجه تطبيق ISO 27001 في قطاع الصحة السعودي بشكل مفصل:

على الرغم من أن بعض الأدبيات السابقة تناولت تحديات تطبيق ISO 27001، إلا أنها تناولت تلك التحديات بشكل عام وسطحي، دون تفصيل يخص القطاع الصحي المحلي السعودي. هذا يمثل فجوة نظرية مهمة، حيث تحتاج المؤسسات الصحية السعودية إلى إطار نظري واضح ومفصل يمكن من خلاله تحديد التحديات بشكل دقيق واقتراح حلول مبنية على أدبيات نظرية عميقة تلائم الواقع المحلي. بناءً على هذه الفجوات النظرية، تأتي هذه الدراسة لسد تلك الثغرات وتقديم إطار نظري شامل وعميق يُمكن الاعتماد عليه لفهم وتحليل أثر تطبيق معايير ISO 27001 في الحد من مخاطر تسرب وفقدان الوثائق الرقمية والمقرنة، خصوصاً في تجمع الطائف الصحي، مما يساهم في تقديم إضافة علمية ونظرية مهمة للباحثين والمختصين في مجال إدارة أمن المعلومات الصحية.

٢.٣.٢.٢ الفجوات التطبيقية

من خلال مراجعة واقع تطبيق معايير ISO 27001 لإدارة أمن الوثائق الرقمية والمقرنة في المؤسسات الصحية بشكل عام، وتجمع الطائف الصحي بشكل خاص، تبين وجود مجموعة من الفجوات التطبيقية التي تستدعي إجراء دراسة ميدانية متخصصة بهدف فهمها وتقديم حلول عملية وفعالة لمعالجتها، وفيما يلي عرض تفصيلي لهذه الفجوات:

أولاً: ضعف تطبيق معايير ISO 27001 بشكل ممنهج في المؤسسات الصحية المحلية:

رغم الإدراك المتزايد لأهمية أمن المعلومات والوثائق الرقمية في المؤسسات الصحية، إلا أن هناك فجوة تطبيقية واضحة تتمثل في عدم تطبيق معايير ISO 27001 بشكل منهجي أو شامل في تجمع الطائف الصحي، مما ينعكس سلباً على أمن الوثائق الرقمية. إن افتقار المؤسسات إلى خطة واضحة لتطبيق هذه المعايير وإجراءات متابعة مستمرة يشكل نقطة ضعف رئيسية في الإدارة التطبيقية للأمن الرقمي.

ثانياً: نقص الوعي والتدريب لدى الموظفين على ممارسات أمن الوثائق الرقمية:

أظهرت الممارسات العملية ضعفاً في برامج التوعية والتدريب المستمرة الموجهة للعاملين في تجمع الطائف الصحي، مما أدى إلى محدودية وعي الموظفين بمخاطر الأمن الرقمي وأهمية تطبيق معايير ISO 27001 بشكل صارم. يتسبب هذا النقص في زيادة الأخطاء البشرية، مثل سوء إدارة كلمات المرور أو عدم الالتزام بإجراءات الأمان، مما يزيد من احتمالية حدوث تسرب أو فقدان الوثائق.

ثالثاً: غياب أو ضعف البنية التحتية التقنية اللازمة لتطبيق ISO 27001:

تبين أن المؤسسات الصحية، تواجه فجوة تطبيقية هامة تتمثل في ضعف البنية التحتية التقنية التي تلبي متطلبات تطبيق معايير ISO 27001، مثل استخدام أنظمة التشفير المتقدمة، وأنظمة النسخ الاحتياطي والتعافي من الكوارث. هذه الفجوة تؤدي إلى انخفاض القدرة العملية على حماية الوثائق الرقمية وتأمينها من التهديدات المختلفة، سواء كانت تقنية أو بشرية أو طبيعية.

رابعاً: ضعف التكامل بين الإدارات في تطبيق ضوابط ومعايير ISO 27001:

أحد التحديات التطبيقية الملحوظة في تجمع الطائف الصحي هو ضعف التنسيق والتكامل بين الإدارات المختلفة في تطبيق سياسات أمن الوثائق الرقمية. إن عدم وجود آليات واضحة أو إجراءات موحدة بين الأقسام مثل إدارة الوثائق، وإدارة تقنية المعلومات، والإدارة القانونية، يؤدي إلى تضارب في التنفيذ العملي للسياسات، ما يقلل من فعالية تطبيق معايير ISO 27001.

خامسًا: محدودية الرقابة والتدقيق الدوري على تطبيق إجراءات أمن المعلومات:

تواجه المؤسسات الصحية المحلية فجوة تطبيقية تتمثل في محدودية المراجعة والتدقيق الدوري لإجراءات الأمن الرقمي. فالمراجعات الدورية لمدى الالتزام بمعايير ISO 27001 إما غير موجودة أو تتم بشكل سطحي، مما يؤدي إلى ضعف في اكتشاف ومعالجة الثغرات الأمنية في الوقت المناسب، وبالتالي زيادة احتمالية وقوع حوادث أمنية أو تسرب في الوثائق الرقمية.

سادسًا: ضعف الدعم والالتزام الإدارة العليا بتطبيق: ISO 27001

تبين من الممارسة العملية أن هناك فجوة في مستوى دعم الإدارة العليا فيما يتعلق بتطبيق معايير ISO 27001 بشكل جدي ومستمر. فغياب الالتزام الجدي من الإدارة العليا من حيث تخصيص الموارد اللازمة وتقديم الدعم المادي والمعنوي الكافي، يجعل تطبيق معايير الأمن المعلوماتي عملية صعبة وتفتقر إلى الفاعلية والاستدامة.

سابعًا: غياب إجراءات واضحة لإدارة الأزمات والتعافي من الكوارث:

تعاني المؤسسات الصحية في الواقع العملي، من غياب خطط واضحة وشاملة لإدارة الأزمات والتعافي من الكوارث، مما يزيد من مخاطر فقدان الوثائق الرقمية في حالات الطوارئ مثل الهجمات الإلكترونية أو الكوارث الطبيعية أو التقنية، الأمر الذي يشكل تهديدًا مباشرًا لاستمرارية العمليات وجودة الخدمات الصحية.

ثامنًا: ضعف تطبيق استراتيجيات حوكمة البيانات:

توجد فجوة تطبيقية في تطبيق استراتيجيات واضحة لحوكمة البيانات في المؤسسات الصحية السعودية، الأمر الذي يؤدي إلى غياب أو عدم وضوح في تحديد المسؤوليات والصلاحيات المرتبطة بالوصول إلى الوثائق الرقمية وإدارتها، ما قد يزيد من احتمالية تسرب البيانات الحساسة أو فقدانها.

وبناءً على هذه الفجوات التطبيقية، تهدف الدراسة الحالية إلى تقديم نموذج متكامل وواضح لسد هذه الثغرات من خلال تقديم توصيات عملية لتحسين إجراءات الأمان الرقمي في تجمع الطائف الصحي وفقًا لمعايير ISO 27001، مما يساهم في تعزيز الأمن المعلوماتي، وتوفير بيئة تشغيلية أكثر أمانًا، وتحقيق أعلى درجات الحماية للوثائق الرقمية والمقرنة.

٢.٣.٣ تميّز الدراسة الحالية ومساهماتها العلمية

تتميّز الدراسة الحالية بتركيزها على نقطة تقاطع حيوية بين أمن المعلومات وإدارة الوثائق الرقمية، وهو مجال لم يحظَ بالاهتمام الكافي في البيئة الصحية على وجه الخصوص، لا سيما في سياق تطبيق المعايير الدولية مثل **ISO 27001**. وتتبع أهمية هذه الدراسة من كونها تتناول موضوعاً حديثاً نسبياً وذو أولوية متنامية في المؤسسات الصحية التي تشهد تحولاً رقمياً متسارعاً، مما يرفع من مستوى المخاطر المرتبطة بفقدان أو تسرب الوثائق الحساسة.

وتُعد الدراسة من أوائل الدراسات التي تطبّق هذا المعيار الدولي ضمن بيئة **تجمع الطائف الصحي**، مما يعزز قيمتها التطبيقية ويوفر بيانات واقعية يمكن البناء عليها في مشاريع التحسين المستقبلية. كما تُسهم الدراسة علمياً في إثراء أدبيات إدارة المخاطر المعلوماتية في المؤسسات الصحية من خلال ربط **معايير الحوكمة الأمنية بتقنيات إدارة الوثائق الرقمية**، وهو ما يعزز من قدرة المؤسسات على الامتثال للمعايير، وتحقيق الكفاءة، وحماية الخصوصية.

وتضيف الدراسة أيضاً بعداً علمياً يتمثل في اقتراح نموذج أولي أو مجموعة توصيات يمكن اعتمادها لتقليل المخاطر، مما يمهد الطريق لمزيد من الدراسات التطبيقية والمقارنة في قطاعات أخرى.

٢.٤ الإطار النظري للدراسة (Theoretical Framework)

استندت هذه الدراسة إلى نظرية إدارة المخاطر (Risk Management Theory) باعتبارها الإطار العلمي الأكثر ملاءمة لطبيعة موضوع الدراسة، والمتمثل في أثر تطبيق معايير ISO 27001 على الحد من مخاطر تسرب وفقدان الوثائق الرقمية والمرفقة.

وتُعد هذه النظرية من أهم النظريات المستخدمة في مجالات الحوكمة وأمن المعلومات، حيث تركز على الإجراءات المنهجية التي تهدف إلى تحديد المخاطر وتقييمها، ومن ثم التحكم فيها أو تقليلها إلى مستويات مقبولة، من خلال تبني سياسات وضوابط استباقية.

تعريف المخاطر (Definition of Risk)

وفقاً للمعيار الدولي ISO 31000، يُعرّف "الخطر" بأنه: "تأثير عدم التأكد على الأهداف". ويشمل هذا التعريف الجوانب الإيجابية (فرص التحسين) والسلبية (التهديدات)، إلا أن تركيز إدارة المخاطر في الدراسات الأمنية عادةً ما يكون على تقليل التهديدات والخسائر المحتملة.

أنواع المخاطر (Types of Risks)

تنقسم المخاطر عموماً إلى عدة أنواع، أبرزها:

١. مخاطر استراتيجية: ناتجة عن قرارات الإدارة العليا أو تغيرات السوق.
٢. مخاطر تشغيلية: ناتجة عن خلل في العمليات، أو النظم، أو الإجراءات.
٣. مخاطر مالية: تتعلق بالتقلبات الاقتصادية، التمويل، التكاليف، وأسعار الصرف.
٤. مخاطر تقنية: مرتبطة بالأنظمة الرقمية، أمن المعلومات، البرمجيات، والبنية التحتية.
٥. مخاطر الامتثال: ناتجة عن عدم الالتزام باللوائح التنظيمية أو القوانين.
٦. مخاطر بشرية: ناجمة عن سلوك الأفراد، الأخطاء البشرية، أو التساهل الأمني.

تصنيف المخاطر

يختلف تصنيف المخاطر باختلاف طبيعة العمل، ومن أمثلة ذلك:

- تسرب معلومات المرضى، اختراق السجلات، خلل في الأنظمة الطبية
- اختراقات إلكترونية، فشل النظام، ضعف النسخ الاحتياطي
- تأخر إداري، مخاطر قانونية، فقدان وثائق رقمية

- تأخيرات تنفيذ، أضرار في المعدات، مخاطر بيئية

مصادر الخطر (Sources of Risk)

١. المصادر الداخلية:

- ضعف في الحوكمة أو الرقابة.
- نقص التدريب أو الوعي الأمني.
- أنظمة تقنية غير محدثة أو ضعيفة الحماية.
- إجراءات غير موثقة أو غير مطبقة بفعالية.

٢. المصادر الخارجية:

- هجمات إلكترونية.
- تغيرات تشريعية مفاجئة.
- كوارث طبيعية (حرائق، فيضانات).
- انقطاع الخدمات السحابية أو المزودين الخارجيين.

خطوات إدارة المخاطر (Risk Management Steps)

تحديد المخاطر (Risk Identification)

تحديد الأحداث المحتملة التي قد تُعيق الأهداف مثل ما هي أنواع الفشل أو التسريب التي قد تهدد الوثائق الرقمية؟

تحليل المخاطر (Risk Analysis)

تحليل كل خطر من حيث احتمال حدوثه (Likelihood)، تأثيره (Impact) وتستخدم أدوات مثل مصفوفة المخاطر، تحليل السيناريو، أو سجل المخاطر.

تقييم المخاطر (Risk Evaluation)

تصنيف المخاطر وتحديد أولويات التعامل معها، بناءً على مقاييس محددة. هل الخطر مقبول؟ هل يحتاج إلى تدخل مباشر؟ هل يجب تجنبه؟

معالجة المخاطر (Risk Treatment)

اختيار استراتيجية للتعامل مع كل خطر، مثل:

- **التقليل (Mitigation):** تقليل احتمال أو تأثير الخطر.
- **النقل (Transfer):** نقل الخطر لطرف ثالث (مثل التأمين).
- **التجنب (Avoidance):** إلغاء النشاط المسبب للخطر.
- **القبول (Acceptance):** تقبل الخطر إذا كان ضمن حدود معقولة.

مراقبة ومراجعة المخاطر (Monitoring & Review)

مراجعة دورية لسجل المخاطر، وتحديث الاستراتيجيات بناءً على التغيرات أو الحوادث.

الاتصال والتشاور (Communication & Consultation)

إشراك أصحاب المصلحة في جميع مراحل إدارة المخاطر، ورفع الوعي بالمخاطر وخطط المعالجة.

٣ الفصل الثالث: منهجية الدراسة

- (١) مقدمة
- (٢) تصميم الدراسة (بصلة البحثي)
- (٣) مجتمع الدراسة وطرق وتقنيات أخذ العينات
- (٤) خصائص عينة الدراسة.
- (٥) تحديد حجم العينة
- (٦) خطوات جمع البيانات / أداة جمع البيانات
- (٧) حدود زمنية، مكانية وحدود موضوعية
- (٨) الأداة المستخدمة للتحليل الإحصائي

٣.١ 1. المقدمة

تم بناء التحليل الإحصائي في هذا الفصل على أسس منهجية واضحة، باستخدام أدوات إحصائية كمية مناسبة لطبيعة البيانات وطبيعة الفرضيات المطروحة.

يبدأ الفصل بتوصيف دقيق لخصائص العينة المستجيبة من خلال الإحصاءات الوصفية، لتكوين صورة مبدئية حول خلفيات المشاركين ومستوى تنوعهم. يلي ذلك إجراء اختبارات الصدق والثبات للاستبيان، للتحقق من مدى اتساق الأداة وقدرتها على قياس المتغيرات المستهدفة بشكل دقيق وموثوق.

بعد ذلك، يتم عرض المتوسطات الحسابية والانحرافات المعيارية لفقرات الاستبيان، لتحليل الاتجاهات العامة للمشاركين نحو محاور الدراسة، واستنباط مدى تطبيق معايير ISO 27001 في الواقع المؤسسي. كما يتم استخدام معامل الارتباط الخطي للكشف عن طبيعة العلاقات بين المتغيرات، ثم اختبار الفرضيات الإحصائية باستخدام اختبارات مناسبة، ومناقشة النتائج في ضوء الإطارين النظري والتطبيقي.

يهدف هذا الفصل إلى تفسير نتائج الدراسة في ضوء أهدافها وتساولاتها ونماذجها النظرية، بما يتيح الخروج باستنتاجات دقيقة وتوصيات عملية مبنية على بيانات إحصائية ذات دلالة علمية. ويُعد هذا الفصل خطوة حاسمة في ربط التحليل الكمي بالأثر الواقعي، تمهيداً لاستخلاص التوصيات في الفصل الختامي.

٣.٢ تصميم الدراسة (بصلة البحثي)

يعتمد تصميم الدراسة على الإطار العام الذي يُحدّد الطريقة التي سيتم من خلالها معالجة مشكلة الدراسة وتحقيق أهدافها. وبما أن هذه الدراسة تهدف إلى قياس أثر تطبيق معايير ISO 27001 على الحد من مخاطر تسرب وفقدان الوثائق المرقمنة والرقمية، فقد تم اختيار المنهج الكمي الوصفي التحليلي بوصفه الأنسب لطبيعة الدراسة وموضوعها.

وقد تم بناء هذا التصميم وفق نموذج "بصلة البحث" الذي اقترحه *Saunders et al.*، والذي يشمل عدة طبقات تبدأ بالفلسفة وتنتهي بأدوات جمع البيانات.

أولاً: فلسفة الدراسة (Research Philosophy)

تتبنّى الدراسة الفلسفة الوضعية (Positivism)، التي تفترض أن الواقع يمكن ملاحظته وقياسه بدقة من خلال أدوات كمية، دون تدخل ذاتي من الباحث. هذه الفلسفة تعزز الحياد العلمي، وتُركّز على اختبار الفرضيات باستخدام البيانات التجريبية.

ثانياً: منهج الدراسة (Research Approach)

تم اعتماد المنهج الاستنتاجي (Deductive Approach) ، حيث بدأ الباحث من إطار نظري قائم وفرضيات مشتقة منه، ليتم اختبارها ميدانياً عبر جمع بيانات وتحليلها إحصائياً. يتناسب هذا المنهج مع طبيعة الدراسة التي تسعى إلى تأكيد أو نفي علاقات سببية بين المتغيرات.

ثالثاً: استراتيجية الدراسة (Research Strategy)

اعتمدت الدراسة على استراتيجية المسح (Survey Strategy) ، والتي تُعد من أكثر الاستراتيجيات شيوعاً في البحوث الكمية، حيث تتيح جمع بيانات من عدد كبير من الأفراد بطريقة منهجية ومنظمة، باستخدام أدوات قياس موحدة مثل الاستبيان.

رابعاً: نوع الدراسة (Research Type)

تندرج الدراسة ضمن فئة البحوث الكمية (Quantitative Research) ، التي تعتمد على بيانات رقمية قابلة للتحليل الإحصائي، وتستخدم لقياس الظواهر واختبار العلاقات بين المتغيرات.

خامساً: الأفق الزمني (Time Horizon)

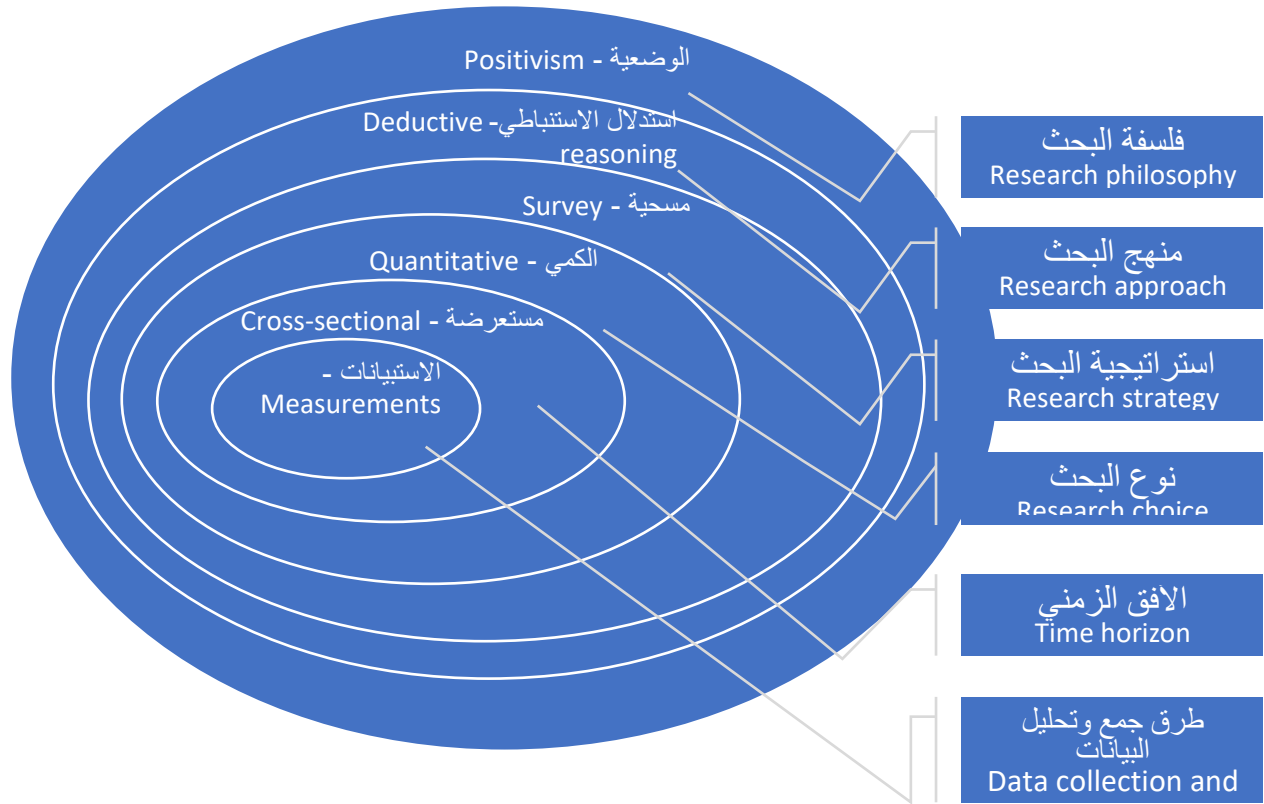
تأخذ الدراسة الأفق الزمني المقطعي (Cross-sectional Time Horizon) ، حيث تم جمع البيانات في نقطة زمنية واحدة، ما يتيح توصيف العلاقة بين المتغيرات كما هي في الواقع أثناء فترة إجراء الدراسة.

سادساً: طرق جمع وتحليل البيانات (Data Collection and Analysis Methods)

اعتمدت الدراسة على أداة الاستبيان المغلق كوسيلة رئيسية لجمع البيانات، نظراً لسهولة توزيعه، ووضوح فقراته، وقدرته على تغطية كافة أبعاد المتغيرات. وتم استخدام برامج التحليل الإحصائي المناسبة لاستخلاص النتائج، والتحقق من صدق الفرضيات، عبر اختبارات إحصائية متعددة (مثل معامل الارتباط، وتحليل الانحدار...).

١. فلسفة الدراسة (الوضعية)
٢. منهج الدراسة (استنتاجي، استقرائي)
٣. استراتيجية الدراسة (المسح)
٤. نوع الدراسة (كمي)
٥. الأفق الزمني (المقطع العرضي)
٦. طرق جمع وتحليل البيانات (استبيانات)

٣-١ تصميم بصلة البحث



٣.٣ مجتمع الدراسة وطرق وتقنيات أخذ العينات

يُعد تحديد مجتمع الدراسة وعينتها خطوة جوهرية في أي بحث علمي، حيث يعتمد عليها مدى دقة النتائج وقابليتها للتعميم. وفي هذه الدراسة، تمثل مجتمع الدراسة في جميع الموظفين المعنيين بإدارة الوثائق والمعلومات الرقمية، وتقنية المعلومات، والجودة، وأمن المعلومات، داخل تجمع الطائف الصحي بمختلف قطاعاته الإدارية والصحية. ويشمل ذلك الموظفين في الإدارات المركزية، إضافة إلى العاملين في المستشفيات والمراكز الصحية الذين لهم ارتباط مباشر بمنظومة إدارة الوثائق أو التعامل مع الوثائق الرقمية والمترقمة.

ونظراً لاتساع المجتمع، وتعذر إجراء مسح شامل لكل أفراد، فقد تم الاعتماد على العينة القصدية (Purposive Sample)، وذلك لاختيار المشاركين ممن يمتلكون معرفة وخبرة كافية بطبيعة الإجراءات المتعلقة بتطبيق معايير ISO 27001 أو إدارة الوثائق الرقمية، بهدف تحقيق دقة أعلى في البيانات.

بلغ حجم العينة (64) مشاركاً، وقد تم تحديده وفقاً لمعادلات إحصائية تراعي حجم المجتمع الأصلي، ودرجة الثقة المطلوبة، وهامش الخطأ المقبول. وتم توزيع الاستبانات إلكترونياً عبر البريد الرسمي للموظفين، إضافة إلى تنسيق مباشر مع إدارات الموارد البشرية وتقنية المعلومات في التجمع لتسهيل الوصول للفئة المستهدفة. ويُعد هذا النوع من العينات مناسباً للدراسات التي تتطلب مشاركة أفراد يمتلكون معرفة تخصصية أو وظائف مرتبطة مباشرة بالمتغيرات محل الدراسة، ما يعزز من صلاحية النتائج وقدرتها على التعبير عن الواقع.

٣.٤ خصائص عينة الدراسة (Sample Characteristics)

تُعدّ خصائص عينة الدراسة من العناصر الأساسية التي تُسهم في تفسير نتائج البحث وفهم مدى تعميمها. وقد تم اختيار عينة الدراسة بعناية من مجتمع مستهدف يتكوّن من موظفي تجمع الطائف الصحي، بما يشمل الإدارات، والمستشفيات، ومراكز الرعاية الصحية الأولية. تهدف العينة إلى تمثيل الشرائح الوظيفية المتنوعة ذات العلاقة بالتعامل مع الوثائق الرقمية والمترقمة.

وفيما يلي عرض لخصائص العينة وفقاً للبيانات الديموغرافية:

جهة العمل:

توزعت العينة على ثلاث جهات رئيسية تمثل الهيكل التنظيمي للتجمع:

- إدارات التجمع.
- مراكز الرعاية الصحية الأولية.
- المستشفيات.

ويُظهر هذا التوزيع شمولية في التمثيل الوظيفي والهيكل، مما يعزز من تنوع وجهات النظر.

الجنس:

شملت العينة مشاركين من كلا الجنسين (ذكور وإناث)، بما يتيح فهماً أوسع للآراء والتجارب ذات العلاقة بتطبيق معايير أمن الوثائق عبر اختلافات النوع الاجتماعي.

المستوى التعليمي:

تنوعت المؤهلات الأكاديمية للمشاركين بين:

- ثانوي.
- بكالوريوس.
- دكتوراه.
- دبلوم.
- ماجستير.

هذا التنوع يعكس مستويات متعددة من الفهم والخبرة التي تؤثر في التعامل مع السياسات والإجراءات التقنية والتنظيمية لأمن المعلومات.

المسمى الوظيفي:

توزعت المسميات الوظيفية للمشاركين إلى:

- تنفيذي.
- طبي.
- سكرتارية.
- إداري.
- تقني.

وهو ما يوفر منظوراً متكاملًا من مختلف الاختصاصات التي تتعامل مع الوثائق الرقمية بشكل مباشر أو غير مباشر.

سنوات الخبرة:

تراوحت خبرات المشاركين بين:

- أقل من سنة.
- 4-7 سنوات.
- 1-3 سنوات.
- أكثر من ٧ سنوات.

هذا التفاوت يتيح مقارنة بين الإدراك الأمني للمبتدئين والمتمرسين في العمل.

الخبرة العملية في حفظ البيانات:

تم استقصاء مدى امتلاك المشاركين لخبرة عملية مباشرة في مجال حفظ البيانات، وهو عامل مهم في تقييم وعيهم بالتطبيق الفعلي للمعايير الأمنية، وتحديد أثر التجربة المهنية على مدى الالتزام بضوابط ISO 27001.

٣.٥ تحديد حجم العينة (Sample Size Determination)

تمثل مجتمع الدراسة في موظفي تجمع الطائفت الصحي من مختلف المواقع الوظيفية (إدارات، مستشفيات، مراكز رعاية صحية أولية)، وهو مجتمع واسع ومتنوع يتعامل بشكل مباشر أو غير مباشر مع الوثائق الرقمية والمرفقة.

طبيعة البحث (وصفي - استقصائي):

نظرًا لأن الدراسة تنتمي إلى فئة الأبحاث الكمية الوصفية التي تعتمد على تحليل اتجاهات وآراء الأفراد حول تطبيق معيار ISO 27001 ، فقد تم اختيار العينة بطريقة تعكس هذا التنوع، مع الحفاظ على التوازن بين الفئات المستهدفة.

الاعتبارات الإحصائية:

تم اعتماد الأسس التالية عند تحديد حجم العينة:

- درجة الثقة 95% (Confidence Level)
 - هامش الخطأ المقبول 5% (Margin of Error)
 - نسبة الاستجابة المتوقعة (Response Rate) بناءً على الدراسات الميدانية المماثلة، مع توقع فقد بعض الاستجابات غير المكتملة.
- بالاعتماد على معادلة "Krejcie & Morgan" لتحديد حجم العينة المناسب لمجتمع مجهول الحجم بدقة، أو كبير الحجم نسبيًا، فإن الحجم الأمثل لعينة البحث يتراوح بين ٥٠ إلى ١٠٠ مفردة لضمان الكفاية الإحصائية، وقد تم فعليًا جمع (عدد المشاركين: 64) استجابة كاملة.

التوزيع المتوازن:

تم الحرص على توزيع الاستبيان بشكل متوازن يغطي:

- التخصصات (الإدارية، التقنية، الطبية).
- التوزيع الجغرافي داخل التجمع.
- التدرج الوظيفي.
- الجنس والمؤهل والخبرة.

٣.٦ خطوات جمع البيانات / أداة جمع البيانات

لتحقيق أهداف الدراسة والإجابة عن تساؤلاتها واختبار فرضياتها، تم استخدام أداة الاستبيان المغلق كأداة رئيسية لجمع البيانات. وقد تم تصميم الاستبيان بعناية ليتماشى مع المتغيرات المحددة في الدراسة، ويقاس كل بعد من أبعادها من خلال مجموعة من الفقرات التي طُوِّرت بناءً على مراجعة الأدبيات والدراسات السابقة ذات الصلة، بالإضافة إلى المعايير الرسمية لمعيار ISO 27001. تألف الاستبيان من ثلاثة أقسام رئيسية:

القسم الأول: البيانات العامة للمشاركين

ويتضمن معلومات مثل الجنس، المؤهل العلمي، عدد سنوات الخبرة، المسمى الوظيفي، والإدارة أو الجهة التي يعمل بها الموظف. يهدف هذا الجزء إلى وصف خصائص العينة وفهم تنوعها.

الجزء الأول: ويحتوي هذه الجزء على القسم التالي:

السمات الشخصية لأفراد العينة

جهة العمل-Work Entity :

إدارات التجمع	مستشفى	مركز رعاية صحية أولية
---------------	--------	-----------------------

الجنس-Gender

ذكر	انثى
-----	------

المؤهل العلمي-Educational Qualification

دكتوراه	ماجستير	بكالوريوس	دبلوم	ثانوي
---------	---------	-----------	-------	-------

الوظيفة-Job Title

تنفيذي	طبي	إداري	تقني	سكرتارية
--------	-----	-------	------	----------

سنوات الخبرة-Years of Experience

أكثر من ٧ سنوات	4-7 سنوات	1-3 سنوات	أقل من سنة
-----------------	-----------	-----------	------------

خبرة عملية في حفظ البيانات - Practical Experience

أكثر من ٧ سنوات	4-7 سنوات	1-3 سنوات	لا يوجد
-----------------	-----------	-----------	---------

• القسم الثاني: تطبيق معايير ISO 27001 (المتغير المستقل)

يشتمل على عدد من الفقرات التي تقيس درجة التزام المؤسسة بتطبيق الأبعاد الخمسة للمعيار:

١. إدارة المخاطر

٢. التحكم في الوصول

٣. حماية البيانات والتشفير

٤. استمرارية الأعمال

٥. الامتثال والتدقيق

• القسم الثالث: الحد من مخاطر تسرب وفقدان الوثائق الرقمية والمقرنة (المتغير التابع)

يتضمن فقرات تقيس مستوى المخاطر من حيث:

١. معدل الحوادث الأمنية المتعلقة بالوثائق

٢. موثوقية نظم الأرشفة

٣. صرامة الضوابط الداخلية

٤. وعي الموظفين بإجراءات الحماية

٥. فعالية السياسات المتبعة

وقد تم بناء الاستبيان باستخدام مقياس ليكرت الخماسي، الذي يمنح المشاركين فرصة تقييم كل فقرة على مدى من (١ = لا أوافق بشدة) إلى (٥ = أوافق بشدة)، بما يسمح بقياس اتجاهات المشاركين بدرجة من التفصيل والوضوح.

التصنيف	أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة
النقاط	١	٢	٣	٤	٥

وقبل التطبيق الميداني، خضع الاستبيان إلى مراجعة تحكيم علمي من قبل خبراء مختصين في مجالات إدارة الوثائق وأمن المعلومات والدراسة العلمي، كما تم إجراء اختبار أولي (Pilot Study) على عينة محدودة للتأكد من وضوح الفقرات وسهولة فهمها، وتحسين صياغة بعض البنود بناءً على الملاحظات الواردة.

٣.٧ حدود زمنية، مكانية وحدود موضوعية

٣.٧.١ المحددات الزمنية:

أُجريت هذه الدراسة خلال فترة زمنية محددة بين 30 يونيو ٢٠٢٤م وحتى ١٠ يوليو ٢٠٢٤م، وهي فترة قصيرة نسبياً قد تؤثر على جودة جمع البيانات وتحليلها. حيث تزامن توقيت تطبيق الاستبيان مع ذروة الأعمال الإدارية والفنية في بعض الإدارات التابعة لتجمع الطائف الصحي، ما انعكس على تأخر بعض الردود أو عدم اكتمالها بالشكل المطلوب.

علاوة على ذلك، شهدت بيئة الدراسة خلال نفس الفترة بدء تنفيذ مبادرات تحول رقمي جديدة على مستوى البنية التحتية لأنظمة الأرشفة والإدارة الإلكترونية للوثائق، وهو ما قد يؤثر على استقرار إدراك الموظفين لواقع تطبيق معايير ISO 27001 إذ قد تتفاوت ردودهم بين ما هو قائم فعلياً وما هو قيد التغيير أو التطوير. هذه التغيرات المرحلية، التي لم تكن قد استقرت بعد، تشكل عاملاً زمنياً مؤثراً ينبغي مراعاته عند تفسير النتائج أو محاولة تعميمها على فترات زمنية أخرى.

٣.٧.١ المحددات المكانية:

اقتصرت هذه الدراسة على نطاق جغرافي محدد يتمثل في تجمع الطائف الصحي، والذي يشمل مجموعة من المستشفيات والمراكز الصحية والإدارات التابعة له. ورغم أن هذا التحديد المكاني يُعد مناسباً لتحقيق أهداف الدراسة

ضمن بيئة محددة بوضوح، إلا أنه يمثل في الوقت ذاته أحد القيود التي تحد من إمكانية تعميم النتائج على تجمعات صحية أخرى داخل المملكة أو خارجها.

فقد تختلف البيانات الصحية في جوانب متعددة مثل البنية التحتية الرقمية، ودرجة نضج الأنظمة التقنية، ومستوى وعي الموظفين بأمن المعلومات، والأنظمة الإدارية والتنظيمية المعتمدة، وهو ما قد يؤدي إلى تباين في نتائج الدراسات المماثلة. وبالتالي، فإن نتائج الدراسة تعكس واقع تطبيق معايير ISO 27001 والضوابط المرتبطة بحماية الوثائق الرقمية في سياق مكاني محدد، ما يستدعي توخي الحذر عند محاولة تعميمها أو إسقاطها على بيانات صحية مختلفة.

٣.٧.٢ محددات العينة:

في هذه الدراسة التي تناولت أثر تطبيق معايير ISO 27001 في الحد من مخاطر تسرب وفقدان الوثائق المرقمنة والرقمية في تجمع الطائف الصحي، تم اختيار العينة من موظفي التجمع العاملين في المستشفيات، مراكز الرعاية الصحية الأولية، والإدارات التنفيذية. ورغم الحرص على تنوع العينة لتشمل مختلف المستويات الوظيفية والتخصصات، إلا أن حجم العينة (٦٤ مشاركاً) يظل محدوداً نسبياً مقارنة بحجم المجتمع الكلي، مما قد يحد من إمكانية تعميم النتائج على جميع منسوبي التجمع الصحي.

كما أن الاعتماد على الاستجابة الطوعية قد أتاح المجال لتباين في تمثيل الفئات، وقد يكون هناك تحيز في الاستجابة لدى الأفراد المهتمين بالأمن المعلوماتي أو ذوي الخلفية التقنية، مما قد يؤثر على حيادية النتائج. لذلك، يجب تفسير نتائج الدراسة في ضوء هذه المحددات التي قد تؤثر في شمولية الاستنتاجات ودقتها.

٣.٧.٣ محددات القياس:

تم الاعتماد على الاستبيان كأداة رئيسية لجمع البيانات المتعلقة بتطبيق معايير ISO 27001 وتأثيرها على الحد من مخاطر تسرب وفقدان الوثائق. وعلى الرغم من صياغة فقرات الأداة استناداً إلى أطر علمية سابقة ومراجعتها من قبل مختصين لضمان ملاءمتها، إلا أن هناك بعض المحددات التي ينبغي أخذها بعين الاعتبار. فقد يختلف فهم المشاركين لعبارات الاستبيان تبعاً لاختلاف خلفياتهم الوظيفية أو التقنية، ما قد يؤثر على دقة الإجابات. بالإضافة إلى ذلك، فإن الطبيعة الكمية للاستبيان قد لا تتيح التعمق في بعض الجوانب السلوكية أو المؤسسية الدقيقة، كما قد لا تعكس الفروقات الثقافية أو الإدارية في إدراك أهمية معايير الأمن السيبراني، مما قد يؤدي إلى بعض الانحرافات في تقدير شدة العلاقة بين المتغيرات المستهدفة. وعليه، يجب تفسير نتائج القياس في ضوء هذه التحديات المنهجية المحتملة.

٣.٧.٤ المحددات المنهجية:

اعتمدت هذه الدراسة على **المنهج الوصفي التحليلي** بوصفه الإطار المناسب لفهم طبيعة العلاقة بين تطبيق معايير ISO 27001 ومستوى الحد من مخاطر تسرب وفقدان الوثائق الرقمية. ورغم ما يوفره هذا المنهج من قدرة على تحليل البيانات الكمية واستخلاص مؤشرات ذات دلالة إحصائية، إلا أن **غياب المنهج النوعي أو التفسيري** قد يشكل أحد جوانب القصور المنهجي.

فقد لا يتمكن المنهج الوصفي بمفرده من **التعمق في التفاعلات السلوكية والإدارية الدقيقة** أو تفسير الممارسات الفعلية المرتبطة بالأمن المعلوماتي وإجراءات الأرشفة من منظور العاملين. كما أن الاعتماد الحصري على أدوات كمية مثل الاستبيان قد يُغفل السياقات التنظيمية والثقافية التي تؤثر في فهم وتطبيق المعايير. وبالتالي، فإن هذه المحددات قد تؤثر على شمولية التفسير وتحد من إمكانات تعميم النتائج على بيئات مؤسسية أخرى.

٣.٧.٥ محددات الوصول:

واجهت الدراسة بعض القيود المتعلقة بإمكانية الوصول إلى مصادر البيانات أو الفئات المستهدفة، والتي تمثل أحد التحديات التي قد تؤثر على شمولية النتائج ودقتها. فقد تعذر الوصول الكامل إلى بعض الإدارات أو الأقسام ذات الصلة الوثيقة بموضوع الدراسة، وذلك نتيجة لسياسات الخصوصية والسرية المعلوماتية المتبعة في التعامل مع الوثائق الرقمية والإجراءات الأمنية.

كما أن تفاوت مستويات التعاون من قبل بعض الموظفين، سواء بدافع ضغط العمل أو الحذر من الإفصاح عن ممارسات إدارية داخلية، قد أدى إلى غياب بعض المدخلات المهمة التي كان من الممكن أن تثري التحليل. إضافة إلى ذلك، فإن محدودية الاطلاع على بيانات فعلية تتعلق بتطبيق معايير ISO 27001 أو تقارير أمن الوثائق داخل التجمع الصحي قد حالت دون التحقق المباشر من بعض المؤشرات. لذا فإن **محددات الوصول تمثل قيداً يجب مراعاته عند تفسير النتائج واستخلاص الاستنتاجات العامة.**

٣.٧.١ القيود الزمنية:

تشكل القيود الزمنية أحد التحديات التي قد تؤثر على دقة وشمولية نتائج الدراسة. فقد تم تنفيذ هذه الدراسة خلال فترة زمنية قصيرة ومحددة تمتد من 30 يونيو ٢٠٢٤م إلى ١٠ يوليو ٢٠٢٤م، وهي فترة قد لا تكون كافية لملاحظة جميع الجوانب المرتبطة بتطبيق معايير ISO 27001 أو التغيرات التدريجية في ممارسات حفظ الوثائق الرقمية.

كما أن هذه الفترة تزامنت مع مرحلة من التحول الرقمي المكثف داخل تجمع الطائف الصحي، مما يعني أن بعض الإجراءات والضوابط التقنية والإدارية قد تكون قيد التحديث أو لم تُفعل بعد بشكل كامل أثناء جمع البيانات.

وبالتالي، قد لا تعكس إجابات المشاركين في الاستبيان الوضع المستقر أو النهائي للأنظمة والممارسات المعتمدة لاحقاً.

علاوة على ذلك، قد تكون الفترة الزمنية المحدودة قد أثرت على توفر المشاركين أو مدى تفرغهم للتفاعل مع الاستبيان بدقة، خاصةً في الإدارات ذات الأحمال التشغيلية المرتفعة، مما قد يؤدي إلى تحيز زمني في الاستجابة أو انخفاض التمثيل لبعض الشرائح.

ومن هنا، تُوصي الدراسة بضرورة النظر في توسيع الفترات الزمنية لجمع البيانات في الدراسات المستقبلية، ويفضّل تنفيذ دراسات متابعة (Follow-up Studies) بعد اكتمال مراحل التحول الرقمي لضمان دقة النتائج وواقعيتها.

٣.٧.١ قيود التمويل:

شكّلت قيود التمويل أحد العوامل المؤثرة على نطاق وإمكانات هذه الدراسة، حيث انعكست بشكل مباشر على حجم العينة، وطبيعة الأدوات المستخدمة، ومستوى الدعم الفني المتاح. فقد حال محدودية الموارد المالية دون تبني منهجيات بحثية أكثر تقدماً، مثل استخدام أدوات تحليل نوعي مكّملة، أو إجراء مقابلات موسعة مع خبراء أمن المعلومات والوثائق الرقمية داخل التجمع.

كما أثرت هذه القيود على إمكانية توسيع نطاق الدراسة ليشمل تجمعات صحية أخرى أو شرائح وظيفية متعددة، مما كان من شأنه تعزيز دقة النتائج وقابليتها للتعميم. بالإضافة إلى ذلك، قلص التمويل المحدود من قدرة الباحث على الاستعانة بخدمات تحليل بيانات متخصصة أو تطوير نماذج تحليل أكثر تعقيداً.

تعد هذه المحددات المالية جزءاً لا يتجزأ من البيئة البحثية التي تمت فيها الدراسة، مما يستوجب أخذها بعين الاعتبار عند تحليل النتائج، وتفسيرها، والبناء عليها في التوصيات والسياسات المستقبلية. كما يجب على الباحثين المهتمين بتطوير دراسات مماثلة أن يراعوا هذا العامل المهم، لضمان شمولية أكبر ونتائج أكثر عمقاً واستقراراً.

٣.٧.١ قيود حجم العينة:

يُعد حجم العينة أحد العوامل الأساسية التي تؤثر على دقة النتائج ومدى قدرتها على تمثيل المجتمع البحثي. في هذه الدراسة، ورغم الحرص على شمول فئات وظيفية متنوعة من إدارات ومستشفيات ومراكز الرعاية الصحية في تجمع الطائف الصحي، إلا أن حجم العينة ظل محدوداً نسبياً مقارنة بحجم المجتمع الكلي. وقد يؤدي هذا إلى ضعف تمثيل بعض الفئات أو التخصصات الدقيقة، مما يحد من إمكانية التعميم الكامل للنتائج على جميع منسوبي التجمع.

وعليه، فإن نتائج هذه الدراسة يجب تفسيرها ضمن حدود هذه العينة، مع الإشارة إلى أهمية التوسع في العينة في الدراسات المستقبلية لضمان نتائج أكثر دقة وموثوقية.

٣.٧.١ قيود الأدوات المستخدمة:

في هذه الدراسة، تم الاعتماد على الاستبانة كأداة رئيسية لجمع البيانات، لما توفره من سهولة في التوزيع والتحليل الكمي المنهجي. ورغم فاعلية هذه الأداة في تحقيق أهداف الدراسة وقياس المتغيرات محل الاهتمام، إلا أن استخدامها لا يخلو من بعض القيود المنهجية التي قد تؤثر على جودة النتائج.

من أبرز هذه القيود أن الاستبانات المغلقة قد لا تعبر بدقة عن السياقات المعقدة أو التجارب الفردية العميقة للمشاركين، خصوصاً في موضوع يتصل بتطبيق معايير أمنية وفنية مثل ISO 27001. كما قد تختلف فهم وتفسير بعض العبارات بين المشاركين بحسب خلفياتهم الوظيفية أو التقنية، مما قد يؤثر على الاتساق في الإجابات.

علاوة على ذلك، فإن الاستبانة لا تتيح فرصة للتوسع أو استكشاف الأسباب الكامنة خلف بعض الممارسات أو الاتجاهات، كما هو الحال في الأدوات النوعية مثل المقابلات أو مجموعات التركيز. لذلك، توصي الدراسة باستخدام أدوات متعددة في المستقبل، تجمع بين الأسلوبين الكمي والنوعي، لضمان فهم أكثر شمولاً وتفصيلاً للظاهرة محل الدراسة.

٣.٧.١ قيود القياس:

تُعد قيود القياس من التحديات المهمة التي تواجه الدراسات الكمية، وخصوصاً تلك التي تعتمد على أدوات جاهزة مثل الاستبانات. وعلى الرغم من الحرص في هذه الدراسة على تطوير الأداة وفقاً لأفضل المعايير العلمية، ومراجعتها من قبل مختصين لضمان صدقها وثباتها، إلا أن القياس قد يتأثر بعدة عوامل.

أولاً، قد لا تكون بعض البنود كافية لقياس العمق المفاهيمي الكامل لبعض الأبعاد، مثل حماية الوثائق الرقمية أو التزام المؤسسة بمعايير ISO 27001، نظراً لتعقيد المفهوم وارتباطه بمتغيرات ثقافية وتقنية وسلوكية يصعب اختزالها في بنود محدودة. ثانياً، تختلف الخبرات والمعرفة الفنية لدى المشاركين، مما قد يؤثر على فهمهم للأسئلة المرتبطة بالجوانب التقنية أو التنظيمية الدقيقة.

كما أن الاعتماد الكامل على المقياس الذاتي (Self-Report) في الإجابة قد يؤدي إلى نوع من التحيز في الاستجابات، مثل المبالغة في تقدير الالتزام المؤسسي أو التقليل من مشكلات الواقع الفعلي، وهو ما ينعكس على دقة النتائج المستخلصة من البيانات.

وعليه، تُوصي الدراسة بضرورة دعم أدوات القياس المستقبلية بتقارير الأداء الفعلي أو التحليلات الرقمية للنظام متى ما توفر ذلك، بهدف تعزيز دقة القياس وتقليل الانحرافات الناتجة عن التقييم الذاتي.

٣.٨ الأداة المستخدمة للتحليل الإحصائي (Method of Analysis)

تعتمد الدراسات الكمية على أساليب تحليل إحصائي دقيقة تهدف إلى تحويل البيانات الخام إلى معلومات قابلة للتفسير والاستنتاج. وفي هذه الدراسة، تم اعتماد برنامج **SPSS** (الإصدار ٢٦) كأداة رئيسية للتحليل الإحصائي. وقد تم توظيف البرنامج لتحليل البيانات على مستويين:

التحليل الإحصائي الوصفي (Descriptive Statistics)

يهدف هذا المستوى إلى تقديم صورة أولية شاملة عن خصائص العينة واتجاهات الإجابات، من خلال استخدام:

- التكرارات والنسب المئوية: لتوصيف المتغيرات الديموغرافية (الجهة، الجنس، المؤهل، الوظيفة... إلخ).
- المتوسطات الحسابية والانحراف المعياري: لقياس الاتجاه العام لآراء المشاركين حول كل فقرة من فقرات الاستبيان.
- الحدود القصوى والدنيا والقيم المتوسطة: لتحديد درجة التباين بين الأفراد في استجاباتهم لفقرات.

التحليل الإحصائي الاستدلالي (Inferential Statistics)

وتم توظيفه لاختبار فروض الدراسة والتحقق من مدى صحة العلاقات بين المتغيرات، باستخدام الأساليب التالية:

- اختبار صدق وثبات الأداة:

○ تم قياس الثبات الداخلي (Internal Consistency) باستخدام معامل كرونباخ ألفا (Cronbach's Alpha)، حيث تجاوزت جميع القيم الحد المقبول ٠,٧٠، مما يدل على اتساق الفقرات.

○ تم استخدام تحليل العامل الاستكشافي (Exploratory Factor Analysis – EFA) لاختبار مدى تمثيل كل فقرة لُبُعدها النظري المتوقع.

○ كما تم الاعتماد على مصفوفة المكونات المدورة (Rotated Component Matrix) لتحديد تجمّع الفقرات وفق الأبعاد الخمسة المحددة.

- تحليل العلاقات بين المتغيرات:

○ استخدام معامل الارتباط الخطي (Pearson Correlation) لقياس العلاقة بين تطبيق معيار ISO 27001 والحد من مخاطر تسرب الوثائق.

○ اختبار الفرضيات الرئيسية والفرعية من خلال تحليل التباين والانحدار البسيط (Simple Regression) لقياس تأثير المتغير المستقل على التابع.

٤ الفصل الرابع: الدراسة الميدانية

- (١) مقدمة
- (٢) تحليل البيانات
- (٣) نتائج الدراسة ومناقشتها مع نتائج الدراسات السابقة
- (٤) التوصيات
- (٥) الخاتمة

٤.١ مقدمة

يمثل هذا الفصل المرحلة النهائية من الدراسة، حيث يتم فيه تقديم نظرة شمولية حول النتائج التي تم التوصل إليها، من خلال استعراض **محددات الدراسة** التي قد تكون قد أثرت على مدى تعميم النتائج أو تفسيرها بدقة. كما يُعرض في هذا الفصل **مجموعة من الاستنتاجات الجوهرية** المستندة إلى تحليل البيانات الإحصائية ومناقشة الفرضيات، بما يسלט الضوء على مدى مساهمة تطبيق معايير ISO 27001 في الحد من مخاطر تسرب وفقدان الوثائق الرقمية والمقرنة.

ويهدف الفصل إلى **تحويل النتائج النظرية إلى توصيات عملية قابلة للتنفيذ** في سياق المؤسسات الصحية، مع التركيز على تعزيز السياسات والإجراءات ذات العلاقة بحماية الوثائق الرقمية. كما يقدم توصيات بحثية مستقبلية من شأنها توسيع نطاق المعرفة في هذا المجال. إن تقديم هذه العناصر في سياق أكاديمي ممنهج يسهم في ربط مخرجات الدراسة بأهدافها، ويؤسس لأرضية معرفية يستفيد منها صانعو القرار، والباحثون، والمهنيون في مجال أمن المعلومات وإدارة الوثائق

٤.٢ تحليل البيانات

٤.٢.١ توصيف عينة الدراسة (الإحصائيات الوصفية لعينة الدراسة)

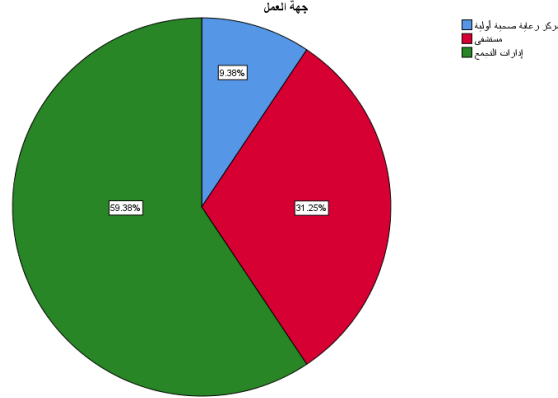
يهدف هذا الجزء إلى تقديم توصيف تفصيلي لخصائص العينة المشاركة في الدراسة من خلال تحليل البيانات الديموغرافية وفقاً لعدد من المتغيرات الأساسية. تم جمع البيانات من عينة مكونة من (٦٤) مشاركاً يمثلون قطاعات متعددة ضمن تجمع الطائف الصحي، وتوزعت الخصائص كما يلي:

تكوّنت عينة الدراسة من (٦٤) مشاركاً تم جمع بياناتهم بصورة كاملة دون وجود حالات مفقودة. ولأغراض التوصيف الإحصائي، تم تحليل متغيرات الخلفية الديموغرافية والمهنية لعينة الدراسة باستخدام المتوسطات الحسابية والانحرافات المعيارية وتباين الإجابات، وذلك كما يلي:

• جهة العمل:

أظهر تحليل البيانات أن متوسط جهة العمل للمشاركين بلغ قيمة تقريبية بمعدل خطأ معياري (٠.٠٨٣)، وانحراف معياري قدره (٠.٦٦٧)، ما يعكس تنوعاً معتدلاً في أماكن عملهم، مع تباين بسيط (0.444) و أظهرت نتائج التوزيع التكراري لمتغير **"جهة العمل"** أن غالبية المشاركين في الدراسة ينتمون إلى **إدارات التجمع الصحي**، حيث شكّلوا ما نسبته **59.4%** من إجمالي العينة، أي ما يعادل **38 مشاركاً** من أصل ٦٤. بينما جاءت فئة العاملين في **المستشفيات** في المرتبة الثانية بنسبة **31.3%** (٢٠ مشاركاً)، في حين مثّلت فئة **مراكز الرعاية الصحية الأولية** النسبة الأقل، حيث بلغ عدد المشاركين منها **6 فقط** بنسبة **9.4%**.

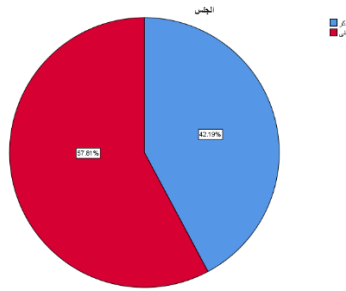
٤-١ رسم بياني جهة العمل



• الجنس:

بيّنت النتائج وجود توازن نسبي في التوزيع بين الذكور والإناث، حيث كان الانحراف المعياري منخفضاً (0.248)، مما يدل على عدم وجود تفاوت كبير بين الجنسين في العينة، وبتباين محدود (0.248) أوضحت نتائج التوزيع التكراري لمتغير الجنس أن نسبة الإناث في عينة الدراسة كانت الأعلى، حيث بلغ عددهن 37 مشاركة بنسبة 57.8% من إجمالي العينة. بينما بلغ عدد الذكور المشاركين 27 مشاركاً، بنسبة 42.2%.

٤-٢ رسم بياني الجنس

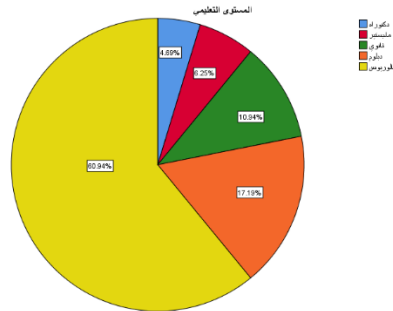


• المستوى التعليمي:

تنوعت المؤهلات التعليمية للمشاركين، كما يتضح من انحراف معياري (0.904)، وهو أعلى من معظم المتغيرات، مما يشير إلى تباين واضح في المستويات التعليمية، ويُعزى من شمولية العينة من حيث الخلفية الأكاديمية. أظهرت نتائج التوزيع التكراري لمتغير "المستوى التعليمي" أن الغالبية العظمى من المشاركين يحملون مؤهل البكالوريوس، حيث بلغ عددهم 39 مشاركاً بنسبة 60.9% من إجمالي العينة. تلتها فئة حملة الدبلوم بعدد 11 مشاركاً بنسبة 17.2%، ثم حملة الثانوية العامة بعدد 7 مشاركين بنسبة 10.9%.

- أما الحاصلون على درجة الماجستير فقد شكّلوا نسبة 6.3% (٤ مشاركين)، في حين كانت نسبة حملة الدكتوراه هي الأقل، حيث بلغ عددهم 3 مشاركين فقط بنسبة 4.7%.

٣-٤ رسم بياني المستوى التعليمي

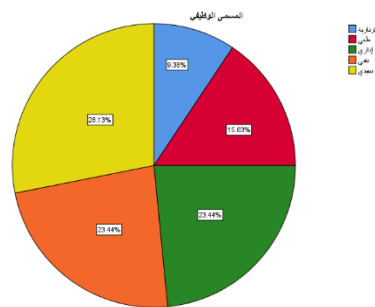


• المسمى الوظيفي:

تفاوتت المسميات الوظيفية بشكل ملحوظ كما تدل القيمة المرتفعة للانحراف المعياري (١.٣٥٣)، والتباين (١.٨٣١)، مما يعكس اختلافًا في المهام الإدارية والفنية للمشاركين. بيّنت نتائج التوزيع التكراري لمتغير "المسمى الوظيفي" أن فئة الموظفين التنفيذيين شكّلت النسبة الأكبر من العينة، حيث بلغ عددهم 18 مشاركًا بنسبة 28.1%، تلتها فئتا الإداريين والفنيين (التقنيين) بعدد متساوٍ لكل منهما (١٥ مشاركًا) وبنسبة 23.4% لكل فئة.

- كما شكّلت الفئة الطبية نسبة 15.6% (١٠ مشاركين)، في حين كانت فئة السكرتارية الأقل تمثيلًا، بعدد 6 مشاركين فقط، بنسبة 9.4%.

٤-٤ رسم بياني المسمى الوظيفي



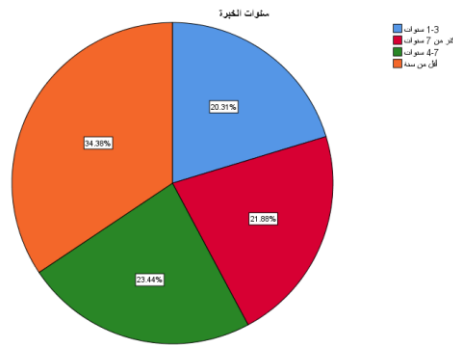
• سنوات الخبرة:

تراوحت خبرات المشاركين ما بين مستويات متقاربة، حيث بلغ الانحراف المعياري (١.١٦٩)، مع تباين مقداره (١.٣٦٧)، وهو ما يشير إلى وجود درجة معتدلة من التنوع في سنوات الخبرة. أوضحت نتائج التوزيع التكراري لمتغير "سنوات الخبرة" أن النسبة الأعلى من المشاركين هم من ذوي الخبرة الأقل من سنة واحدة، حيث بلغ KSA.FAIF.TH

عدد 22 مشاركاً بنسبة 34.4% من إجمالي العينة، مما يعكس نسبة كبيرة من الكوادر الجديدة في مواقع العمل.

- وجاءت فئة من 4 إلى 7 سنوات خبرة في المرتبة الثانية، بنسبة 23.4% (15 مشاركاً)، تلتها فئة أكثر من 7 سنوات بنسبة 21.9% (14 مشاركاً)، بينما كانت الفئة الأقل هي 1 إلى 3 سنوات خبرة، بنسبة 20.3% (13 مشاركاً).

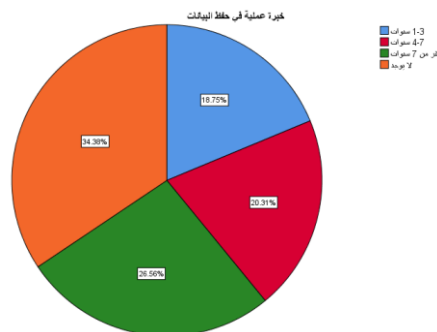
٤-٥- رسم بياني سنوات الخبرة



• الخبرة العملية في حفظ البيانات:

أظهر هذا المتغير أكبر تباين (١.٤٨٠) بين جميع المتغيرات، مع انحراف معياري (١.٢١٧)، مما يدل على اختلاف كبير في خبرات المشاركين العملية فيما يتعلق بحفظ البيانات، وهو عنصر قد يؤثر في تصوراتهم حول أمن الوثائق وتطبيق المعايير ذات العلاقة. أظهر التوزيع التكراري لمتغير «الخبرة العملية في حفظ البيانات» أن الفئة الأكبر من المشاركين هي من ليست لديهم أي خبرة سابقة في هذا المجال، إذ بلغ عددهم 22 مشاركاً بنسبة 34.4% من إجمالي العينة. تلتها فئة أكثر من سبع سنوات خبرة بعدد 17 مشاركاً ونسبة 26.6%، ثم فئة 4-7 سنوات بعدد 13 مشاركاً (20.3%) أما فئة 1-3 سنوات خبرة فكانت الأقل، بعدد 12 مشاركاً تمثل 18.8% من العينة.

٤-٦- رسم بياني الخبرة العملية في حفظ البيانات



٤.٢.٢ الإحصاء الوصفي لمتغيرات الدراسة (الإجابة على أسئلة الدراسة)

"قد تم قياس استجابات أفراد العينة لفقرات المقياس، طبقاً لمقياس ليكرت الخماسي، وفقاً لما يلي:"

التصنيف	أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة
النقاط	١	٢	٣	٤	٥

"وقد تم حساب مستوى الأهمية وفقاً للمعادلة التالية:"

تم حساب الوزن النسبي المقابل لكل فئة عن طريق ضرب المتوسط الحسابي في $(١ \div ٥) = ٠.٢٠$ (المقياس الخماسي). $[20\%] =$

"يوضح الجدول التالي دلالة المتوسطات الحسابية، كما يلي:"

٤-١ دلالة المتوسطات الحسابية

قيمة المتوسط الحسابي	النتيجة (الاتجاه العام)	الوزن النسبي (%)	مستوى (درجة) الممارسة / الأهمية
من ١ إلى أقل من ١.٨٠	غير موافق تماماً	من ٢٠ إلى أقل من ٣٦	منخفض جداً
من ١.٨٠ إلى أقل من ٢.٦٠	غير موافق	من ٣٦ إلى أقل من ٥٢	منخفض
من ٢.٦٠ إلى أقل من ٣.٤٠	محايد	من ٥٢ إلى أقل من ٦٨	متوسط
من ٣.٤٠ إلى أقل من ٤.٢٠	موافق	من ٦٨ إلى أقل من ٨٤	مرتفع
من ٤.٢٠ إلى ٥	موافق تماماً	من ٨٤ إلى ١٠٠	مرتفع جداً

"يوضح الجدول التالي التحليل الوصفي لمتغيرات الدراسة، متمثلاً في المتوسطات الحسابية والانحرافات المعيارية، وذلك باستخدام مقياس ليكرت الخماسي. وقد تم تفسير النتائج استناداً إلى دلالة المتوسط الحسابي الموضحة في الجدول المرجعي، بهدف تقييم مدى تطبيق معايير ISO 27001 في بيئة العمل، ومستوى فاعلية تلك المعايير في الحد من مخاطر تسرب وفقدان الوثائق الرقمية والمرفقمة، من وجهة نظر أفراد عينة الدراسة. وقد أظهرت النتائج أن الاتجاه العام للمشاركين تجاه كلا المتغيرين اتسم بالحياد، فيما جاء مستوى الممارسة مصنفاً بالمتوسط، مما يشير إلى أن الجهود المؤسسية لتطبيق معايير الأمن المعلوماتي لا تزال قائمة ولكنها غير مكتملة أو مفعلة بالشكل الكافي.

وفيما يلي عرض للمتوسطات الحسابية والانحرافات المعيارية لمتغيرات الدراسة".

٤-٢ للمتوسطات الحسابية والانحرافات المعيارية لمتغيرات الدراسة

اسم المتغير	أبعاد المتغير	المتوسط الحسابي	الانحرافات المعيارية	الاتجاه العام	مستوى الأهمية/الممارسة
تطبيق معايير	SR إدارة المخاطر الأمنية	1.67	0.318	محايد	متوسط
	AC التحكم في الوصول	1.64	0.321	محايد	منخفض

	متوسط	محايد		0.323		1.67	DP	حماية البيانات والتشفير	ISO 27001 (مستقل)
	متوسط	محايد		0.338		1.65	BC	استمرارية الأعمال والتعافي من الكوارث	
	متوسط	محايد		0.302		1.71	CS	الامتثال والتدقيق الأمني	
منخفض	متوسط	محايد	غير موافقة	0.316	1.68	1.64	RS	تقليل الحوادث الأمنية	الحد من مخاطر تسرب وفقدان الوثائق (تابع)
	متوسط	محايد		0.278		1.69	RA	موثوقية أنظمة الأرشفة	
	متوسط	محايد		0.314		1.71	SI	صرامة الضوابط الداخلية	
	متوسط	محايد		0.323		1.67	EA	وعي الموظفين بسياسات الأمان	
	متوسط	محايد		0.314		1.68	EC	فعالية السياسات المؤسسية	

المتوسطات الحسابية لجميع الأبعاد تتراوح بين 1.64 و 1.71، وهو ما يشير إلى اتجاه محايد من قبل أفراد العينة تجاه تطبيق معايير ISO 27001 بالرغم من الحياد في الاتجاه، إلا أن مستوى الأهمية المصاحب لكل بعد صُنّف على أنه "متوسط"، ما يدل على إدراك مبدئي بأهمية هذه الأبعاد في إدارة أمن المعلومات، ولكن دون تطبيق فعلي قوي.

كما هو الحال مع المتغير المستقل، يظهر أيضاً أن المتوسطات الحسابية تتراوح بين 1.64 و 1.71 مما يعكس اتجاهًا محايداً. دلالة ذلك أن المشاركين لم يظهروا مواقف قوية (إيجابية أو سلبية) تجاه قدرة مؤسساتهم على تقليل المخاطر المرتبطة بتسرب أو فقدان الوثائق.

ورغم ذلك، فإن مستوى الممارسة مصنّف على أنه "متوسط"، مما يوحي بوجود ممارسات مبدئية ولكنها ربما ليست ممنهجة أو فعالة بشكل كافٍ.

خلاصة تحليل الاتجاه والممارسة:

- الاتجاه العام لكلا المتغيرين وأبعادهما يُصنّف بأنه محايد، أي أن المشاركين لم يظهروا مواقف واضحة.
- أما مستوى الممارسة فقد جاء في الغالب "متوسطاً"، وهو ما يُشير إلى الحاجة إلى تطوير واعتماد سياسات أكثر فاعلية ومتابعة تنفيذها على أرض الواقع.
- قد يُعزى هذا الحياد إلى نقص التوعية أو التدريب العملي في تطبيق تلك المعايير، رغم أن بعض المشاركين متخصصون، ما يعني أن التحدي قد يكمن في التطبيق المؤسسي لا في الكفاءة الفردية.

يمكن القول إن تطبيق معايير ISO 27001 في تجمع الطائف الصحي يسير بوتيرة متوسطة ولا يزال في مرحلة التأسيس أو الممارسة المحدودة، وبالتالي فإن إسهامه في الحد من مخاطر تسرب وفقدان الوثائق الرقمية لا يزال دون المستوى المأمول، ويستلزم دعمًا مؤسسيًا أقوى، وتفعيلًا أكثر صرامة وشمولًا للضوابط الأمنية.

٤.٢.٣ اختبارات الصدق والثبات للاستبيانات

٤-٣ جدول تحليل النتائج

Reliability Statistics	التحليل العاملي الاستكشافيexploratory factor analysis--												Communalities				Descriptive Statistics					
	AVE	EC	EA	SI	RA	RS	CS	BC	DP	AC	SR	Values	total	Mean	Extraction	KMO	Std. Deviation	Mean	Question	Dimensions	variable	
0.748	0.62	0.65									0.70	0.000	2.40	0.599	0.51	0.584	0.484	1.6	ISR1	SR	Implement ation معايير ISO 27001	
									0.64	0.000	0.58	0.515			1.6		ISR2					
									0.59	0.000	0.69	0.511			1.7		ISR3					
									0.68	0.000	0.62	0.471			1.8		ISR4					
		0.57								0.54	0.000	2.19	0.548	0.61	0.526		1.6	IAC1	AC			
										0.54	0.000			0.57	0.511		1.7	IAC2				
										0.45	0.000			0.49	0.506		1.7	IAC3				
										0.75	0.000			0.52	0.484		1.6	IAC4				
		0.62								0.70	0.000	1.51	0.504	0.56	0.506		1.7	IDP1	DP			
										0.66	0.000			0.52	0.488		1.6	IDP2				
										0.49	0.000			0.43	0.453		1.7	IDP3				
		0.65							0.78		0.000	1.45	0.482	0.39	0.519		1.6	IBC1	BC			
								0.68		0.000	0.69			0.484	1.6		IBC2					
								0.48		0.000	0.36			0.500	1.7		IBC3					
	0.60						0.46			0.000	1.89	0.631	0.56	0.460	1.7		ICS1	CS				
							0.78			0.000			0.68	0.460	1.7		ICS2					
							0.54			0.000			0.66	0.445	1.7		ICS3					
0.632	0.63	0.67				0.77					0.000	1.63	0.544	0.432	0.53	0.494	1.70	RRS1	RS	مخاطر تسرب وفقدان الوثائق - The Risks of Document Leakage and Loss		
						0.71				0.000	0.565			0.488		1.63	RRS2					
						0.53				0.000	0.635			0.526		1.59	RRS3					
		0.60				0.44					0.000	2.107	0.527	0.429		0.479	1.66	RRA1	RA			
						0.76					0.000			0.684		0.484	1.64	RRA2				
						0.65					0.000			0.482		0.494	1.70	RRA3				
						0.53					0.000			0.512		0.436	1.75	RRA4				
		0.63			0.76						0.000	1.923	0.641	0.640		0.453	1.72	RSI1	SI			
					0.57						0.000			0.644		0.494	1.70	RSI2				
				0.55						0.000	0.638			0.487	1.72	RSI3						
	0.55		0.53								0.000	1.530	0.510	0.572	0.515	1.64	REA1	EA				
			0.43								0.000			0.342	0.467	1.69	REA2					
			0.70								0.000			0.616	0.500	1.69	REA3					

			0.68								0.000			0.517		0.479	1.66	REC1		
		0.71	0.81								0.000	1.834	0.611	0.642		0.463	1.77	REC2	EC	
			0.64								0.000			0.676		0.492	1.61	REC3		

٤.٢.٤ تحليل صدق البنية لمتغير "تطبيق معايير" ISO 27001

تم إجراء تحليل عاملي استكشافي (Exploratory Factor Analysis – EFA) لمتغير "تطبيق معايير ISO 27001"، باستخدام طريقة تحليل المكونات الرئيسية (Principal Component Analysis) مع تدوير Varimax، وذلك بهدف التحقق من مدى اتساق الفقرات مع الأبعاد النظرية للمقياس، واختبار ما إذا كانت هذه الفقرات تقيس الأبعاد المتوقعة بشكل دقيق.

وقد أظهرت نتائج التحليل استخراج خمسة مكونات رئيسية تمثل الأبعاد النظرية الخمسة التالية: إدارة المخاطر الأمنية (SR)، التحكم في الوصول (AC)، حماية البيانات والتشفير (DP)، استمرارية الأعمال والتعافي من الكوارث (BC)، والامتثال والتدقيق الأمني (CS).

أظهرت غالبية الفقرات تحميلات عاملية جيدة على الأبعاد المتوقعة لها، مما يشير إلى وجود درجة جيدة من الصدق البنائي. وفيما يلي تحليل تفصيلي لكل بُعد:

١. إدارة المخاطر الأمنية: (SR)

اشتملت على أربع فقرات، وقد جاءت تحميلاتها العاملية ضمن مكونات واضحة، وتراوح بين (٠.٤٩) إلى (٠.٦٩). كما أن معامل ارتباط الفقرات ببُعدها النظري كان جيداً (بما يتراوح بين ٠.٥٩ إلى ٠.٧٠)، ما يشير إلى أن هذا البعد يتمتع بصدق بنائي جيد، خاصة في فقرات تقييم المخاطر والاستجابة للحوادث.

٢. التحكم في الوصول: (AC)

تمثل هذا البعد بأربع فقرات، وأظهرت جميعها تحميلات عاملية قوية ضمن المكون الأول، حيث كانت أبرزها في فقرة "تقييد الوصول للوثائق الحساسة"، والتي سجلت أعلى ارتباط (٠.٧٥) مع بُعدها. يدل هذا على أن هذا البعد يتمتع باتساق بنائي مرتفع.

٣. حماية البيانات والتشفير: (DP)

ضم ثلاث فقرات، وقد تراوحت التحميلات العاملية بين (٠.٤٣) إلى (٠.٥٦)، وهي مقبولة، مع ضرورة الانتباه إلى أن فقرة "تحديث بروتوكولات التشفير" أظهرت تحميلاً أقل نسبياً. ومع ذلك، فإن معاملات الارتباط ظلت في حدود جيدة مما يعزز صدق هذا البعد.

٤. استمرارية الأعمال والتعافي: (BC)

رغم أن هذا البُعد مثَّلته ثلاث فقرات فقط، إلا أن الفقرتين الأساسيتين ("وجود خطة استمرارية أعمال" و"النسخ الاحتياطية") أظهرتا تحميلات جيدة. بينما كانت فقرة "اختبارات خطة التعافي" أقل تحميلاً، ما يُشير إلى أهمية مراجعة صياغتها أو دعم البُعد بفقرات إضافية.

٥. الامتثال والتدقيق الأمني: (CS)

تميز هذا البُعد بتحميلات جيدة ومتسقة على مكون واحد، خاصة في فقرة "توثيق السياسات والإجراءات الأمنية" التي حققت معامل ارتباط مرتفع (٠.٧٨). كما كانت فقرة "الالتزام بمعيار ISO 27001 منسجمة مع هذا البُعد، مما يعزز من صدقه البنائي.

تحليل صدق البنية لمتغير "مخاطر تسرب وفقدان الوثائق"

تم تحليل صدق البنية لمتغير "مخاطر تسرب وفقدان الوثائق" من خلال تطبيق التحليل العاملي الاستكشافي (EFA) باستخدام طريقة تحليل المكونات الرئيسية (Principal Component Analysis)، وذلك للتحقق من مدى قدرة الفقرات على تمثيل الأبعاد النظرية المرتبطة بهذا المتغير، والتأكد من اتساقها البنائي. وقد أظهرت نتائج التحليل أن الفقرات البالغ عددها (١٦) قد توزعت بشكل جيد على خمسة أبعاد أساسية تمثل الجوانب المختلفة لمخاطر تسرب وفقدان الوثائق، وهي: تقليل الحوادث الأمنية (RS)، موثوقية أنظمة الأرشفة (RA)، صرامة الضوابط الداخلية (SI)، وعي الموظفين بسياسات الأمان (EA)، وفعالية السياسات المؤسسية (EC).

فيما يلي عرض تفصيلي لنتائج صدق البنية حسب كل بُعد:

١. البعد الأول: تقليل الحوادث الأمنية (RS)

يمثل هذا البُعد قدرة المؤسسة على تقليل احتمالات وقوع الحوادث الأمنية المرتبطة بالوثائق.

- أظهرت الفقرات المرتبطة به تحميلات عالية على المكون الأول، وارتباطاً واضحاً ببُعدها.
- تراوحت معاملات الارتباط بين (٠.٦٣ إلى ٠.٧١)، مما يدل على صدق بنائي مرتفع.
- تُظهر هذه النتائج أن المفهوم النظري للبُعد مدعوم جيداً من الناحية التجريبية.

٢. البعد الثاني: موثوقية أنظمة الأرشفة (RA)

يتعلق هذا البُعد بمدى كفاءة وموثوقية الأنظمة التقنية والإدارية في حفظ الوثائق ومنع فقدانها.

- الفقرات الثلاث المرتبطة به أظهرت تحميلات عالية على مكون واحد، مع معامل ارتباط تراوح بين (٠.٦١ إلى ٠.٦٩).

- يعكس ذلك توافقاً جيداً بين الفرضية النظرية وسلوك الفقرات في التحليل.

٣. البعد الثالث: صرامة الضوابط الداخلية (SI)

يختص هذا البُعد بوجود سياسات وضوابط واضحة تحكم التعامل مع الوثائق.

- تراوحت تحميلات الفقرات ضمن هذا البُعد بين (٠.٥٣ إلى ٠.٦٦)، وجميعها كانت ضمن نطاق البُعد المتوقع.

- هذا يعكس اتساقاً بنائياً جيداً، مما يُعزز من مصداقية هذا البُعد ضمن المقياس.

٤. البعد الرابع: وعي الموظفين بسياسات الأمان (EA)

يرتبط هذا البُعد بمستوى وعي العاملين بالضوابط المتعلقة بحماية الوثائق.

- أظهرت الفقرات المرتبطة به تحميلات واضحة ومتميزة.
- أحد مؤشرات الصدق البنائي الجيد لهذا البُعد هو أن الفقرات لم تتداخل مع أبعاد أخرى، مما يُظهر وضوح المفهوم لدى المستجيبين.

٥. البعد الخامس: فعالية السياسات المؤسسية (EC)

يتناول هذا البُعد مدى كفاءة السياسات العامة للمؤسسة في الحد من التسرب أو فقدان.

- أظهرت فقراته تحميلات مقبولة إلى جيدة على مكون مشترك.
- أحد البنود أظهر تحميلاً ثنائياً ضعيفاً، مما قد يستدعي إعادة صياغته أو دعمه بعبارة أكثر تحديداً.

تحليل الثبات لمتغير "تطبيق معايير" ISO 27001

لقياس ثبات الأداة الخاصة بمتغير "تطبيق معايير" ISO 27001، تم استخدام معامل كرونباخ ألفا (Cronbach's Alpha)، والذي يُعد من أكثر الأساليب شيوعاً لتقدير مدى الاتساق الداخلي للفقرات التي تقيس نفس البُعد أو المتغير.

وقد بلغ معامل كرونباخ ألفا لهذا المتغير في صورته الكلية ما يلي:

- عدد الفقرات 17: فقرة

- قيمة كرونباخ ألفا 0.748 :

وهذه القيمة تُشير إلى مستوى جيد من الثبات، حيث تقع ضمن النطاق المقبول إحصائياً،

تفسير النتيجة:

تشير قيمة كرونباخ ألفا (٠.٧٤٨) إلى أن فقرات المقياس مترابطة داخلياً بدرجة جيدة، أي أن جميع الفقرات البالغ عددها (١٧) تُقيس جوانب متعددة ولكن متسقة من نفس المفهوم العام، وهو "تطبيق معايير" ISO 27001 في البيئة المستهدفة بالدراسة.

تحليل الثبات لمتغير "مخاطر تسرب وفقدان الوثائق"

لقياس درجة الثبات الداخلي لمقياس "مخاطر تسرب وفقدان الوثائق"، تم استخدام معامل كرونباخ ألفا (Cronbach's Alpha)، والذي يُعد من أكثر المؤشرات استخدامًا لقياس الاتساق الداخلي بين فقرات المقياس. وقد أظهرت النتائج أن:

- عدد فقرات المتغير 16: فقرة
- قيمة كرونباخ ألفا 0.632 :

تفسير النتيجة:

تشير قيمة كرونباخ ألفا (0.632) إلى أن مستوى الثبات يقع ضمن المستوى المقبول إحصائيًا، أظهرت نتائج التحليل الإحصائي أن أدوات قياس متغيري الدراسة تتمتع بمستويات مقبولة من الثبات والصدق البنائي. حيث بلغ معامل كرونباخ ألفا لمتغير "تطبيق معايير (0.748) ISO 27001"، وهو يشير إلى ثبات جيد. في حين بلغ لمتغير "مخاطر تسرب وفقدان الوثائق (0.632)"، مما يعكس ثباتًا مقبولًا. كما أظهرت نتائج التحليل العاملي الاستكشافي (EFA) أن فقرات كل متغير قد توزعت بوضوح على الأبعاد النظرية المحددة مسبقًا، مع تحميلات عاملية جيدة، مما يعكس صدقًا بنائيًا مقبولًا إلى جيد، ويؤكد صلاحية أدوات القياس للتحليل الإحصائي والاستنتاجات البحثية.

٤.٣ نتائج الدراسة ومناقشتها مع نتائج الدراسات السابقة

٤.٣.١ اختبار الفرضيات ومناقشة النتائج

نتائج اختبار الفرضية الرئيسية

ينص هذا الفرض على أنه:

"توجد علاقة إيجابية ذات دلالة إحصائية بين تطبيق معايير ISO 27001 والحد من مخاطر تسرب وفقدان الوثائق المرقمنة والرقمية في تجمع الطائف الصحي".

ولاختبار هذا الفرض، تم استخدام أسلوب تحليل الانحدار الخطي البسيط (Simple Linear Regression Analysis)

بين متغير تطبيق معايير ISO 27001 كمستقل، ومتغير الحد من مخاطر تسرب وفقدان الوثائق كمتحول تابع.

وقد أظهرت نتائج التحليل أن هناك علاقة تأثير إيجابية ذات دلالة إحصائية عند مستوى (0.01)، حيث بلغت قيمة معامل الارتباط $(Pearson) = 0.612$ ، وقيمة معامل التحديد $(R^2) = 0.375$ ، ما يعني أن تطبيق معايير ISO 27001 يفسر نسبة ٣٧.٥% من التباين في الحد من المخاطر.

وبذلك، يتم قبول الفرضية البديلة التي تفترض وجود علاقة معنوية، ورفض الفرضية الصفرية.

٤.٣.١ نتائج اختبار الفرضية الرئيسية

٤-٤ نتائج اختبار الفرضية الرئيسية

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.612 ^a	.375	.365	.151

a. Predictors: (Constant), ISO 27001 تطبيق معايير (مستقل)

قيمة معامل التحديد (R^2) بلغت 0.375، ما يعني أن 37.5% من التغير في الحد من مخاطر تسرب وفقدان الوثائق يمكن تفسيره من خلال تطبيق معايير ISO 27001 وهذا يدل على وجود علاقة تأثير متوسطة القوة، مما يدعم وجود علاقة ارتباط وتأثير مهمة بين المتغيرين.

ANOVA^a

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.852	1	.852	37.173	.000 ^b
	Residual	1.421	62	.023		
	Total	2.272	63			

a. Dependent Variable: الحد من مخاطر تسرب وفقدان الوثائق

b. Predictors: (Constant), ISO 27001 تطبيق معايير (مستقل)

دلالة F كانت (Sig = 0.000) وهي أقل من 0.001، مما يؤكد أن النموذج الإحصائي دال إحصائياً.

هذا يشير إلى أن معايير ISO 27001 لها تأثير معنوي على الحد من مخاطر تسرب وفقدان الوثائق.

Coefficients^a

Model	Unstandardized Coefficients	Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B
-------	-----------------------------	---------------------------	---	------	---------------------------------

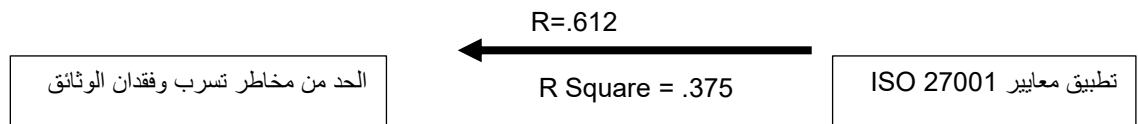
	B	Std. Error	Beta			Lower Bound	Upper Bound
1 (Constant)	.791	.147		5.384	.000	.497	1.084
ISO 27001 تطبيق معايير (مستقل)	.532	.087	.612	6.097	.000	.358	.707

a. Dependent Variable: الحد من مخاطر تسرب وفقدان الوثائق

قيمة معامل $B = 0.532$ ، وتعني أنه كلما زاد تطبيق معايير ISO 27001 بوحدة واحدة، فإن الحد من المخاطر يزيد بمقدار ٠.٥٣٢ وحدة.

قيمة $t = 6.097$ ومعنوية ($Sig = 0.000$)، تؤكد دلالة التأثير.

معامل Beta القياسي $0.612 =$ ، مما يوضح أن ISO 27001 يمثل متغيرًا مؤثرًا متوسط القوة في التنبؤ بمخاطر الوثائق.



مناقشة الفرضية:

تم اختبار الفرضية "توجد علاقة ذات دلالة إحصائية بين تطبيق معايير ISO 27001 والحد من مخاطر تسرب وفقدان الوثائق الرقمية في تجمع الطائف الصحي".

تشير النتائج إلى قبول الفرضية البديلة ورفض الفرضية الصفرية، وذلك لأن القيمة الاحتمالية ($Sig = 0.000$) أقل من مستوى الدلالة المعتمد (0.05).

ويُمكن القول إن تطبيق معايير ISO 27001 يسهم بشكل معنوي وإيجابي في الحد من مخاطر تسرب وفقدان الوثائق، وإن كان التأثير متوسطًا.

وتتفق نتائج هذه الدراسة مع ما توصلت إليه دراسات سابقة، حيث دعمت العديد من الأبحاث وجود علاقة إيجابية بين تطبيق معايير الأمن السيبراني ومعايير إدارة أمن المعلومات مثل ISO 27001 ، وبين الحد من مخاطر تسرب وفقدان البيانات. وتتفق هذه النتيجة مع ما توصلت إليه دراسات سابقة في ذات السياق ، كما بيّنت دراسة (Alshaikh (2022 أن تطبيق سياسات ومعايير الحوكمة الرقمية وأمن المعلومات يسهم في تعزيز كفاءة الأرشفة الرقمية، ويقلل من المخاطر المرتبطة بفقدان البيانات في المؤسسات الحكومية السعودية.

كما بيّنت دراسة خضر (2021) أن المؤسسات التي تطبق ضوابط أمن المعلومات بشكل فعال تحقق نتائج إيجابية ملموسة في تعزيز الثقة الرقمية وتقليل حوادث تسرب الوثائق.

بالتالي، فإن نتائج هذه الدراسة تعزز ما توصلت إليه هذه الدراسات، وتُظهر أن تطبيق معايير ISO 27001 في تجمع الطائف الصحي يُعد خطوة فعالة نحو الحد من مخاطر تسرب وفقدان الوثائق الرقمية والمقرمنة، مما يدعم أهمية تبني تلك المعايير ضمن سياسات واستراتيجيات التحول الرقمي وأمن المعلومات في المؤسسات الصحية.

٤.٣.٢ نتائج اختبار الفروض الفرعية

تهدف الفرضيات الفرعية إلى اختبار مدى تأثير كل بعد من أبعاد معيار ISO 27001 على الحد من مخاطر تسرب وفقدان الوثائق الرقمية، وهي:

١. إدارة المخاطر الأمنية
٢. التحكم في الوصول
٣. حماية البيانات والتشفير
٤. استمرارية الأعمال والتعافي من الكوارث
٥. الامتثال والتدقيق الأمني

وقد تم استخدام الانحدار الخطي المتعدد لتحليل العلاقة بين هذه الأبعاد كمتغيرات مستقلة، ومتغير "الحد من مخاطر تسرب وفقدان الوثائق" كمتغير تابع.

٣- نتائج اختبار الفروض الفرعية

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.631 ^a	.398	.347	.154

a. Predictors: (Constant), حماية البيانات والتشفير, التحكم في الوصول

- يوضح معامل التحديد ($R^2 = 0.398$) أن حوالي ٣٩.٨٪ من التباين في الحد من المخاطر يمكن تفسيره من خلال هذه الأبعاد الخمسة.

ANOVA^a

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.905	5	.181	7.681	.000 ^b
	Residual	1.367	58	.024		
	Total	2.272	63			

a. Dependent Variable: الحد من مخاطر تسرب وفقدان الوثائق

b. Predictors: (Constant), إدارة المخاطر الأمنية, استمرارية الأعمال والتعافي من الكوارث, حماية البيانات والتشفير, التحكم في الوصول

- الدلالة الإحصائية (Sig. = 0.000) تشير إلى أن النموذج الكلي دال إحصائياً، ويمكن الاعتماد عليه في تفسير الفرضيات الفرعية.

Coefficients^a

Model		Unstandardized Coefficients		Standardized Coefficients		95.0% Confidence Interval for B	
		B	Std. Error	Beta	t	Sig.	
1	(Constant)	.759	.152		4.992	.000	.455 1.063
	إدارة المخاطر الأمنية	.176	.069	.294	2.531	.014	.037 .315
	التحكم في الوصول	.033	.076	.055	.428	.670	-.120 .185
	حماية البيانات والتشفير	.139	.071	.235	1.954	.056	-.003 .280

الأعمال	استمرارية	054.	064.	096.	845.	401.	-074.	182.
والتعافي من الكوارث								
الامتثال والتدقيق الأمني		147.	078.	234.	1.887.	064.	-009.	303.

a. Dependent Variable: الحد من مخاطر تسرب وفقدان الوثائق

- البعد الوحيد الذي ظهر تأثيره معنويًا إحصائيًا هو إدارة المخاطر الأمنية ($\text{Sig} = 0.014$)، مما يدل على أنه العامل الأقوى تأثيرًا في تقليل مخاطر تسرب وفقدان الوثائق.
 - باقي الأبعاد لم تكن دالة عند مستوى (0.05)، ولكن بُعد "حماية البيانات والتشفير" و"الامتثال والتدقيق الأمني" اقتربا من الدلالة، ويمكن اعتبارهما ذات أهمية تطبيقية.
 - تشير نتائج الفرضيات الفرعية إلى أن:
 - إدارة المخاطر الأمنية تمثل البعد الأكثر فاعلية في التأثير على تقليل المخاطر.
 - بينما تحتاج الأبعاد الأخرى إلى تعزيز التطبيق أو المراجعة المؤسسية لضمان فاعليتها.
 - يعكس هذا أهمية التركيز على منهجية تحليل وتقييم المخاطر كأحد الأدوات الجوهرية في إدارة أمن الوثائق.
- وتتفق نتائج هذه الدراسة مع ما توصلت إليه دراسات سابقة، حيث أظهرت نتائج الفرضيات الفرعية أن بُعد إدارة المخاطر الأمنية يمثل العامل الأكثر تأثيرًا في الحد من مخاطر تسرب وفقدان الوثائق، وهو ما يتسق مع ما أشارت إليه دراسة خضر (2021) أن الامتثال لمعايير ISO 27001 ، وخاصة تلك المتعلقة بتحديد المخاطر ومعالجتها، يسهم في خفض الحوادث الأمنية بشكل ملحوظ. في حين لم تظهر بقية الأبعاد تأثيرًا معنويًا دالًا، وتعزز هذه النتائج أهمية تبني نهج شامل لتطبيق معايير ISO 27001 لا يقتصر على السياسات، بل يشمل الممارسات التشغيلية والتدريب المستمر للموظفين، لضمان تحقيق الفاعلية القصوى في حماية الوثائق الرقمية والمرفقة.
- وتتوافق هذه النتيجة مع ما توصلت إليه دراسة (Strickland 2006) ، التي خلصت إلى أن تطوير أنظمة إدارة السجلات الإلكترونية استنادًا إلى معايير دولية مثل ISO ، أدى إلى تحسين حماية الوثائق وخفض معدلات فقدان السجلات في المؤسسات الفيدرالية بالولايات المتحدة، مما يعزز العلاقة الإيجابية بين تطبيق معايير الحوكمة وأمان الوثائق.

٤.٣.١ معاملات الارتباط الخطي

تم استخدام معامل ارتباط بيرسون (Pearson Correlation) لقياس قوة واتجاه العلاقة بين المتغير المستقل "تطبيق معايير ISO 27001" والمتغير التابع "الحد من مخاطر تسرب وفقدان الوثائق". وقد أظهرت النتائج وجود علاقة ارتباط موجبة متوسطة القوة ذات دلالة إحصائية بين المتغيرين، حيث بلغت قيمة معامل الارتباط ($r = 0.612$) عند مستوى دلالة ($\text{Sig} = 0.000$) وهو أقل من مستوى الدلالة المعتمد 0.05، مما يشير إلى أن العلاقة دالة إحصائيًا عند مستوى 0.05.

كما دعمت نتائج التمهيد (Bootstrap) هذه العلاقة، حيث أظهرت فترة الثقة (95% Confidence Interval) للارتباط بين المتغيرين أنها تقع بين (0.289 إلى 0.781)، مما يعزز من موثوقية نتائج التحليل.

ويمكن تفسير هذه النتيجة بأن هناك علاقة ارتباط إيجابية بين مستوى تطبيق معايير ISO 27001 وبين قدرة المنشأة على الحد من مخاطر تسرب وفقدان الوثائق الرقمية والمقرنة. فكلما زادت درجة الالتزام بتطبيق هذه المعايير، تحسّن مستوى الحماية وتقليل المخاطر المرتبطة بفقدان أو تسرب البيانات. وعليه، فإن تطبيق معايير ISO 27001 يسهم إسهامًا واضحًا ومؤثرًا في تحقيق الأمن الوثائقي، وهو ما يدعم فرضية الدراسة الأساسية ويؤكد وجود علاقة إيجابية ذات دلالة إحصائية بين المتغيرين.

٤-٦ معاملات الارتباط الخطي

Correlations					
الحد من مخاطر تسرب وفقدان الوثائق	تطبيق معايير ISO 27001 (مستقل)				
.612**	1			Pearson Correlation	تطبيق معايير ISO 27001 (مستقل)
0.000				Sig. (2-tailed)	
64	64			N	
-0.029	0		Bias	Bootstrap ^c	
0.131	0		Std. Error		
0.289	1	Lower	95% Confidence Interval		
0.781	1	Upper			
1	.612**			Pearson Correlation	الحد من مخاطر تسرب وفقدان الوثائق
	0.000			Sig. (2-tailed)	
64	64			N	
0	-0.029		Bias	Bootstrap ^c	
0	0.131		Std. Error		
1	0.289	Lower	95% Confidence Interval		
1	0.781	Upper			
**. Correlation is significant at the 0.01 level (2-tailed).					
c. Unless otherwise noted, bootstrap results are based on 1000 bootstrap samples					

٤.٤ التوصيات

استنادًا إلى نتائج الدراسة وتحليلاتها الإحصائية، وبالنظر إلى مستوى تطبيق معايير ISO 27001 والحد من مخاطر تسرب وفقدان الوثائق الرقمية في تجمع الطائف الصحي، تُقدم الدراسة التوصيات التالية لتعزيز فعالية إدارة أمن الوثائق وتطوير ممارسات الحفظ الرقمي:

١. تعزيز الالتزام المؤسسي بمعايير ISO 27001

يجب العمل على ترسيخ التزام التجمع بتطبيق كافة بنود المعيار ISO 27001 ، بما في ذلك السياسات المكتوبة، وتحديث تقييمات المخاطر، والإجراءات المرتبطة باستمرارية الأعمال والتعافي من الكوارث.

٢. رفع مستوى الوعي والتدريب الوظيفي

توصي الدراسة بتقديم برامج تدريبية متخصصة لجميع الفئات الوظيفية حول مفاهيم أمن المعلومات وإدارة الوثائق الرقمية، بما يشمل التشفير، إدارة الوصول، وأفضل ممارسات الحفظ والتصنيف.

٣. تحديث الأدوات والتقنيات الداعمة

يجب الاستثمار في أنظمة إدارة وثائق حديثة تدعم خصائص الأمان والنسخ الاحتياطي والتتبع الآلي، وربطها بأنظمة المصادقة والتحقق الثنائي لضمان حماية البيانات.

٤. تفعيل المراقبة والتدقيق الداخلي

من الضروري إنشاء آلية مستمرة للمراجعة الداخلية والتحقق من الامتثال للسياسات الأمنية، وتوثيق أي اختلالات أو حوادث وصول غير مصرح بها وإجراء التحسينات بناءً على نتائج التدقيق.

٥. دمج الأبعاد الإدارية مع التقنية

يجب عدم الاكتفاء بالإجراءات التقنية فقط، بل من المهم تعزيز الأطر الإدارية والتنظيمية المرتبطة بإدارة الوثائق، كتعريف الصلاحيات، وتوزيع المسؤوليات، وتوثيق العمليات المرتبطة بالوصول والحفظ والأرشفة.

٦. توسيع نطاق الدراسات المستقبلية

توصي الدراسة بإجراء أبحاث مستقبلية في بيئات صحية أخرى داخل المملكة لمقارنة النتائج، مع التوسع في العينة واستخدام أدوات قياس متعددة تشمل المقابلات والتحليل النوعي.

٧. دعم استمرارية التقييم والتحسين

يُستحسن أن يتم إنشاء لجنة أمن معلومات مختصة داخل التجمع لمتابعة التغيرات التكنولوجية والتهديدات الجديدة، وتحديث السياسات بشكل دوري بناءً على التقييمات الواقعية للمخاطر.

٤.٥ الدراسات المستقبلية

بناءً على نتائج الدراسة الحالية وما تم التوصل إليه من تحديات ومحددات، يمكن اقتراح عدد من الاتجاهات البحثية المستقبلية التي تسهم في تعميق الفهم وتوسيع نطاق المعرفة في مجال تطبيق معايير أمن المعلومات وإدارة الوثائق الرقمية داخل المؤسسات الصحية، ومنها:

١. دراسات مقارنة بين التجمعات الصحية

يُوصى بإجراء دراسات مقارنة بين أكثر من تجمع صحي داخل المملكة لفهم مدى اختلاف تطبيق معايير SO 27001 وتأثيرها على أمان الوثائق، ومدى تأثير ذلك بالعوامل التنظيمية أو التقنية أو البشرية.

٢. تحليل نوعي لتجارب الموظفين

يمكن إجراء دراسات نوعية تعتمد على المقابلات المعمقة أو مجموعات التركيز لفهم التحديات التي يواجهها الموظفون في التعامل مع أنظمة الأرشفة الرقمية وإجراءات الحماية، مما يوفر بُعدًا تكميليًا للبيانات الكمية.

٣. تقييم أثر برامج التوعية والتدريب

من الممكن تصميم دراسات مستقبلية لقياس تأثير برامج التوعية والتدريب على وعي الموظفين بممارسات الحفاظ الآمن للوثائق، وربط ذلك بمستوى الامتثال الأمني الفعلي داخل المؤسسة.

٤. توسيع نطاق الدراسة لتشمل القطاع الخاص

يُقترح إجراء أبحاث مماثلة في المستشفيات والمراكز الصحية الخاصة لفحص مدى التزامها بمعايير أمن المعلومات، ومقارنة نتائجها بالقطاع الحكومي.

٥. قياس الجاهزية الرقمية للأرشفة الآمنة

من المفيد تطوير نماذج تقييم شاملة لقياس جاهزية المؤسسات الصحية من حيث البنية التحتية والسياسات والموارد البشرية لتطبيق أرشفة رقمية آمنة وفق المعايير الدولية.

٦. دراسات حول الربط بين الأرشفة الرقمية والتحول الرقمي

نظراً لتسارع التحول الرقمي في القطاع الصحي، يُستحسن إجراء دراسات تستكشف العلاقة بين نظم الأرشفة الرقمية والاستراتيجية العامة للتحول الرقمي، بما في ذلك الأثر على الكفاءة التشغيلية وجودة الخدمات.

٧. تحليل العائد على الاستثمار (ROI) في أمن الوثائق

يمكن أن تركز الدراسات المستقبلية على الجوانب الاقتصادية، مثل تحليل كفاءة الاستثمار في تطبيق معايير أمن المعلومات ومدى تقليلها لتكاليف الحوادث الأمنية أو فقدان البيانات.

٤.٦ الخاتمة

تتأول هذا الفصل أبرز الجوانب التطبيقية للدراسة من خلال تحليل البيانات واختبار الفرضيات، مما أتاح فهماً أعمق للعلاقة بين تطبيق معايير ISO 27001 ومستوى الحد من مخاطر تسرب وفقدان الوثائق الرقمية والمقرنة في بيئة تجمع الطائف الصحي. أظهرت النتائج أن هناك ارتباطاً معنوياً موجباً بين الالتزام بتلك المعايير وتعزيز أمن الوثائق، وهو ما يدعم الفرضيات الرئيسية للدراسة.

كما تم استعراض الإحصاءات الوصفية التي سلطت الضوء على وعي المشاركين وتقييمهم لممارسات الحفظ والأرشفة، بالإضافة إلى تقييم الصدق والثبات الذي أظهر ملاءمة الأداة المستخدمة لقياس المتغيرات. ومن خلال اختبار الارتباط الخطي وتحليل الفرضيات، أمكن الوصول إلى استنتاجات دقيقة تمهد الطريق لوضع توصيات عملية قابلة للتنفيذ.

وتأسيساً على ما سبق، يشكل هذا الفصل الركيزة التحليلية التي بنيت عليها توصيات الدراسة، كما يُعد تمهيداً منطقياً للفصل الأخير الذي سيعرض محددات الدراسة واستنتاجاتها العامة وتوصياتها المستقبلية.

المراجع

a. العربية

- د/بوفاس الشريف & أ/طلحي فاطمة الزهراء. (٢٠١٤). نحو بناء نظم لإدارة حماية المعلومات ISO27001 في المؤسسات الجزائرية In. *الملتقى الدولي الثاني حول النقطة الإستراتيجية و نظم المعلومات في المؤسسة الاقتصادية*.
- كحيلة, & سارة. (٢٠٢١). أمن وحماية الوثائق الإلكترونية من خلال المعايير الدولية والنصوص التشريعية: دراسة تحليلية للمعيارين ISO 27001 و ISO 27002 والقانون ١٥-٠٤ المتعلق بالتوقيع الإلكتروني. *Aleph*, ١(٣), ٥٠٣-٥١٧.
- علام, & ناهد علام. (٢٠٢٣). البرامج الآلية لإدارة الوثائق والأرشيف: مفاهيم وقضايا. *المجلة العلمية للمكتبات و الوثائق و المعلومات*, ٥(١٣.٢), ٢٠٢-٢٢٦.
- بن محمد, هدى, طوبال, ابتسام, كورتل, & نجاه. (٢٠٢٣). المعايير الدولية لإدارة أمن المعلومات. *مجلة البحوث والدراسات*, ٢٠(٢), ١٧١-١٩٦.
- سليمان, & حنان زكريا محمد. (٢٠٢٥). دور معايير حوكمة تكنولوجيا المعلومات في تحقيق جودة المعلومات المحاسبية وفق IFRS-دراسة ميدانية. *المجلة العلمية للبحوث التجارية (جامعة المنوفية)*, ٥٦(١), ٣١٩-٣٥٠.
- حلمي, & عائشة أحمد. (٢٠٢٣). معايير نظم إدارة الوثائق (MSR 30300) الصادرة عن المنظمة الدولية للتوحيد القياسي (ISO). *المجلة العلمية للمكتبات و الوثائق و المعلومات*, ٥(١٣.٢), ١٧٢-٢٠١.

.b. الاجنبية

- Hsu, H.-H., & Shih, J.-R. (2023). ISO 27001 Information Security Survey of Medical Service Organizations. *Engineering Proceedings*, 55(1), 19.
<https://doi.org/10.3390/engproc2023055019>
- Moghaddam, P. A., & Amirsharifi, R. (2024). E-Health and Legal Regulation: Protecting Patient Privacy and Data in the Digital Age. *Legal Studies in Digital Age*, 3(1), 1-8.
- Meissonnier, A., & Roques, R. (2015). L'archiviste, les normes et le droit. *La Gazette des archives*, 240(4), 135-151.
- Kurdi, M. H., Denden, M., & Paul, D. (2024). A Study on the Challenges of Human-Centric Cyber-Security and the Guarantee of Information Quality. *Journal of Information Security*, 15(2), 218-231.
- Hsu, H.-H., & Shih, J.-R. (2023). ISO 27001 Information Security Survey of Medical Service Organizations. *Engineering Proceedings*, 55(1), 19.
<https://doi.org/10.3390/engproc2023055019>
- • Moghaddam, P. A., & Amirsharifi, R. (2024). E-Health and Legal Regulation: Protecting Patient Privacy and Data in the Digital Age. *Legal Studies in Digital Age*, 3(1), 1-8.
- Scholl, M. (2024). Neue Wege für mehr Informationssicherheit in KMU: Projektdokumentation Awareness Labor KMU (ALARM) Informationssicherheit. BoD–Books on Demand.
- Alshaikh, M. (2022). *Information Security Governance and Document Management in Saudi Government Entities: A Study of ISO 27001 Application*. *International Journal of Information Management*, 62, 102435.
<https://doi.org/10.1016/j.ijinfomgt.2021.102435>
- Strickland, L. S. (2006). *Electronic Records Management in the Federal Government: Opportunities and Challenges*. *Government Information Quarterly*, 23(3–4), 365–376.
<https://doi.org/10.1016/j.giq.2006.08.005>

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared			Rotation Sums of Squared Loadings		
	Total	% of		Total	% of		Total	% of	
		Variance	Cumulative %		Variance	Cumulative %		Variance	Cumulative %
1	3.504	20.609	20.609	3.504	20.609	20.609	2.162	12.721	12.721
2	1.857	10.925	31.534	1.857	10.925	31.534	1.974	11.614	24.335
3	1.493	8.782	40.316	1.493	8.782	40.316	1.972	11.601	35.936
4	1.377	8.102	48.418	1.377	8.102	48.418	1.807	10.632	46.568
5	1.206	7.096	55.515	1.206	7.096	55.515	1.521	8.947	55.515
6	1.102	6.480	61.994						
7	.996	5.859	67.853						
8	.865	5.089	72.942						
9	.821	4.829	77.771						
10	.696	4.096	81.867						
11	.626	3.685	85.552						
12	.574	3.376	88.927						
13	.484	2.844	91.772						
14	.443	2.605	94.377						
15	.440	2.587	96.964						
16	.299	1.756	98.721						
17	.217	1.279	100.000						

Extraction Method: Principal Component Analysis.

Study Title

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

Prepared by:

Fahad Raja Allah Al-Thubaiti

Student ID: 2021202249

Master of Risk Management

Supervised by:

Dr. Al-Faisal Abdul Hameed

Dr. Fayez Jarad

Academic Year:

2025