Comprehensive Journal of Science
Volume (11), Issue (41), (JUNE, 2026)
ISSN: 3014-6266

مجلة العلوم الشاملة
المجلد (11) العدد 41 يونيو 2026
ردمد: 3014-6266

أثر مستوى الالتزام بتطبيق معيار ISO/IEC 27001 على الأمن السيبراني في المصارف التجارية الليبية

عادل العكرمي البشير الاسود
جامعة الزاوية- كلية الاقتصاد/ العجيلات

The Impact of the Level of Compliance with the ISO/IEC 27001 Standard on Cybersecurity in Libyan Commercial Banks

ADEL AB ALASWAD
Faculty of Economics - Al –Ajailat- University of Zawia
a.adela.alaswad@zu.edu.ly
https://orcid.org/0009-0005-9562-5824

تاريخ الاستلام:2026/4/04 –تاريخ المراجعة:2026/05/04– تاريخ القبول: 2026/05/16– تاريخ للنشر2026/06/05

ملخص الدراسة

تهدف هذه الدراسة إلى قياس أثر مستوى الالتزام بتطبيق متطلبات معيار **ISO/IEC 27001** على مستوى الأمن السيبراني في المصارف التجارية الليبية، في ظل التوسع في استخدام الأنظمة الرقمية والخدمات المصرفية الإلكترونية وما يرافقها من مخاطر وتهديدات سيبرانية متزايدة. اعتمدت الدراسة على المنهج الوصفي التحليلي، واستخدمت الاستبانة كأداة لجمع البيانات من العاملين في إدارات أمن المعلومات وتقنية المعلومات وإدارة المخاطر والتدقيق الداخلي في المصارف التجارية الليبية، حيث تم تحليل (26) استبانة صالحة باستخدام برنامج SPSS من خلال معامل ألفا كرونباخ، واختبار ارتباط بيرسون، وتحليل الانحدار المتعدد. أظهرت النتائج أن مستوى الالتزام بتطبيق متطلبات معيار ISO/IEC 27001 ومستوى الأمن السيبراني جاءا بدرجة مرتفعة، كما تبين وجود علاقة إيجابية ذات دلالة إحصائية بين أبعاد المعيار والأمن السيبراني، وأن أبعاد الالتزام بالمعيار تفسر نسبة (65.8%) من التغير في مستوى الأمن السيبراني. كما أظهرت النتائج أن إدارة المخاطر السيبرانية تعد أكثر الأبعاد تأثيراً، تليها الضوابط التقنية والإجرائية ثم الحوكمة وسياسات أمن المعلومات، بينما يحتاج بُعد الوعي الأمني والعامل البشري إلى مزيد من التطوير. وتوصي الدراسة بتعزيز تطبيق معيار ISO/IEC 27001 وتطوير برامج التدريب والتوعية الأمنية وتحسين ممارسات إدارة المخاطر السيبرانية بما يدعم حماية المعلومات واستمرارية الأعمال المصرفية..

الكلمات المفتاحية: معيار ISO/IEC 27001 ، الأمن السيبراني، نظام إدارة أمن المعلومات، إدارة المخاطر السيبرانية، المصارف التجارية الليبية.

Abstract

This study aims to examine the impact of the level of compliance with ISO/IEC 27001 requirements on cybersecurity in Libyan commercial banks, considering the increasing adoption of digital systems and electronic banking services and the growing cyber threats associated with digital transformation. The study adopted a descriptive analytical approach and used a questionnaire to collect data from employees in information security, information technology, risk management, and internal audit departments in Libyan commercial banks. A total of (26) valid questionnaire were analysed using SPSS through Cronbach's Alpha, Pearson correlation, and multiple regression analysis. The findings revealed that the level of compliance with ISO/IEC 27001 requirements and the level of cybersecurity were high. The results also showed a statistically significant positive relationship between ISO/IEC 27001 compliance dimensions and cybersecurity, and that these dimensions explain (65.8%) of the variation in

cybersecurity level. Cybersecurity risk management was found to have the strongest impact, followed by technical and procedural controls and information security governance, while security awareness and human factors require further improvement. The study recommends strengthening ISO/IEC 27001 implementation, developing cybersecurity awareness and training programs, and improving cybersecurity risk management practices to enhance information protection and ensure business continuity in the banking sector.

Keywords: ISO/IEC 27001, Cybersecurity, Information Security Management System, Cybersecurity Risk Management, Libyan Commercial Banks.

1- المقدمة:

يشهد القطاع المصرفي العالمي تحوّلًا رقميًا متسارعًا أسهم في تطوير الخدمات المالية ورفع كفاءة العمليات التشغيلية، إلا أنّ هذا التحول صاحبه تصاعد ملحوظ في المخاطر السيبرانية التي تهدد أمن المعلومات واستمرارية الأعمال المصرفية. وتُعد المصارف من أكثر المؤسسات عرضة للهجمات الإلكترونية نظرًا لما تديره من بيانات مالية حساسة وبنى تقنية معقدة، الأمر الذي جعل الأمن السيبراني عنصرًا استراتيجيًا لا غنى عنه لضمان الاستقرار المالي والثقة المؤسسية (ENISA, 2024). وفي هذا الصدد، برز معيار ISO/IEC 27001 بوصفه أحد أهم المعايير الدولية المعتمدة لإدارة أمن المعلومات، حيث يحدد المتطلبات اللازمة لإنشاء وتطبيق وصيانة نظام إدارة أمن المعلومات (ISMS) قائم على منهجية تحليل المخاطر ومعالجتها بصورة منهجية ومنظمة .(ISO/IEC, 2022) ويركز هذا المعيار على تحقيق مبادئ السرية والسلامة والتوافر، إلى جانب تعزيز الحوكمة المؤسسية والتحسين المستمر لأداء نظم أمن المعلومات، مما يجعله ملائمًا بشكل خاص للقطاع المصرفي (Humphreys, 2016) وتشير الأدبيات الحديثة إلى أن الالتزام الفعلي بتطبيق معيار ISO/IEC 27001 يسهم في تعزيز الجاهزية السيبرانية للمؤسسات المالية، وتحسين قدرتها على إدارة المخاطر السيبرانية والتشغيلية، والحد من آثار الحوادث الأمنية عند وقوعها(Hyseni, 2025). إلا أن فعالية هذا المعيار لا تتحقق بمجرد تبنيه شكليًا، بل تعتمد بصورة جوهرية على مستوى الالتزام العملي بتطبيق متطلباته التنظيمية والتقنية والإجرائية داخل المؤسسة. وفي البيئة الليبية، يكتسب موضوع الالتزام بتطبيق معيار ISO/IEC 27001 أهمية متزايدة في ظل توسع المصارف التجارية في استخدام الأنظمة المصرفية الإلكترونية، مقابل بيئة تتسم بتحديات مؤسسية وتنظيمية وتكنولوجية، مثل محدودية البنية التحتية الرقمية، وتفاوت مستويات النضج السيبراني، ونقص الكفاءات المتخصصة في أمن المعلومات وانطلاقًا من ذلك، تبرز الحاجة إلى دراسة علمية منهجية تسعى إلى تقييم مستوى الالتزام بتطبيق معيار ISO/IEC 27001 في المصارف التجارية الليبية، وتحليل أثر هذا الالتزام على مستوى الأمن السيبراني، بما يسهم في سد فجوة بحثية واضحة في الأدبيات العربية، ودعم صناع القرار المصرفي في تعزيز المرونة السيبرانية وتحقيق الاستقرار التشغيلي في القطاع المصرفي الليبي.

2- الدراسات السابقة:

2-1 دراسة (Ewuga, Egieya, Omotosho, & Adegbite, 2023): تناولت الدراسة تطبيق معيار ISO/IEC 27001في القطاع المصرفي بهدف تقييم مستوى تطبيقه وفعاليته في تعزيز أمن المعلومات في ظل التحول الرقمي وتزايد التهديدات السيبرانية. وركّزت على خصوصية البيئة المصرفية التي تتطلب مستويات عالية من حماية سرية وسلامة وتوافر المعلومات، مع استعراض دوافع تبني المعيار ومراحل تنفيذه وآثاره التنظيمية. وأظهرت النتائج أن تطبيق المعيار يسهم في تحسين إدارة المخاطر، وتعزيز الاستجابة للحوادث السيبرانية، ورفع مرونة الضوابط الأمنية، إضافة إلى ترسيخ ثقافة الوعي الأمني لدى العاملين. وخلصت الدراسة إلى أن ISO/IEC 27001 يُعد إطارًا استراتيجيًا فعالًا لتعزيز أمن المعلومات في المصارف، شريطة الالتزام الفعلي بمتطلباته.

2-2 دراسة (Ryanto & Tundjungsari, 2024): ركزت الدراسة على توحيد إدارة أمن المعلومات في القطاع المصرفي من خلال تطبيق إطار ISO/IEC 27001:2022 ، وذلك عبر دراسة حالة في Bank Victoria International Tbk باستخدام المنهج النوعي بالاعتماد على المقابلات ومجموعات النقاش المركزة. وهدفت إلى تقييم ممارسات الأمن السيبراني، خاصة ما يتعلق بمخاطر تسرب البيانات والتهديدات الخارجية ومدى الالتزام بالسياسات والإجراءات التنظيمية. وأظهرت النتائج أن المصرف ما يزال في مرحلة التحسين المستمر للأمن السيبراني، رغم تبنيه إجراءات وقائية إيجابية، إلا أن دمجها ضمن السياسات الرسمية لم يكتمل. وخلصت الدراسة إلى أن الالتزام المؤسسي الشامل بمتطلبات ISO/IEC 27001:2022 ، ولا سيما على مستوى السياسات والحوكمة، يعد عاملًا حاسمًا في تعزيز فعالية الأمن السيبراني في المصارف.

2-3 دراسة (Kristian Gala 2025): هدفت الدراسة إلى تحليل تطبيق معيار ISO/IEC 27001:2013 في مصرف PT. Bank Sulselbar وتقييم دوره في تحسين نظام أمن المعلومات، بالاعتماد على المنهج الوصفي النوعي من خلال المقابلات وتحليل الوثائق. وركزت على مدى تطبيق نظام إدارة أمن المعلومات وفق متطلبات المعيار، بما يشمل السياسات الأمنية وتقييم المخاطر وضوابط التحكم. وأظهرت النتائج أن التطبيق المنهجي للمعيار أسهم في تعزيز حماية المعلومات ورفع المرونة في مواجهة التهديدات السيبرانية، مع وجود قصور في وعي الموارد البشرية والحاجة إلى تعزيز التدريب. وخلصت الدراسة إلى أن فعالية المعيار تتطلب التزامًا مستمرًا وشاملًا يشمل الأبعاد التنظيمية والبشرية، بما يدعم توجه الدراسة الحالية.

2-4 دراسة (محمد & البركي, 2020): هدفت الدراسة إلى تقييم واقع تطبيق متطلبات نظم إدارة أمن المعلومات وفق المواصفة الدولية ISO/IEC 27001:2005 في خمسة مصارف ليبية بمدينتي بنغازي والبيضاء، باستخدام المنهج الوصفي التحليلي والاستبانة. وأظهرت النتائج أن مستوى التطبيق جاء بدرجة متوسطة، بما يعكس وعيًا أوليًا بأهمية أمن المعلومات دون الوصول إلى الامتثال الكامل للمعيار. كما كشفت الدراسة عن قصور في الهياكل التنظيمية المتخصصة وضعف في برامج التدريب ونشر الثقافة الأمنية. وأوصت بضرورة إنشاء إدارات متخصصة لأمن المعلومات وتعزيز الوعي الأمني لدى العاملين لتحسين فاعلية نظم إدارة أمن المعلومات والأمن السيبراني في المصارف الليبية.

2-5 دراسة (Putri, Bernandy, Aulia, Fikri, & Jasmine, 2024): هدفت الدراسة إلى تحليل ممارسات إدارة مخاطر الأمن السيبراني في منظمة حاصلة على شهادة ISO/IEC 27001 ، بالاعتماد على المنهج الوصفي التحليلي ومراجعة الأدبيات ذات الصلة. وأظهرت النتائج أن تطبيق المعيار يسهم في رفع الوعي المؤسسي بأمن المعلومات، وتعزيز فاعلية إدارة المخاطر من خلال خطوات منهجية لتحديد المخاطر وتقييمها ومعالجتها. كما بينت الدراسة أن المنظمات المعتمدة وفق ISO/IEC 27001 تتمتع بمستوى أعلى من النضج المؤسسي في مواجهة التهديدات السيبرانية، مؤكدة أهمية المعيار كأداة استراتيجية لتحسين أمن المعلومات.

2-6 دراسة (Styoutomo & Ruldeviyani, 2023): سعت الدراسة إلى تقييم مستوى الوعي بأمن المعلومات لدى العاملين في مؤسسة مالية حكومية (XYZ) تتعامل مع بيانات مصرفية عالية السرية، في ظل تصاعد هجمات التصيد الاحتيالي خلال فترة العمل عن بُعد أثناء جائحة كوفيد-19. واعتمدت على المنهج الكمي والنوعي باستخدام استبيان مبني على أداة HAIS-Q ومعيار ISO/IEC 27001:2013 ، إلى جانب مجموعات نقاش مركزة لتحليل سلوكيات الموظفين. وأظهرت النتائج أن مستوى الوعي جاء متوسطًا، مع وجود ضعف في ممارسات إدارة كلمات المرور واستخدام البريد

الإلكتروني والإنترنت والإبلاغ عن الحوادث. وخلصت الدراسة إلى أن محدودية المعرفة تؤثر سلبًا في السلوكيات الأمنية، مؤكدة أهمية تعزيز برامج التوعية الأمنية وفق معيار ISO/IEC 27001.

2-7 دراسة (Legowo & Juhartoyo, 2022): هدفت الدراسة إلى تقييم إدارة مخاطر نظم أمن تكنولوجيا المعلومات في أحد المصارف في ظل التوسع في الخدمات المصرفية الإلكترونية وما يرتبط بها من مخاطر تقنية وبشرية. واعتمدت على المنهج الوصفي التحليلي من خلال قياس مستوى نضج أمن المعلومات باستخدام معيار ISO/IEC 27001 الملحق (A). أظهرت النتائج أن مستوى نضج نظم أمن المعلومات بلغ نحو 75%، مع تباين بين المجالات، حيث سجلت إدارة استمرارية الأعمال أدنى مستوى نضج (55%)، بينما حقق مجال الالتزام أعلى مستوى (93%). كما كشفت الدراسة عن وجود أصول ذات مخاطر مرتفعة جدًا وأخرى مرتفعة تستوجب أولوية المعالجة. وخلصت إلى تقديم مجموعة من التوصيات الرقابية للحد من المخاطر وتعزيز فعالية إدارة المخاطر السيبرانية في القطاع المصرفي.

2-8 دراسة (فيلالي & أسماء, 2021): سعت هذه الدراسة إلى إبراز دور المواصفة الدولية ISO/IEC 27001 في تعزيز مصداقية وفعالية نظام إدارة أمن المعلومات داخل المؤسسات، في ظل تنامي أهمية أمن المعلومات كعنصر استراتيجي لضمان استمرارية الأعمال وحماية الأصول المعلوماتية. واعتمدت الدراسة على المنهج الوصفي التحليلي من خلال تحليل الإطار المفاهيمي لمعيار ISO/IEC 27001 وبيان دوره في تنظيم ممارسات أمن المعلومات وفق أفضل المعايير الدولية. وأظهرت النتائج أن تطبيق المواصفة يسهم في إرساء منهجية واضحة لإدارة أمن المعلومات، ويعزز الثقة والمصداقية في النظم الأمنية المطبقة، سواء في المؤسسات المعتمدة أو غير المعتمدة. كما أكدت الدراسة أن معيار ISO/IEC 27001 يُعد أداة استراتيجية لتحسين الأداء الأمني ورفع مستوى الحوكمة المعلوماتية داخل المؤسسات.

2-9 دراسة (Sharma & Dash, 2012): هدفت الدراسة إلى تحليل فعالية معيار ISO/IEC 27001 كنظام لإدارة أمن المعلومات، مع التركيز على الجوانب المالية والتنظيمية، من خلال مقارنة التوقعات المؤسسية قبل التطبيق بالنتائج الفعلية بعد الحصول على شهادة الاعتماد. واعتمدت على المنهج التحليلي لتقييم قدرة المعيار على الحد من حوادث أمن المعلومات أو تقليل آثارها عمليًا. وأظهرت النتائج أن تطبيق ISO/IEC 27001 يعزز تبني منهجية قائمة على المخاطر، ويسهم في تحسين الرقابة الداخلية على العمليات المالية وتقليل الازدواجية في نظم الرقابة. كما أكدت الدراسة أن فعالية المعيار ترتبط بالتحسين المستمر وفق دورة PDCA، مما يجعله أداة داعمة لتعزيز كفاءة وفعالية إدارة أمن المعلومات داخل المؤسسات.

3- الفجوة البحثية

على الرغم من تزايد الدراسات التي تناولت معيار ISO/IEC 27001 ودوره في تعزيز أمن المعلومات والأمن السيبراني في المؤسسات المالية والمصرفية، فإن معظم هذه الدراسات أُجريت في بيئات مصرفية خارجية تختلف من حيث البنية التنظيمية والتكنولوجية والرقابية عن البيئة الليبية. كما ركزت العديد من الدراسات على الجوانب المفاهيمية أو على تقييم تطبيق المعيار بصورة عامة، دون التعمق في قياس أثر أبعاده الرئيسة على مستوى الأمن السيبراني داخل المصارف. وفي البيئة الليبية، ما تزال الدراسات التطبيقية التي تناولت العلاقة بين مستوى الالتزام بمتطلبات معيار ISO/IEC 27001 ومستوى الأمن السيبراني في المصارف التجارية محدودة ونادرة، خاصة تلك التي تدرس أثر أبعاد المعيار المتمثلة في الحوكمة وسياسات أمن المعلومات، وإدارة المخاطر السيبرانية، والضوابط التقنية والإجرائية، والوعي الأمني والعامل البشري ضمن نموذج تحليلي واحد. ومن ثم تسعى هذه الدراسة إلى سد هذه الفجوة من خلال اختبار أثر مستوى الالتزام بتطبيق متطلبات معيار ISO/IEC 27001على مستوى الأمن السيبراني في المصارف التجارية الليبية.

4- مشكلة الدراسة

يشهد القطاع المصرفي الليبي توسعاً متزايداً في استخدام الأنظمة الرقمية والخدمات المصرفية الإلكترونية، الأمر الذي صاحبه ارتفاع في المخاطر والتهديدات السيبرانية التي تستهدف البيانات والأنظمة المصرفية الحساسة. ويُعد معيار ISO/IEC 27001من أهم المعايير الدولية المعتمدة لإدارة أمن المعلومات، لما يوفره من إطار متكامل للحوكمة وإدارة المخاطر وتطبيق الضوابط الأمنية اللازمة لحماية المعلومات وتعزيز استمرارية الأعمال .ورغم تزايد اهتمام المصارف التجارية الليبية بتبني متطلبات المعيار، إلا أن مستوى الالتزام الفعلي بتطبيقه ما يزال غير واضح، كما لا تتوافر أدلة علمية كافية توضح مدى انعكاس هذا الالتزام على مستوى الأمن السيبراني في البيئة المصرفية الليبية. ومن ثم تبرز الحاجة إلى دراسة العلاقة بين مستوى الالتزام بتطبيق متطلبات معيار ISO/IEC 27001 ومستوى الأمن السيبراني في المصارف التجارية الليبية. وتتمحور مشكلة هذه الدراسة حول محاولة الإجابة عن التساؤل الرئيس الآتي: **ما أثر مستوى الالتزام بتطبيق معيار ISO/IEC 27001على مستوى الأمن السيبراني في المصارف التجارية الليبية؟**

5- اهداف الدراسة:

تهدف هذه الدراسة إلى تحقيق الأهداف الآتية:

5-1 تحليل أثر مستوى الالتزام بالحوكمة وسياسات أمن المعلومات وفق متطلبات معيار ISO/IEC 27001 على مستوى الأمن السيبراني في المصارف التجارية الليبية.

5-2 تحليل أثر مستوى الالتزام بإدارة المخاطر السيبرانية وفق متطلبات معيار ISO/IEC 27001 على مستوى الأمن السيبراني في المصارف التجارية الليبية.

5-3 تحليل أثر مستوى الالتزام بتطبيق الضوابط التقنية والإجرائية لأمن المعلومات المنصوص عليها في معيار ISO/IEC 27001على مستوى الأمن السيبراني في المصارف التجارية الليبية.

6- فروض الدراسة:

الفرض الرئيسي: يوجد أثر ذو دلالة إحصائية لمستوى الالتزام بتطبيق متطلبات معيار ISO/IEC 27001 على مستوى الأمن السيبراني في المصارف التجارية الليبية.

الفروض الفرعية

6-1 يوجد أثر ذو دلالة إحصائية لمستوى الالتزام بالحوكمة وسياسات أمن المعلومات وفق متطلبات معيار ISO/IEC 27001 على مستوى الأمن السيبراني في المصارف التجارية الليبية.

6-2 يوجد أثر ذو دلالة إحصائية لمستوى الالتزام بإدارة المخاطر السيبرانية وفق متطلبات معيار ISO/IEC 27001 على مستوى الأمن السيبراني في المصارف التجارية الليبية.

6-3 يوجد أثر ذو دلالة إحصائية لمستوى الالتزام بتطبيق الضوابط التقنية والإجرائية لأمن المعلومات وفق متطلبات معيار ISO/IEC 27001على مستوى الأمن السيبراني في المصارف التجارية الليبية.

7- متغيرات الدراسة

تعتمد هذه الدراسة على مجموعة من المتغيرات الرئيسة التي تم تحديدها في ضوء الإطار النظري وأهداف الدراسة وفروضها، وذلك بهدف تحليل أثر مستوى الالتزام بتطبيق متطلبات معيار ISO/IEC 27001 على مستوى الأمن السيبراني في المصارف التجارية الليبية. وتنقسم متغيرات الدراسة إلى متغير تابع ومتغيرات مستقلة، على النحو الآتي:

7-1 المتغير التابع

مستوى الأمن السيبراني في المصارف التجارية الليبية: ويقصد به مستوى قدرة المصارف على حماية أنظمتها المعلوماتية وبياناتها الرقمية من التهديدات والهجمات السيبرانية، وضمان سرية المعلومات وسلامتها وتوافرها، وتقليل الحوادث الأمنية، وتعزيز الجاهزية والاستجابة للحوادث، وضمان استمرارية الأعمال المصرفية في بيئة رقمية تتسم بارتفاع المخاطر.

2-7 المتغيرات المستقلة

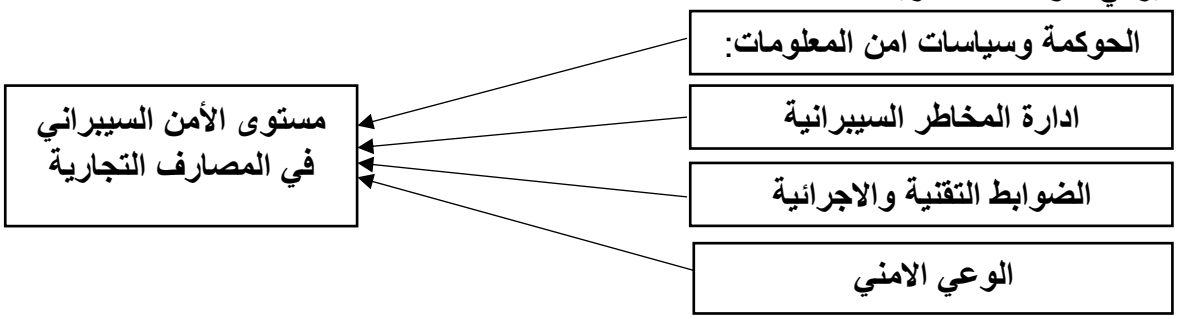
تمثل المتغيرات المستقلة مستوى الالتزام بتطبيق متطلبات معيار ISO/IEC 27001 ، وقد جرى تحليل هذا الالتزام من خلال مجموعة من الأبعاد الرئيسة، وهي:

1-2-7 **الالتزام بالحوكمة وسياسات امن المعلومات:** الالتزام بالحوكمة وسياسات أمن المعلومات ويشير إلى مدى التزام المصارف بتطبيق متطلبات الحوكمة الأمنية، من حيث دعم الإدارة العليا، ووضوح السياسات الأمنية، وتحديد الأدوار والمسؤوليات، ووجود آليات رقابية تضمن الامتثال الفعلي لمتطلبات أمن المعلومات.

2-2-7 الالتزام بادارة المخاطر السيبرانية : ويقصد به مدى تطبيق المصارف لنهج منهجي قائم على تحديد وتقييم ومعالجة المخاطر السيبرانية وفق متطلبات معيار ISO/IEC 27001 ، بما يسهم في تقليل احتمالية وقوع الحوادث الأمنية والحد من آثارها عند حدوثها.

3 -2-7 الالتزام بتطبيق الضوابط التقنية والاجرائية (Annex A): ويتمثل في مدى تنفيذ المصارف للضوابط الأمنية التقنية والإجرائية، مثل التحكم في الوصول، والتشفير، وإدارة الحوادث، وضمان استمرارية الأعمال، بما يعزز الحماية الفعلية للأنظمة المصرفية.

4-2-7 الوعي الامني والعامل البشري: ويشير إلى مستوى وعي العاملين بأمن المعلومات، ومدى خضوعهم لبرامج التدريب والتوعية الأمنية، والتزامهم بالسلوكيات الأمنية السليمة، باعتبار العامل البشري أحد أكثر مصادر المخاطر السيبرانية تأثيرًا في المؤسسات المصرفية.



شكل رقم (1) النموذج المفاهيمي للدراسة

ثانيا: الاطار النظري للدراسة

يهدف الإطار النظري لهذه الدراسة إلى توضيح المفاهيم النظرية والأساسية للأمن السيبراني في القطاع المصرفي، واستعراض معيار ISO/IEC 27001 كنظام لإدارة أمن المعلومات، مع التركيز على أبعاد الالتزام بتطبيقه. كما يسعى إلى تحليل دور الحوكمة، وإدارة المخاطر السيبرانية، والضوابط التقنية والإجرائية في تعزيز مستوى الأمن السيبراني داخل المصارف التجارية، بما يوفر أساسًا علميًا لتفسير نتائج الدراسة واختبار فرضياتها. وتستند الدراسة إلى **نظرية إدارة المخاطر (Risk Management Theory)** وإلى مبادئ **حوكمة تقنية المعلومات(IT Governance)** ، حيث تفترض هاتان المقاربتان أن التطبيق المنهجي للسياسات والإجراءات والضوابط الأمنية يسهم في تقليل المخاطر السيبرانية وتعزيز قدرة المؤسسات المصرفية على حماية معلوماتها وأصولها الرقمية.

2-1 الأساس النظري للدراسة: نظرية الموارد والقدرات (Resource-Based View Theory)

تستند هذه الدراسة إلى نظرية الموارد والقدرات(Resource-Based View - RBV) ، التي تعد من النظريات الإدارية التي تفسر اختلاف مستويات الأداء بين المؤسسات بناءً على امتلاكها موارد وقدرات تنظيمية تساعدها على تحقيق أهدافها وتعزيز قدرتها التنافسية. ووفقاً لهذه النظرية، فإن الموارد الداخلية للمؤسسة لا تحقق قيمة حقيقية إلا عندما يتم تطويرها وإدارتها بطريقة فعالة بما يجعلها تسهم في تحسين الأداء المؤسسي.

وفي إطار هذه الدراسة، يُنظر إلى نظام إدارة أمن المعلومات وفق معيار ISO/IEC 27001 باعتباره قدرة تنظيمية استراتيجية تمتلكها المصارف لتعزيز قدرتها على حماية الأصول المعلوماتية وإدارة المخاطر السيبرانية. فالتزام المصارف بتطبيق متطلبات المعيار لا يمثل مجرد امتثال لإجراءات أو ضوابط فنية، بل يعكس بناء منظومة متكاملة تشمل الحوكمة الأمنية، وإدارة المخاطر، والسياسات والإجراءات، والضوابط التقنية، وتنمية الوعي الأمني لدى العاملين.

وبناءً على ذلك، تفترض النظرية أن المصارف التي تمتلك مستوى أعلى من الالتزام بتطبيق متطلبات ISO/IEC 27001 تكون أكثر قدرة على تطوير ممارسات الأمن السيبراني، ورفع مستوى الجاهزية والاستجابة للحوادث، وتقليل المخاطر المرتبطة بالتهديدات الرقمية. ومن هذا المنطلق، فإن مستوى تطبيق معيار ISO/IEC 27001 يمثل مورداً تنظيمياً يسهم في تعزيز المرونة السيبرانية وتحسين حماية المعلومات واستمرارية الأعمال المصرفية.

2-2 الإطار المفاهيمي للأمن السيبراني في القطاع المصرفي

2-2-1 مفهوم الأمن السيبراني وأمن المعلومات: يقصد بأمن المعلومات مجموعة السياسات والضوابط التي تهدف إلى حماية سرية المعلومات وسلامتها وتوافرها، بغضّ النظر عن شكلها أو وسيلة تخزينها. أما الأمن السيبراني فيُعد فرعًا متخصصًا من أمن المعلومات يركز على حماية الأنظمة والشبكات الرقمية من التهديدات الإلكترونية. ورغم التداخل بين المفهومين، فإن الأمن السيبراني يعالج المخاطر الرقمية الحديثة بشكل مباشر، بينما يشمل أمن المعلومات نطاقًا أشمل للحماية. وتبرز أهمية هذين المفهومين في القطاع المصرفي نظرًا لاعتماده المتزايد على التقنيات الرقمية، مما يجعل تبنّي أطر معيارية مثل ISO/IEC 27001 ضرورة لتعزيز إدارة المخاطر وحماية الأصول المعلوماتية (G'ofurova Laziza, 2025) ويمكن التمييز بين مفهوم الامن السيبراني ومفهوم امن المعلومات (Von Solms & Von Solms, 2004) من خلال الجدول التالي: *جدول (1): المقارنة بين أمن المعلومات والأمن السيبراني*

العنصر	أمن المعلومات	الأمن السيبراني
نطاق الحماية	يركز على حماية المعلومات والبيانات بمختلف أشكالها ووسائل تخزينها	يركز على حماية البيئة الرقمية بما تشمل الأنظمة والشبكات والبنية التحتية الرقمية
الهدف الأساسي	ضمان سرية المعلومات وسلامتها وتوافرها (CIA Triad)	مواجهة التهديدات والهجمات الإلكترونية وتعزيز القدرة على المنع والكشف والاستجابة
طبيعة المخاطر	مخاطر فقدان البيانات أو تعديلها أو الوصول غير المصرح به	الهجمات السيبرانية مثل الاختراق والبرمجيات الخبيثة والتصيد الإلكتروني
الأدوات والإجراءات	سياسات أمن المعلومات، إدارة الصلاحيات، الضوابط التنظيمية والإجرائية	الدفاع السيبراني، مراقبة الشبكات، الاستجابة للحوادث، التحليل والكشف عن التهديدات
العلاقة بينهما	يمثل الإطار الأوسع لحماية المعلومات	يعد جزءاً متخصصاً يركز على المخاطر في البيئة الرقمية

2-2-2 خصائص الأمن السيبراني في المؤسسات المصرفية :تتسم خصائص الأمن السيبراني في المؤسسات المصرفية بالتعقيد نتيجة الاعتماد المكثف على الأنظمة الرقمية وحساسية البيانات المالية، مما يجعل المصارف عرضة لمختلف الهجمات السيبرانية. ويستلزم ذلك اعتماد نهج أمني متكامل يجمع بين الضوابط التقنية والحوكمة وإدارة المخاطر، مع الاستناد إلى أطر معيارية مثل ISO/IEC 27001 لتعزيز حماية البيانات وضمان استمرارية الأعمال(Yesugad, 2024)

2-2-3 التهديدات السيبرانية التي تواجه المصارف التجارية :تواجه المصارف التجارية تهديدات سيبرانية متزايدة تستهدف الأنظمة الرقمية والبيانات الحساسة، وتشمل البرمجيات الخبيثة، والبرامج الفدية، والتصيّد الاحتيالي، وانتهاكات البيانات، وهجمات الحرمان من الخدمة، مما يشكّل تحديًا رئيسًا لاستقرار القطاع المصرفي في ظل التحول الرقمي. ويؤدي الاعتماد المتنامي على الخدمات الرقمية إلى توسيع سطح الهجوم، الأمر الذي يستدعي تبنّي أطر معيارية قوية مثل ISO/IEC 27001للحد من هذه المخاطر وحماية الأصول المصرفية الحيوية (ENISA, 2024; Katuri, 2025).

2-2-4 انعكاسات المخاطر السيبرانية على الاستقرار المصرفي: تمثل المخاطر السيبرانية مصدرًا متناميًا للمخاطر النظامية التي تهدد الاستقرار المصرفي، إذ تتجاوز آثارها الخسائر التشغيلية لتشمل تعطّل الخدمات، تآكل الثقة، وارتفاع المخاطر التشغيلية والسمعة، مع احتمالية انتقال الصدمات داخل الأنظمة المصرفية عالية الترابط. وفي هذا السياق، تُعد الأطر المعيارية مثل ISO/IEC 27001 أداة أساسية لتعزيز الحوكمة السيبرانية وإدارة المخاطر ودعم الاستقرار المصرفي (Adelmann et al., 2020).

2-3 معيار ISO/IEC 27001 كنظام لإدارة أمن المعلومات

2-3-1 نشأة وتطور معيار ISO/IEC 27001 : نشأ معيار ISO/IEC 27001 استجابةً لتزايد مخاطر المعلومات الرقمية، ويُعد جزءًا من عائلةISO/IEC 27000 ، مع جذور تعود إلى المعيار البريطاني .BS 7799 وقد اعتُمد دوليًا عام 2005 كنظام لإدارة أمن المعلومات قائم على المخاطر، ثم طُوّر في إصداري 2013 و2022 لمواكبة التطور التقني وتعزيز حوكمة المخاطر السيبرانية في المؤسسات (Culot, Nassimbeni, Podrecca, & Sartor, 2021).

2-3-2 أهداف المعيار وأهميته للقطاع المصرفي: يُعد اعتماد نظام إدارة أمن المعلومات (ISMS) وفق معيار ISO/IEC 27001خطوة محورية نحو تعزيز الامتثال التنظيمي وإدارة المخاطر، إذ يؤكد هذا المعيار التزام المؤسسة بمعالجة مخاطر أمن المعلومات بشكل منهجي والتحسين المستمر لإطارها الأمني. ويسهم تطبيقه في حماية البيانات المالية الحساسة وضمان استمرارية الأعمال أثناء الحوادث السيبرانية، إلى جانب دعم الالتزام بالتشريعات المالية وتقليل المخاطر القانونية. كما يعزز ثقة العملاء وأصحاب المصلحة ويرفع السمعة المؤسسية في قطاع قائم على الثقة، ويحسن الجاهزية للاستجابة للحوادث وتقليل فترات التوقف والخسائر التشغيلية. إضافة إلى ذلك، يوفر المعيار ميزة تنافسية من خلال تمييز المؤسسات المعتمدة وزيادة مصداقيتها، مع دعم التحسين المستمر والقدرة على التكيف مع التهديدات السيبرانية المتغيرة، بما يعزز المرونة التشغيلية والاستدامة طويلة الأجل (Choubey & Bhargava, 2018).

2-3-3 مكونات نظام إدارة أمن المعلومات وفق معيارISO/IEC 27001:2022

يتكون نظام إدارة أمن المعلومات (Information Security Management System – ISMS) وفق معيار ISO/IEC 27001:2022من مجموعة من المتطلبات التنظيمية والإدارية التي تهدف إلى بناء نظام متكامل لإدارة مخاطر أمن المعلومات وتحسين مستوى الحماية داخل المؤسسات. ولا يقتصر تطبيق المعيار على استخدام الضوابط التقنية فقط،

بل يعتمد على إطار إداري شامل يربط بين الحوكمة، وإدارة المخاطر، والعمليات التشغيلية، والتحسين المستمر. وتشمل متطلبات المعيار البنود الرئيسية الآتية (ISO/IEC 27001:2022, 2022) :

2-3-3-1 سياق المؤسسة (Context of the Organization)

يركز هذا البند على فهم طبيعة المؤسسة وبيئتها الداخلية والخارجية، وتحديد الأطراف ذات العلاقة، وتحديد نطاق نظام إدارة أمن المعلومات بما يتناسب مع طبيعة أعمال المؤسسة ومخاطرها. وفي القطاع المصرفي يساعد ذلك على تحديد الأصول المعلوماتية الحساسة والتهديدات المرتبطة بالأنظمة والخدمات المصرفية الرقمية.

2-3-3-2 القيادة (Leadership)

يشير هذا البند إلى أهمية دور الإدارة العليا في دعم نظام إدارة أمن المعلومات، من خلال وضع سياسات واضحة، وتوفير الموارد اللازمة، وتحديد المسؤوليات والصلاحيات المتعلقة بأمن المعلومات، بما يضمن دمج الأمن السيبراني ضمن الاستراتيجية المؤسسية.

2-3-3-3 التخطيط (Planning)

يركز التخطيط على تحديد مخاطر أمن المعلومات والفرص المرتبطة بها، ووضع أهداف أمنية قابلة للقياس، وتحديد الإجراءات اللازمة لمعالجة المخاطر وفق منهج قائم على التقييم والتحليل المستمر.

2-3-3-4 الدعم (Support)

يتعلق هذا البند بتوفير الموارد والكفاءات والوعي والتدريب اللازم للعاملين، إضافة إلى ضمان التواصل الداخلي والخارجي وإدارة الوثائق والسجلات المرتبطة بنظام إدارة أمن المعلومات.

2-3-3-5 التشغيل (Operation)

يتضمن تنفيذ العمليات والإجراءات اللازمة لإدارة مخاطر أمن المعلومات، وتطبيق الضوابط الأمنية المناسبة، ومتابعة الإجراءات التشغيلية التي تضمن حماية الأنظمة والبيانات المصرفية.

2-3-3-6 تقييم الأداء (Performance Evaluation)

يركز على قياس ومراجعة فاعلية نظام إدارة أمن المعلومات من خلال المراقبة، والتدقيق الداخلي، وقياس مدى تحقيق الأهداف الأمنية، بهدف اكتشاف نقاط الضعف وتحسين الأداء.

2-3-3-7 التحسين (Improvement)

يهتم هذا البند بالتحسين المستمر لنظام إدارة أمن المعلومات من خلال معالجة أوجه القصور واتخاذ الإجراءات التصحيحية وتطوير الضوابط الأمنية بما يتناسب مع تغير طبيعة التهديدات السيبرانية. وبذلك يمثل معيار ISO/IEC 27001:2022 إطاراً إدارياً متكاملاً لا يركز فقط على الجوانب التقنية، بل يجمع بين الحوكمة وإدارة المخاطر والعوامل البشرية والضوابط التشغيلية، مما يجعله مناسباً لتعزيز مستوى الأمن السيبراني والمرونة التشغيلية في المؤسسات المصرفية.

2-3-4 مبادئ نظام إدارة أمن المعلومات (ISMS): يُعد نظام إدارة أمن المعلومات (ISMS) إطارًا منهجيًا لحماية أصول المعلومات، ويرتكز وفق معيار ISO/IEC 27001 على مبادئ السرية والسلامة والتوافر، مع اعتماد منهج قائم على إدارة

المخاطر والتحسين المستمر بدعم الإدارة العليا. ويسهم تطبيقه في تعزيز موثوقية النظم المعلوماتية ورفع الثقة المؤسسية، لا سيما في القطاع المصرفي. (Al-Dhahri, Al-Sarti, & Abdul, 2017).

2-3-5 دورة التحسين المستمر(PDCA) : تُعد دورة التحسين المستمر Plan – Do – Check – Act (PDCA) إطارًا منهجيًا لتطبيق نظم إدارة أمن المعلومات في المصارف، تقوم على التخطيط، والتنفيذ، والمراجعة، والتحسين المستمر للضوابط الأمنية. ويسهم اعتمادها في تقليل المخاطر السيبرانية وتعزيز قدرة المصارف على مواجهة التهديدات الرقمية المتغيرة (ISO/IEC 27001:2022, 2022).

2-4 الالتزام بتطبيق معيار ISO/IEC 27001 وأثره على تعزيز الأمن السيبراني في المصارف التجارية

انطلاقًا من ذلك، تفترض هذه الدراسة أن مستوى الالتزام بتطبيق متطلبات معيار ISO/IEC 27001 يُعد عاملًا حاسمًا في تفسير مستوى الأمن السيبراني داخل المصارف التجارية، حيث يسهم الالتزام المتكامل بأبعاد الحوكمة، وإدارة المخاطر السيبرانية، وتنفيذ الضوابط التقنية والإجرائية، وتعزيز الوعي الأمني في رفع مستوى النضج السيبراني وتقليل المخاطر التشغيلية، بما يعزز حماية الأصول المعلوماتية واستمرارية الأعمال. وتدعم هذه الفرضية الأدبيات التي تؤكد أن التطبيق المنهجي والشامل لمعيار ISO/IEC 27001 يرتبط إيجابيًا بتحسين الأداء الأمني والمرونة التنظيمية في المؤسسات المالية(Culot et al., 2021)

2-4-1 الحوكمة وسياسات أمن المعلومات وأثرها على الأمن السيبراني: بناء على ذلك، تنطلق فرضية الحوكمة في هذه الدراسة من اعتبار حوكمة أمن المعلومات متغيرًا تفسيريًا رئيسًا في تعزيز الأمن السيبراني داخل المصارف، إذ يسهم وضوح الأدوار والمسؤوليات، ودعم الإدارة العليا، وفاعلية آليات الرقابة—وفق متطلبات معيار—ISO/IEC 27001 في رفع مستوى الالتزام المؤسسي بالسياسات الأمنية، وتحسين الاستجابة للحوادث السيبرانية، وتعزيز النضج والثقة المؤسسية. وفي المقابل، يؤدي ضعف الحوكمة إلى تراجع فعالية الضوابط الأمنية وزيادة التعرض للمخاطر السيبرانية، وهو ما تدعمه الأدبيات التجريبية ذات الصلة (Mohammed Alharbi, 2025; Von Solms & Von Solms, 2004).

2-4-2 إدارة المخاطر السيبرانية ودورها في تقليل الحوادث الأمنية: تفترض هذه الدراسة أن فاعلية إدارة المخاطر السيبرانية، وفق نهج ISO/IEC 27001 القائم على المخاطر، تمثل عاملًا حاسمًا في تعزيز مستوى الأمن السيبراني في المصارف التجارية، إذ يسهم التحديد المنهجي للتهديدات وتقييم آثارها والمراجعة المستمرة للمخاطر في خفض معدلات الحوادث الأمنية، وتعزيز القدرة على التعافي، وضمان استمرارية الأعمال. وفي المقابل، يؤدي ضعف إدارة المخاطر أو غياب الطابع الديناميكي لها إلى زيادة التعرض للمخاطر السيبرانية وتراجع فعالية الضوابط الوقائية، وهو ما تؤكده الأدبيات التجريبية الحديثة(Culot et al., 2021)

2-4-3 الضوابط التقنية والإجرائية (Annex A) وأثرها على استمرارية الأعمال: يشكل الملحقAnnex A)) في معيار ISO/IEC 27001 الإطار التنفيذي للضوابط التقنية والإجرائية لمعالجة المخاطر السيبرانية، ويُعد ركيزة أساسية لحماية الأنظمة المصرفية وضمان استمرارية الخدمات. وتبين الأدبيات أن التطبيق المتكامل لضوابط مثل التحكم في الوصول والتشفير وإدارة الحوادث يسهم في تقليل الانقطاعات التشغيلية وتعزيز قدرة المصارف على العمل في بيئات عالية المخاطر، على أن ترتبط فاعلية هذه الضوابط بدرجة الالتزام المؤسسي الفعلي بها، وليس بمجرد إدراجها ضمن السياسات المكتوبة (Kamil, Lund, & Islam, 2023)

2-4-4 الوعي الأمني والعامل البشري ومستوى النضج السيبراني: يعد العامل البشري أحد أكثر عناصر الأمن السيبراني حساسية وتأثيرًا، إذ تشير الدراسات إلى أن نسبة كبيرة من الحوادث السيبرانية تعود إلى أخطاء بشرية أو ضعف الوعي بالتهديدات الإلكترونية. ويؤكد معيار ISO/IEC 27001 على أهمية بناء ثقافة أمنية قائمة على التدريب المستمر والتوعية المنظمة، بما يعزز السلوكيات الأمنية السليمة لدى الموظفين. وتُظهر الأدبيات أن المصارف التي تستثمر في برامج الوعي الأمني تحقق مستويات أعلى من النضج السيبراني، وتقل فيها حالات الاختراق الناتجة عن الهندسة الاجتماعية أو سوء استخدام الأنظمة(Khadka & Ullah, 2025) . كما يسهم تعزيز الوعي الأمني في دعم فعالية الضوابط التقنية والإجرائية، وتحقيق التكامل بين الأبعاد البشرية والتنظيمية والتقنية للأمن السيبراني.

2-4-5 العلاقة بين مستوى الالتزام بمعيار ISO/IEC 27001 ومستوى النضج السيبراني: تشير الأدبيات الحديثة إلى وجود علاقة إيجابية قوية بين مستوى الالتزام الفعلي بتطبيق متطلبات معيار ISO/IEC 27001 وبين مستوى النضج السيبراني داخل المؤسسات المصرفية، حيث يؤدي الالتزام المتكامل بأبعاد الحوكمة، وإدارة المخاطر، والضوابط التقنية، والوعي الأمني إلى تحسين القدرة الوقائية والاستجابية للمصارف في مواجهة التهديدات السيبرانية. وتؤكد هذه الدراسات أن النضج السيبراني لا يتحقق من خلال تطبيق جزئي أو شكلي للمعيار، بل من خلال دمجه ضمن الاستراتيجية المؤسسية والتحسين المستمر وفق دورة (PDCA)، مما ينعكس إيجابًا على الاستقرار التشغيلي وحماية الأصول المعلوماتية (ISO/IEC 27001:2022, 2022; Sharma & Dash, 2012)

ثالثا: الإطار العملي (الدراسة الميدانية)

يهدف هذا الفصل إلى اختبار الإطار التحليلي للدراسة ميدانيًا، وقياس أثر مستوى الالتزام بتطبيق متطلبات معيار **ISO/IEC 27001** على مستوى الأمن السيبراني في المصارف التجارية الليبية. ويتناول عرض منهجية الدراسة، ومجتمعها وعينتها، وأداة جمع البيانات وصدقها وثباتها، إضافة إلى الأساليب الإحصائية المستخدمة لاختبار الفروض. كما يعرض نتائج التحليل الإحصائي وتفسيرها في ضوء الإطار النظري والدراسات السابقة.

3-1 منهجية الدراسة ومجتمع وعينة الدراسة

اعتمدت هذه الدراسة على المنهج الوصفي التحليلي، وذلك لملاءمته لطبيعة الدراسة التي تهدف إلى قياس أثر مستوى الالتزام بتطبيق متطلبات معيار **ISO/IEC 27001** على مستوى الأمن السيبراني في المصارف التجارية الليبية، من خلال تحليل العلاقة بين أبعاد تطبيق المعيار والممارسات المرتبطة بحماية الأنظمة والبيانات المصرفية. ويتيح هذا المنهج وصف واقع تطبيق متطلبات نظام إدارة أمن المعلومات(ISMS) داخل المصارف، وتحليل أثرها في تعزيز القدرة على مواجهة المخاطر والتهديدات السيبرانية. ويتكون مجتمع الدراسة من العاملين في المصارف التجارية الليبية، وبصفة خاصة العاملين في الإدارات ذات العلاقة المباشرة بأمن المعلومات وإدارة المخاطر وتقنية المعلومات والتدقيق الداخلي، باعتبارهم الأكثر معرفة وإدراكاً بممارسات الأمن السيبراني ومتطلبات تطبيق معيار .ISO/IEC 27001 ونظراً للطبيعة التخصصية لموضوع الدراسة، فقد تم الاعتماد على **العينة القصدية** (Purposive Sampling)، حيث تم اختيار أفراد العينة ممن تتوافر لديهم الخبرة والمعرفة المرتبطة بمجال أمن المعلومات والمخاطر السيبرانية داخل المصارف. وقد تم اختيار العينة القصدية بسبب محدودية عدد الموظفين المتخصصين في أمن المعلومات وإدارة المخاطر داخل المصارف الليبية، وهم يمثلون الفئة الأكثر ارتباطاً بموضوع الدراسة والأقدر على تقييم مستوى الالتزام بتطبيق متطلبات معيار .ISO/IEC 27001 وبناءً على ذلك تم توزيع (35) استبانة على عدد من العاملين في بعض المصارف التجارية الليبية، وبعد مراجعة الاستبانات واستبعاد غير الصالح منها، بلغ عدد الاستبانات الصالحة للتحليل الإحصائي (26) استبانة، بنسبة استجابة بلغت (74.3%) من إجمالي

الاستبانات الموزعة. وقد تم استخدام الاستبانة كأداة رئيسة لجمع البيانات الأولية، وتم إعداد فقراتها بالاعتماد على الأدبيات السابقة ومتطلبات معيار ISO/IEC 27001 ، بحيث تضمنت أبعاد الالتزام بتطبيق المعيار والمتمثلة في: الحوكمة وسياسات أمن المعلومات، وإدارة المخاطر السيبرانية، والضوابط التقنية والإجرائية، والوعي الأمني والعامل البشري، بالإضافة إلى قياس مستوى الأمن السيبراني بوصفه المتغير التابع. وتم قياس استجابات أفراد العينة باستخدام مقياس ليكرت الخماسي، كما تم تحليل البيانات باستخدام برنامج (SPSS) من خلال مجموعة من الأساليب الإحصائية شملت المتوسطات الحسابية والانحرافات المعيارية، ومعامل ألفا كرونباخ للتحقق من ثبات الأداة، ومعامل ارتباط بيرسون، وتحليل الانحدار المتعدد لاختبار فرضيات الدراسة.

3-3 ثبات أداة الدراسة

تم التحقق من ثبات أداة الدراسة باستخدام معامل ألفا كرونباخ (Cronbach's Alpha)، وأظهرت النتائج أن جميع معاملات الثبات تجاوزت الحد الأدنى المقبول إحصائياً (0.70)، حيث تراوحت بين (0.789) و(0.884)، مما يدل على تمتع الاستبانة بدرجة مرتفعة من الثبات والاتساق الداخلي، وبالتالي صلاحيتها لأغراض التحليل الإحصائي واختبار فرضيات الدراسة.

جدول رقم (2) ثبات اداة الدراسة

المتغيرات	عدد العبارات	معامل الفا كورنباخ (Cronbach's Alpha)	الاتساق الداخلي
الحوكمة وسياسات امن المعلومات GOV	6	0.842	ممتازة
ادارة المخاطر السيبرانية RISK	5	0.865	ممتازة
الضوابط التقنية والاجرائية CTRL	6	0.811	ممتاوة
الوعي الامني والعامل البشري AWARE	4	0.789	جيد جدا
مستوى الامن السيبراني CYB	9	0.884	ممتازة

4-3 التحليل الوصفي لمتغيرات الدراسة (المتوسطات والانحرافات)

تم استخدام المتوسطات الحسابية والانحرافات المعيارية لوصف استجابات أفراد العينة تجاه أبعاد الدراسة ومتغيراتها الرئيسة، وذلك بهدف تحديد مستوى الالتزام بتطبيق متطلبات معيار ISO/IEC 27001 في المصارف التجارية الليبية، فضلاً عن التعرف على مستوى الأمن السيبراني. ويُعد المتوسط الحسابي مؤشراً لقياس درجة الاتفاق على فقرات كل بُعد، في حين يعكس الانحراف المعياري مدى تشتت استجابات أفراد العينة حول المتوسط الحسابي. ويبين الجدول ( ) نتائج التحليل الوصفي لأبعاد الدراسة مرتبة تنازلياً وفقاً لمتوسطاتها الحسابية.

الجدول (3) نتائج التحليل الوصفي لأبعاد الدراسة

الترتيب	البعد الاحصائي	المتوسط الحسابي	الانحراف المعياري	مستوى الموافقة
1	البعد الاول: ادارة المخاطر السيبرانية	4.38	0.51	مرتفع جدا
2	البعد الثاني: الحوكمة وسياسات امن المعلومات	4.29	0.56	مرتفع جدا
3	البعد الثالث: الضوابط التقنية والاجرائية	4.18	0.59	مرتفع
4	البعد الرابع: الوعي الامني والعامل البشري	3.84	0.74	متوسط
–	المتغير التابع: مستوى الامن السيبراني الاجمالي	4.21	0.53	مرتفع

أظهرت نتائج التحليل الوصفي أن مستوى الالتزام بتطبيق متطلبات معيار ISO/IEC 27001 في المصارف التجارية الليبية جاء مرتفعاً بصورة عامة، حيث بلغ المتوسط الحسابي لمستوى الأمن السيبراني (4.21) بانحراف معياري قدره (0.53)، مما يعكس إدراكاً مرتفعاً لدى أفراد العينة لمستوى الممارسات المرتبطة بالأمن السيبراني داخل المصارف محل الدراسة . كما بينت النتائج أن بُعد إدارة المخاطر السيبرانية جاء في المرتبة الأولى بمتوسط حسابي بلغ (4.38) وانحراف معياري (0.51)، وهو ما يشير إلى ارتفاع مستوى الاهتمام بالممارسات المرتبطة بتحديد المخاطر السيبرانية وتقييمها ومعالجتها داخل المصارف. وجاء بُعد الحوكمة وسياسات أمن المعلومات في المرتبة الثانية بمتوسط حسابي بلغ (4.29) وانحراف معياري (0.56)، مما يعكس وجود اهتمام واضح بتطبيق السياسات والإجراءات المرتبطة بحوكمة أمن المعلومات . واحتل بُعد الضوابط التقنية والإجرائية المرتبة الثالثة بمتوسط حسابي بلغ (4.18) وانحراف معياري (0.59)، بما يدل على ارتفاع مستوى تطبيق الضوابط الفنية والإجرائية الداعمة لحماية المعلومات والأنظمة المصرفية. في المقابل، جاء بُعد الوعي الأمني والعامل البشري في المرتبة الأخيرة بمتوسط حسابي بلغ (3.84) وانحراف معياري (0.74)، وهو ما يشير إلى أن هذا البُعد يمثل أقل الأبعاد من حيث مستوى التطبيق مقارنة ببقية الأبعاد، فضلاً عن وجود تباين نسبي في استجابات أفراد العينة تجاهه .

وتشير هذه النتائج بصورة عامة إلى وجود اهتمام ملحوظ بتطبيق الجوانب التنظيمية والفنية المرتبطة بمعيار ISO/IEC 27001داخل المصارف التجارية الليبية، مع استمرار الحاجة إلى تعزيز برامج التوعية والتدريب الأمني بما يسهم في رفع مستوى الوعي السيبراني لدى العاملين وتحسين فعالية الممارسات الأمنية بشكل متكامل

3-5 اختبار الفرضيات وتحليل الاثر Inferential statistics

3-5-1 مصفوفة ارتباط بيرسون Pearson correlation

لقياس طبيعة وقوة العلاقة بين المتغيرات المستقلة (ابعاد المعيار) والمتغير التابع (الامن السيبراني)

(الحوكمة والسياسات ←→ الأمن السيبراني) r = 0.67 : علاقة طردية قوية دالة

(إدارة المخاطر ←→ الأمن السيبراني) r = 0.76 : علاقة طردية قوية جداً وهي الأعلى

(الضوابط التقنية ←——— الأمن السيبراني) r = 0.71 : علاقة طردية قوية دالة

(الوعي الأمني ———→ الأمن السيبراني) r = 0.58 : علاقة طردية متوسطة إلى قوية

جميع *العلاقات دالة إحصائياً عند مستوى دلالة* $\alpha \leq 0.01$

3-5-2 تحليل الانحدار المتعدد(Multiple Regression)

لاختبار الفرضية الرئيسة للدراسة "يوجد أثر ذو دلالة إحصائية لتطبيق متطلبات معيار ISO/IEC 27001 على مستوى الأمن السيبراني."

نتائج نموذج الانحدار:

- **معامل التحديد (R^2 = 0.658)** : يعنى أن أبعاد الالتزام بالمعيار الدولي ISO/IEC 27001 تفسر ما نسبته **65.8%** من التباين الحاصل في مستوى الأمن السيبراني داخل المصارف التجارية الليبية، في حين تعود النسبة المتبقية (34.2%) لعوامل أخرى خارجة عن نموذج الدراسة الحالي.
- **قيمة (F) المحسوبة:** بلغت قيمتها دلالة إحصائية عالية جداً ($p < 0.001$) ، مما يثبت صلاحية النموذج و**قبول الفرضية الرئيسة للدراسة.**

تحليل الأثر التفاضلي للأبعاد (اختبار الفروض الفرعية):

- **بُعد إدارة المخاطر(RISK)** : حقق أعلى أثر معنوي ($p < 0.05$,$t = 3.64$, $\beta = 0.39$) ودال إحصائياً **تُقبل الفرضية الفرعية الأولى.**
- **بُعد الضوابط التقنية (CTRL):** بأثر دال إحصائياً ($p < 0.05$,$t = 2.98$, $\beta = 0.32$) جاء في المرتبة الثانية. **تُقبل الفرضية الفرعية الثانية**
- **بُعد الحوكمة والسياسات (GOV)** : أظهر أثراً إيجابياً دالاً ($p \le 0.05$,$t = 2.11$, $\beta = 0.24$) **تُقبل الفرضية الفرعية الثالثة**
- **بُعد الوعي الأمني (AWARE):** أظهر أثراً إيجابياً ضعيفاً إحصائياً في وجود بقية المتغيرات ($p > 0.05$,$t = 1.34$, $\beta = 0.15$) **تقبل إحصائياً في الارتباط وتضعف في الانحدار نظراً للحاجة إلى تطويره ميدانياً.**

رابعاً: مقارنة النتائج النهائية بالدراسات السابقة

عند إسقاط هذه النتائج على الدراسات المرجعية في المتن النظري:

4-1 الاتفاق مع دراسة (Kristian Gala 2025; محمد & البركي, 2020) أكدت النتائج الحالية أن المصارف الليبية تعاني من فجوة واضحة في "الوعي الأمني وسلوك العاملين"؛ فرغم الصرف المالي والتقني على جدران الحماية وإدارة المخاطر، إلا أن تدريب الموظفين لا يزال أقل الأبعاد تطبيقاً، وهو ما حذرت منه دراسة البركي في البيئة الليبية.

4-2 الاتفاق مع دراسة (Ryanto & Tundjungsari, 2024): بينت دراسة ريانتو أن الإدارة الصارمة للمخاطر وفق تحديثات ISO 27002:2022 هي الداعم الأول لاستقرار الأنظمة المصرفية، وهو ما تطابق رقمياً مع دراستك حيث جاء بُعد المخاطر كأعلى متوسط حسابي وأقوى ارتباط وتأثير.

4-3 مفارقة دراسة (Sharma & Dash, 2012): أشارت دراسة شارما إلى أن الحوكمة توفر الحماية القصوى؛ بينما أظهرت نتائج عينة المصارف الليبية أن الحوكمة تأتي ثانياً بعد إدارة المخاطر، والسبب يعود

إلـى الطـابع التشـغيلي للمصـارف الليبيـة التـي تركـز علـى سـد الثغـرات الفنيـة والماليـة العاجلـة قبـل الالتـزام بالحوكمـة الشاملة طويلة الأجل.

خامساً: النتائج والتوصيات

5-1 النتائج

1- أظهرت نتائج الدراسة أن مستوى الالتزام بتطبيق متطلبات معيار ISO/IEC 27001 في المصارف التجارية الليبية جاء مرتفعاً بصورة عامة.

2- جاء بُعد إدارة المخاطر السيبرانية في المرتبة الأولى من حيث مستوى التطبيق، مما يعكس اهتمام المصارف بتحديد المخاطر وتقييمها ومعالجتها بصورة مستمرة.

3- احتل بُعد الحوكمة وسياسات أمن المعلومات المرتبة الثانية، مما يدل على وجود اهتمام بتطوير السياسات والإجراءات المنظمة لأمن المعلومات.

4- أظهرت النتائج ارتفاع مستوى تطبيق الضوابط التقنية والإجرائية الداعمة لحماية الأنظمة والبيانات المصرفية.

5- سجل بُعد الوعي الأمني والعامل البشري أدنى متوسط بين أبعاد الدراسة، مما يشير إلى الحاجة إلى تعزيز برامج التدريب والتوعية الأمنية للعاملين.

6- بينت نتائج تحليل الارتباط وجود علاقات إيجابية ذات دلالة إحصائية بين جميع أبعاد معيار ISO/IEC 27001 ومستوى الأمن السيبراني.

7- أوضحت نتائج الانحدار المتعدد أن أبعاد المعيار تفسر نسبة كبيرة من التباين في مستوى الأمن السيبراني بالمصارف التجارية الليبية.

8- تبين أن إدارة المخاطر السيبرانية تمثل أكثر الأبعاد تأثيراً في تعزيز الأمن السيبراني، تليها الضوابط التقنية والإجرائية، ثم الحوكمة وسياسات أمن المعلومات.

9- أكدت النتائج أهمية الالتزام المتكامل بمتطلبات معيار ISO/IEC 27001 في تحسين مستوى الأمن السيبراني داخل المصارف التجارية الليبية.

5-2 التوصيات

1- تعزيز الالتزام الشامل بمتطلبات معيار ISO/IEC 27001 وتبني أفضل الممارسات الدولية في إدارة أمن المعلومات.

2- تطوير برامج تدريب وتوعية أمنية دورية للعاملين لرفع مستوى الوعي بالمخاطر السيبرانية وأساليب التعامل معها.

3- تعزيز تطبيق منهجية إدارة المخاطر السيبرانية وتحديثها بصورة مستمرة لمواكبة التهديدات الناشئة.

4- الاستمرار في تطوير الضوابط التقنية والإجرائية المتعلقة بحماية البيانات وإدارة الوصول والتشفير واستمرارية الأعمال.

5- دعم دور الإدارة العليا في تبني سياسات أمن المعلومات ومتابعة تنفيذها وتقييم فعاليتها بشكل دوري.

6- إجراء اختبارات دورية للأمن السيبراني وخطط الاستجابة للحوادث وخطط التعافي من الكوارث.

7- تشجيع المصارف التجارية الليبية على الحصول على شهادة الاعتماد ISO/IEC 27001 لتعزيز مستوى الامتثال والموثوقية.

8- توجيه الدراسات المستقبلية نحو دراسة متغيرات إضافية مثل الذكاء الاصطناعي، والتشريعات السيبرانية، والبنية التحتية الرقمية وأثرها على الأمن السيبراني في القطاع المصرفي

المراجع:

- Adelmann, F., Ergen, I., Gaidosch, T., Jenkinson, N., Khiaonarong, M. T., Morozova, A., . . . Wilson, C. (2020). *Cyber risk and financial stability: It'sa small world after all*: International Monetary Fund.
- Al-Dhahri, S., Al-Sarti, M., & Abdul, A .(2017) .Information security management system. *International Journal of Computer Applications, 158*(7), 29-33 .
- Choubey, S., & Bhargava, A. (2018). Significance of ISO/IEC 27001 in the implementation of governance, risk and compliance. *International Journal of Scientific Research in Network Security and Communication, 6*(2), 30-33 .
- Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *The TQM Journal, 33*(7), 76-105 .
- ENISA. (2024). ENISA Threat Landscape. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
- Ewuga, S. K., Egieya, Z., Omotosho, A., & Adegbite, A. (2023). ISO 27001 in banking: An evaluation of its implementation and effectiveness in enhancing information security. *Finance and Accounting Research Journal, 5*(12), 405-425 .
- G'ofurova Laziza, R. S. (2025). DIFFERENCES BETWEEN INFORMATION SECURITY AND CYBERSECURITY. *Modern Science and Research, 4*(6), 234-237.
- Humphreys, E. (2016). *Implementing the ISO/IEC 27001: 2013 ISMS Standard*: Artech house.
- Hyseni, V. (2025, ,). Information security in banks and financial institutions. *PECB.* Retrieved from https://pecb.com/en/article/information-security-in-banks-and-financial-institutions?utm_source=chatgpt.com
- ISO/IEC 27001:2022. (2022). ISO/IEC 27001:2022 - information security management systems. Retrieved from https://www.iso.org/standard/27001
- Kamil, Y., Lund, S., & Islam, M. S. (2023). Information security objectives and the output legitimacy of ISO/IEC 27001: stakeholders' perspective on expectations in private organizations in Sweden. *Information Systems and e-Business Management, 21*(3), 699-722 .
- Katuri, S. (2025). Cybersecurity threats in digital banking :A comprehensive analysis. *IJSAT-International Journal on Science and Technology, 16* .(1)
- Kristian Gala , R. S., Muh. Ashary Anshar,. (2025). ANALYSIS OF THE IMPLEMENTATION OF ISO/IEC 27001:2013 STANDARDS IN PT. SULSELBAR BANK. *International Journal of Multidisciplinary Research and Literature, Vol. 4, No. 4, July 2025, pp. 771-783* .
- Legowo, N., & Juhartoyo, Y. (2022). Risk management; risk assessment of information technology security system at bank using ISO 27001. *Journal of System and Management Sciences, 12*(3), 181-199 .
- Mohammed Alharbi, T. S. (2025). Cybersecurity governance and organizational resilience: A framework for sustainable risk management. *EDPACS*, 1-16 .
- Putri, S. R. M., Bernandy, M. P., Aulia, C., Fikri, M. G. R., & Jasmine, J. (2024). Cyber Security Risk Management Practices: Insights From an ISO 27001 Certified Organization. *Journal of Digital Business and Innovation Management, 3* .(2)
- Ryanto, K., & Tundjungsari, V. (2024). Standardization of Information Security Management in the Banking Sector using the ISO 27001: 2022 Framework. *Journal La Multiapp, 5*(4), 361-379 .

- Sharma, N., & Dash, P. K. (2012). Effectiveness of ISO 27001, as an information security management system: an analytical study of financial aspects. *Far East Journal of Psychology and Business, 9*(3), 42-55 .
- Styoutomo, Y. A., & Ruldeviyani, Y. (2023). Information security awareness raising strategy using fuzzy ahp method with hais-q and iso/iec 27001: 2013: A case study of xyz financial institution. *CommIT (Communication and Information Technology) Journal, 17*(2), 133-149 .
- Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & security, 23*(5), 371-376 .
- Yesugad, K. D. (2024). CYBERSECURITY CHALLENGES IN THE MODERN BANKING SECTOR. *IPE Journal of Management, 14, No 16, July-December 2024* .

- فيلالي, & أسماء. (2021). دور المواصفة الدولية ISO/IEC 27001 في الرفع من مصداقية نظام إدارة أمن المعلومات في المؤسسة. مجلة إضافات إقتصادية, 5(1), 204-223.
- هدى محمد حسن عبد الرحمن. (2026). دور معايير الأنتوساي (INTOSAI) في تحسين جودة الأداء المالي (دراسة ميدانية على الديوان الليبي). *مجلة الفاروق للعلوم , 2* (3), 16-28.
- محمد, أ., & البركـي, ح. (2020). واقع تطبيق مُتطلبات نُظم إدارة أمن المعلومات المتوافقة مع المواصفة 27001: ISO 2005 بالمصارف العاملة بمدينتي بنغازي والبيضاء. مجلة الاقتصاد الدولي والعولمة, 3(2), 143-162.