Vol.(9) Issue. (1) April 2026,
Faculty of Economics, Sirte University (Vol (9), No (1)
Economic Studies Journal (ESJ), مجلة الدراسات الاقتصادية
كلية الاقتصاد – جامعة سرت Faculty of Economics, Sirte University
https://journal.su.edu.ly/index.php/esj/ar
https://doi.org/10.37375/esj.v9i1.3988

دور حوكمة الأمن السيبراني في تعزيز دقة التقارير المالية: دراسة ميدانية بالمصارف التجارية الليبية

أ. مريم مصباح مفتاح سحيم
أستاذ مساعد، قسم المحاسبة، كلية الاقتصاد–العجيلات، جامعة الزاوية، ليبيا
m.sheem@zu.edu.ly

تاريخ الاستلام:2025.12.10 تاريخ القبول: 2026.02.21 تاريخ النشر:2026.04.01

الكلمات المفتاحية

حوكمة الأمن السيبراني، دقة التقارير المالية، المصارف التجارية.

الملخّص

في ظل التحول الرقمي المتسارع وتنامي التهديدات السيبرانية، تواجه المصارف التجارية الليبية تحدياً جوهرياً يتمثل في حماية نظم المعلومات المحاسبية وضمان سلامة البيانات المالية من الاختراق أو التلاعب، بما ينعكس مباشرة على دقة التقارير المالية وموثوقيتها. ويثير هذا الواقع إشكالية تتعلق بمدى فاعلية ممارسات حوكمة الأمن السيبراني في الحد من المخاطر السيبرانية وتعزيز جودة المخرجات المالية. انطلاقاً من ذلك، هدف البحث إلى تحليل أثر حوكمة الأمن السيبراني في تعزيز دقة التقارير المالية في المصارف التجارية الليبية. واعتمد البحث على المنهج الوصفي التحليلي، حيث تم جمع البيانات من خلال استبيان وُزّع على عينة من العاملين بالمصارف التجارية، ثم تحليلها باستخدام الأساليب الإحصائية المناسبة. وخلص البحث إلى وجود أثر ذي دلالة إحصائية لحوكمة الأمن السيبراني بأبعادها المختلفة في تعزيز دقة التقارير المالية، مما يعكس أهمية وجود أطر تنظيمية مما يدل على أن تطبيق حوكمة الأمن السيبراني يسهم بشكل فعال في تحسين وتعزيز دقة التقارير المالية. وضوابط رقابية فعّالة لإدارة المخاطر السيبرانية. ويوصي البحث بضرورة تبني إطار مؤسسي متكامل لحوكمة الأمن السيبراني، يتضمن إنشاء لجان متخصصة وتعزيز الرقابة والسياسات التنظيمية، بما يدعم موثوقية المعلومات المالية ويرفع مستوى الثقة في التقارير الصادرة عن المصارف.

The Role of Cybersecurity Governance in Enhancing the Accuracy of Financial Reporting: A Field Study in Libyan Commercial Banks

Mariam Misbah Muftah sheem
Assistant Professor, Department of Accounting, Faculty of Economics - Ajilat, University of Zawiya, Libya
m.sheem@zu.edu.ly

Abstract

In light of the rapid digital transformation and the growing cyber threats, Libyan commercial banks face a fundamental challenge: protecting their accounting information systems and ensuring the integrity of their financial data from breaches or manipulation. This directly impacts the accuracy and reliability of financial reports. This reality raises the question of the effectiveness of cybersecurity governance practices in mitigating cyber risks and enhancing the quality of financial outputs. Therefore, this research aims to analyze the impact of cybersecurity governance on enhancing the accuracy of financial reports in Libyan commercial banks. The research employed a descriptive-analytical approach, collecting data through a questionnaire distributed to a sample of commercial bank employees and then analyzing it using appropriate statistical methods. The research concluded that cybersecurity governance, in its various dimensions, has a statistically significant impact on enhancing the accuracy of financial reports. This demonstrates that implementing cybersecurity governance effectively contributes to improving and strengthening the accuracy of financial reports, highlighting the importance of having effective regulatory frameworks and oversight controls for managing cyber risks. The research recommends the need to adopt an integrated institutional framework for cybersecurity governance, which includes the establishment of specialized committees and the strengthening of oversight and regulatory policies, in order to support the reliability of financial information and raise the level of confidence in reports issued by banks.

Keywords

Cybersecurity Governance, Financial Reporting Accuracy, Commercial Banks

أولا: الجانب التمهيدي

1.1 مقدمة

يرتبط نظام المعلومات المحاسبية بشكل خاص بإدارة المؤسسة فهو يُنتج تقارير مالية بالغة الأهمية من أجل الاستجابة بشكل مناسب لمتطلبات الإدارة واتخاذ القرارات، وهذا يعتبر دافع أولي لتحسين محتوى المعلومات، كما يعكس تطور إعداد التقارير بشكل مباشر تطور أنظمة المعلومات المحاسبية، حيث أن التحول من أساليب معالجة البيانات التقليدية في المحاسبة إلى أساليب أحدث له عدد من المزايا، أهمها أن المعلومات المبلغ عنها ستكون متكاملة وموثوقة وفي الوقت المناسب ودقيقة، مما يعزز دقة التقارير المالية وكفاءتها(Halasa, 2024). فدقة التقارير المالية تمثل عنصرًا أساسيًا في جودة التقارير المالية والتي تعني أهمية توفير تمثيل صادق، والتأكد من أن المعلومات المالية المبلغ عنها تعكس بدقة الأداء الاقتصادي الأساسي للمؤسسة، إذ تعزز هذه الدقة الثقة بين أصحاب المصلحة، وتمكنهم من اتخاذ قرارات مستنيرة بناءً على تصوير موثوق للوضع المالي لها(Johri, 2024)، ومع ذلك، فإن هذا التحول يقدم أيضًا تحديات جديدة تتعلق بحماية البيانات والخصوصية والامتثال للمعايير التنظيمية، بسبب إن التهديدات السيبرانية تتزايد تواتراً وتعقيداً، والبيانات المالية التي غالباً ما تعتبر حساسة وقيمة، تشكل هدفاً رئيساً لمجرمي الإنترنت (Jumble & Mirza, 2025).

تشمل مخاطر الأمن السيبراني التي يمكن أن تؤثر على دقة وموثوقية تقارير الجودة المالية التهديدات الداخلية والخارجية لسرية البيانات المالية ودقتها وتوافرها، و يمكن أن تتراوح هذه المخاطر من الفيروسات إلى القراصنة، وبرامج الفدية، وهجمات رفض الخدمة، (Basiouny et al., 2024) ، لذا تعمل حوكمة الأمن السيبراني كحماية للشبكات وأنظمة التكنولوجيا التشغيلية وأنظمة تكنولوجيا المعلومات في المصارف، بما في ذلك مكوناتها من البرامج والأجهزة والبيانات والخدمات ضد أي وصول غير مصرح به أو تعطيل أو تغيير (Al-Rawashdeh et AL., 2024).

ويؤكد قانون ساربينز أوكسلي (SOX)، واللائحة العامة لحماية البيانات (GDPR)، وإطار بازل 3 على الحاجة إلى قيام المؤسسات بإنشاء حوكمة قوية للأمن السيبراني، وإجراء تقييمات منتظمة للمخاطر للكشف عن الأنشطة غير المصرح بها(Emmanuel, 2025) ، ونتيجة لتزايد الوعي بالأمن السيبراني في مختلف المؤسسات، لذلك تركز العديد منها جهودها على وضع سياسات سيبرانية فعالة (Lubua & Pretorius, 2019)، وإعطاء الأولوية لدقة وتناسق وتحقق بياناتها المالية للحفاظ على الشفافية والامتثال للوائح والحفاظ على ثقة المستثمرين والجهات التنظيمية وأصحاب المصلحة الآخرين (Jumble & Mirza, 2025)، ويستوجب ذلك على أعضاء مجلس الإدارة والرؤساء التنفيذيين وغيرهم من أصحاب المصلحة العمل معًا بشكل وثيق لضمان الالتزام بسياسات الأمن السيبراني (Alnor et AL., 2024) . لذا جاء هذا البحث لاستكشاف وتحليل دور الحوكمة السيبرانية في تعزيز دقة التقارير المالية من وجهة نظر العاملين بالمصارف التجارية.

2.1 الدراسات السابقة

– دراسة (شقلوف، 2024) بعنوان: الحوكمة وأثرها على الإفصاح المحاسبي وجودة التقارير المالية: دراسة تطبيقية على المصارف التجارية بمدينة طرابلس.

هدفت هذه الدراسة إلى التعرف على قواعد الحوكمة على الإفصاح وجودة التقارير الصادرة عن المصارف التجارية العاملة في مدينة طرابلس. وتمثل مجتمع الدراسة في المصارف التجارية العاملة في مدينة طرابلس، وتتكون عينة الدراسة من أعضاء مجلس الإدارة وأعضاء الإدارة التنفيذية والوسطى، ولغرض جمع البيانات الأولية، تم إعداد صحيفة استبيان تحتوي على (20) فقرة موزعة على ثلاثة محاور لخدمة فرضيات الدراسة، حيث تم توزيع عدد (60)

صحيفة استبيان في حين كان عدد الصحف المستلمة والصالحة للتحليل (55). ولغرض تحليل البيانات الأولية واستخراج نتائج الدراسة، تم استخدام الأسلوب الإحصائي المناسب (one Sample T- test)، وتوصلت هذه الدراسة إلى أن هناك وجود أثر لقواعد الحوكمة على الإفصاح المحاسبي وجودة التقارير المالية الصادرة عن المصارف التجارية قيد الدراسة. وعدم وجود أثر معنوي ذو دلالة إحصائية للمؤشرات المعاملة المتكافئة للمساهمين ومبدأ الإفصاح والشفافية على جودة التقارير المالية بالمصارف، أيضا توصلت الدراسة إن مستوى تطبيق مبادئ الحوكمة بالمصارف قيد الدراسة كان متوسطاً، وإن مستوى جودة التقارير المالية بالمصارف قيد الدراسة كان متوسطاً.

– دراسة (محمد، 2023) بعنوان: المقدرة التقييمية للالتزام بضوابط حوكمة الأمن السيبراني وتأثيره على قرارات المستثمرين: دراسة تطبيقية على شركات الاتصالات السعودية (زين –STC).

هدفت هذه الدراسة إلى قياس المقدرة التقييمية (المباشرة – غير المباشرة للإفصاح عن ضوابط حوكمة الأمن السيبراني باستخدام نموذج (Ohlson, 1995) والذى يشمل نموذجي (سعر السهم – عائد السهم) بالإضافة إلى قياس تأثير الإفصاح عن ضوابط حوكمة الأمن السيبراني على قرارات المستثمرين ، ولتحقيق هدفي البحث قامت الباحثة باشتقاق فروض البحث واختبارها من خلال إجراء دراسة تطبيقية باستخدام بيانات التقارير المالية السنوية لشركتي زين و STC، و توصلت الدراسة باستخدام تحليل الانحدار الخطي المتعدد إلى وجود مقدرة تقييمية مباشرة للإفصاح عن ضوابط حوكمة الأمن السيبراني من خلال تأثيرها على سعر السهم وعائد السهم ولكن معامل استجابة سعر السهم كان أعلى من معامل استجابة عائد السهم ووجود تأثير إيجابي معنوي لربحية السهم على سعر السهم وعائد السهم وتأثير إيجابي غير معنوي للقيمة الدفترية للسهم على سعر السهم وعائد السهم ، كما تبين وجود تفاوت في المقدرة التقييمية للإفصاح عن ضوابط حوكمة الأمن السيبراني ، ووجود تأثير معنوي للإفصاح عن ضوابط حوكمة الأمن السيبراني على قرارات المستثمرين بدلالة التأثير على (حجم التداول والمدى السعرى للسهم).

– دراسة (عبد الله، 2023) بعنوان: الأمن السيبراني في القطاع المالي مع الإشارة لواقع الأمن السيبراني في ليبيا.

هدفت هذه الدراسة إلى التعرف على أهم التهديدات والمخاطر السيبرانية التي تواجه القطاع المالي، وكذلك التعرف على واقع الأمن السيبراني في ليبيا. وتم الاعتماد على المنهج الاستقرائي بأداتيه الوصف والتحليل؛ وذلك من خلال الرجوع إلى مختلف الأدبيات النظرية والتطبيقية والتقارير؛ بهدف التعرف على الجوانب النظرية المتعلقة بالأمن السيبراني وما يحتويه من مخاطر وتهديدات للقطاع المالي، بالإضافة إلى إجراء المقابلات الشخصية مع ذوي الاختصاص وعلاقتهم المباشرة بموضوع الدراسة. توصلت الدراسة إلى أن الدولة الليبية تمتلك بنية تحتية تقنية قابلة للتطوير وتغطي معظم مناطق ليبيا تساعد في إمكانية الاستثمار في الفضاء السيبراني، وإمكانية التحول للاقتصاد الرقمي، وكذلك إمكانية تطوير كافة الخدمات الحكومية المقدمة للمواطنين، كما توصلت إلى عدم وجود استراتيجية واضحة المعالم للاستثمار في الفضاء السيبراني بليبيا. ولا يوجد أطر قانونية تسند عليها الدولة الليبية فيما يخص الأمن السيبراني.

– دراسة (Lisnawati, 2024) بعنوان: financial performance is influenced by adaptation to financial technology and cyber governance.

"كيف يتأثر الأداء المالي بالتكيف مع التكنولوجيا المالية والحوكمة السيبرانية". هدفت هذه الدراسة إلى دراسة تأثير التكيف مع التكنولوجيا المالية والحوكمة السيبرانية على

الأداء المالي في المؤسسات المالية. وتم استخدام الأساليب الكمية في هذه الدراسة، مع تقنيات جمع بيانات تحليل المحتوى لـ 94 بيانات مراقبة مصرفية واردة في بورصة إندونيسيا (BEI) في عامي 2022 و2023. بناءً على الاختبار الهيكلي لنموذج PLS SEM، وتوصلت إلى أن التكيف مع التكنولوجيا المالية له تأثير إيجابي كبير على الأداء المالي. في حين أن الحوكمة السيبرانية ليس لها تأثير على الأداء المالي. وذلك لان العدد المحدود من المصارف التي تكشف عن الحوكمة السيبرانية هو قيد رئيس في هذه الدراسة.

- دراسة (Al-Rawashdeh et AL., 2024) بعنوان: The impact of cyber governance on financial technology implementation: The mediating role of internal control effectiveness.

" أثر الحوكمة السيبرانية على تنفيذ التكنولوجيا المالية: الدور الوسيط لفعالية الرقابة الداخلية". هدفت هذه الدراسة إلى التعرف على أثر الحوكمة السيبرانية على تطبيق التكنولوجيا المالية، بالإضافة إلى الدور الوسيط لفعالية الرقابة الداخلية في البنوك التجارية الأردنية باستخدام المنهج الوصفي التحليلي. وقد تم استخدام أسلوب المسح الشامل الذي شمل جميع البنوك التجارية الأردنية المدرجة في بورصة عمان، مما أدى إلى حجم عينة بلغ 12 بنكًا أردنيًا. وقد تم توزيع الاستبانة المصممة على الموظفين في مختلف المستويات الإدارية في جميع البنوك التجارية الأردنية وتحليلها باستخدام كل من برنامج (SPSS) وبرنامج AMOS. وقد توصلت الدراسة إلى أن هناك تأثيرًا كبيرًا للحوكمة السيبرانية على تطبيق التكنولوجيا المالية من خلال الدور الوسيط لفعالية الرقابة الداخلية. ويشير هذا الاكتشاف إلى التأثير الإيجابي للحوكمة السيبرانية على تطبيق التكنولوجيا المالية، والذي يتحقق من خلال تأثيرها المباشر على فعالية الرقابة الداخلية، مما يؤثر بدوره على تطبيق التكنولوجيا المالية في البنوك التجارية الأردنية.

- دراسة (Al-Mohaerb, 2025) بعنوان: Impact of Cyber Governance Quality on Dividend Policy in Mitigating Cybersecurity Breaches.

" تأثير جودة الحوكمة السيبرانية على سياسة توزيع الأرباح في التخفيف من انتهاكات الأمن السيبراني". هدفت هذه الدراسة إلى دراسة العلاقة بين المخاطر السيبرانية وسياسة توزيع الأرباح، وكذلك كيف تؤثر مجالس الإدارة، كآلية للحوكمة، على سياسة توزيع الأرباح في ظل المخاطر السيبرانية. جمعت هذه الدراسة التمويل على مستوى الشركة، والحوكمة المؤسسية، ومتغيرات التحكم من قاعدة بيانات بلومبرج خلال الفترة 2013-2022. تقيس هذه الدراسة المخاطر السيبرانية من خلال الإفصاحات المتاحة للجمهور للشركات على النموذج K-10. وتوصلت إلى أن المخاطر السيبرانية تؤثر بشكل كبير على سياسة توزيع الأرباح من خلال فرض تحديات على الاتصالات الفنية للشركات والشفافية المالية. وتؤدي مجالس الإدارة الفعالة دورًا حاسمًا في توجيه الشركات نحو استراتيجيات الحوكمة التي تعزز سياسة توزيع الأرباح وتحسن الأمن السيبراني.

ما يميز الدراسة الحالية عن الدراسات السابقة: تتميز الدراسة الحالية بانها تُعد من الدراسات القليلة التي تناقش بشكل خاص استكشاف وتحليل دور حوكمة الأمن السيبراني في دقة التقارير المالية، ولم تتناول أي دراسة سابقة في ليبيا هذا الموضوع حسب علم الباحثة، إذ أن هذه الدراسة أضافت إلى هذه الدراسات أبعاداً أخرى بإظهار دور حوكمة الأمن السيبراني في دقة التقارير المالية.

3.1 مشكلة البحث

يزيد استخدام النظام الألي في جمع البيانات وتخزينها ونقلها من احتمالية الاحتيال أو التلف أو التعطيل وتسرب المعلومات مما يشكل تهديدًا للمؤسسات المالية، ويؤثر على قدرتها على العمل بشكل صحيح وتوليد عوائد مالية (Basiouny et al., 2024)، ومع اعتماد المؤسسات بشكل متزايد على الأنظمة الرقمية لإدارة البيانات المالية، فقد نمت المخاطر المرتبطة بالتهديدات السيبرانية وانتهاكات البيانات وعدم دقة التقارير بشكل كبير، وفي هذا السياق، لا يعد الأمن السيبراني وسلامة البيانات مجرد مخاوف فنية ولكنها عناصر أساسية لاستراتيجية أوسع تهدف إلى الحفاظ على ثقة أصحاب المصلحة وضمان الامتثال للمعايير التنظيمية (Jumble & Mirza, 2025)، وتحميل الإدارة مسؤولية إجراءات إدارة المخاطر، يتطلب وجود مجلس إدارة مؤهل يتمتع بالخبرة اللازمة(Alnor et AL., 2024).

علاوة على ذلك، يتعين على جميع المصارف إجراء تقييمات مستمرة على الأقل سنويًا لمخاطر التكنولوجيا، خاصة عند تقديم أنظمة جديدة (Al-Rawashdeh et AL., 2024)، فعلى الرغم من التحسينات المستمرة في مجال الأمن السيبراني، فإن خطر الاختراق لا يزال قائمًا بسبب التطور المستمر لمهارات المتسللين (Al-Mohaerb, 2025)، على سبيل المثال، قد تشكل السياسات غير الشاملة والتي تفتقر إلى دعم الإدارة العليا تحديًا أمنيًا، كما تتطلب سياسة الأمن السيبراني مراجعة دورية لاستيعاب التهديدات الجديدة (Lubua & Pretorius, 2019). ويمكن أن يؤدي عدم الامتثال للوائح ومعايير الأمن السيبراني إلى تعريض المؤسسات للمخاطر القانونية والتنظيمية، التي تشير عدم الامتثال وإلى نقاط ضعف في ممارسات الحوكمة (Basiouny et al., 2024). لذا يؤكد (Al-Rawashdeh et AL., 2024) على ضرورة قيام المصارف والجهات الرقابية التابعة لها بتبني نظام شامل لحوكمة الأمن السيبراني والتكنولوجيا المالية المتقدمة كجزء لا يتجزأ من حوكمة الأمن السيبراني.

وفي ليبيا فإن سمات الفضاء الإلكتروني للمؤسسات العامة الليبية هي ضعف أو انعدام الحوكمة، وارتفاع كبير في مستوى المخاطر السيبرانية (القصير، 2024)، وعملية التحول الرقمي في المؤسسات الليبية لم يراعَ فيها الأمان الكافي، كما يعاني مصرف ليبيا المركزي في الفترة الأخيرة من هجمات سيبرانية متعددة، إذ تعرضت منصة حجز العملة الأجنبية للأفراد إلى هجوم سيبراني (عبد الله، 2024). وأكد (شوران، 2025) على ضرورة تحديث التشريعات الليبية في مجال الأمن السيبراني، معتبرًا أن البلاد تفتقر إلى قوانين شاملة لحماية البيانات والبنية التحتية الحيوية. وفي أغسطس 2023، أصدر مصرف ليبيا المركزي دليل حوكمة تكنولوجيا المعلومات، وحدد الستة أشهر من النصف الثاني لعام 2024 مرحلة الشروع في تقييم وتنفيذ ما ورد من تعليمات تتعلق بحوكمة الأمن السيبراني وما في حكمه، وستقوم إدارة الرقابة على المصارف والنقد بمتابعة الموضوع من خلال المهام التفتيشية للتأكد من مدى امتثال مؤسساتِكُم لما ورد فيه، وهذا الدليل جيد من حيث الإجراءات العملية كأساس، لكن لم يوضح كيفية حوكمة الأمن السيبراني.

وعلى الرغم من الوعي المتزايد بدور الأمن السيبراني في إعداد التقارير المالية، لا تزال هناك فجوة في البحث التجريبي الذي يستكشف تأثيره المباشر على دقة البيانات المالية (Emmanuel, 2025)، **ومما سبق يمكن تلخيص مشكلة البحث في التساؤل الرئيس التالي:**

– ما دور حوكمة الأمن السيبراني في تعزيز دقة التقارير المالية من وجهة نظر العاملين بالمصارف التجارية؟

ومن التساؤل الرئيس تمت صياغة التساؤلات الفرعية التالية:

- ما دور التزام مجلس الإدارة بالأمن السيبراني في تعزيز دقة التقارير المالية؟

- ما دور سياسات الأمن السيبراني في تعزيز دقة التقارير المالية؟
- ما هو دور الامتثال لمتطلبات الأمن السيبراني في تعزيز دقة التقارير المالية؟

4.1 أهداف البحث:

يهدف هذا البحث لتحقيق الهدف الرئيس التالي:

– استكشاف وتحليل دور حوكمة الأمن السيبراني في تعزيز دقة التقارير المالية من وجهة نظر العاملين بالمصارف التجارية.

ولتحقيق هذا الهدف يستلزم تحقيق الأهداف التالية:

- بيان دور التزام مجلس الإدارة بالأمن السيبراني في تعزيز دقة التقارير المالية.
- التعرف على فعالية سياسات الأمن السيبراني في تعزيز دقة التقارير المالية.
- التعرف على دور الامتثال لمتطلبات الأمن السيبراني في تعزيز دقة التقارير المالية.

5.1 فرضيات البحث:

للإجابة عل تساؤلات البحث، ولتحقيق أهداف البحث تمت صياغة الفرضيات التالية:

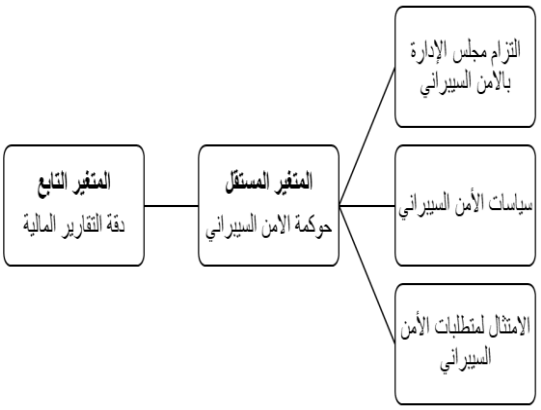
– الفرضية الرئيسة: تسهم حوكمة الأمن السيبراني في تعزيز دقة التقارير المالية في المصارف التجارية.

ومن الفرضية الرئيسة تمت صياغة الفرضيات الفرعية التالية:

- الفرضية الفرعية الأولى: يسهم التزام مجلس الإدارة بالأمن السيبراني في تعزيز دقة التقارير المالية.
- الفرضية الفرعية الثانية: يسهم وجود سياسات للأمن السيبراني في تعزيز دقة التقارير المالية.
- الفرضية الفرعية الثالثة: يسهم الامتثال لمتطلبات الأمن السيبراني في تعزيز دقة التقارير المالية.

6.1 نموذج البحث:

يوضح الشكل التالي متغيرات البحث (المتغير التابع والمتغير المستقل).



الشكل رقم (1) نموذج البحث

المصدر: (إعداد الباحثة).

7.1 أهمية البحث:

تكمن أهمية هذا البحث في كونه محاولة علمية حديثة لاستكشاف وتحليل دور حوكمة الأمن السيبراني في دقة التقارير المالية، وتنبع الأهمية العلمية للبحث من اعتباره من الدراسات المثيرة للاهتمام التي تبحث في دور حوكمة الأمن السيبراني في دقة التقارير المالية، وبالتالي فإن هذا البحث قد يسهم في زيادة المعرفة لدى الباحثين بحيث يمكن لهم الاعتماد عليه واستقصاء المعلومات اللازمة في إعداد دراساتهم المستقبلية ذات الصلة، كما تبرز الأهمية العملية للبحث من خلال مساهمة نتائج البحث في رفع وعي العاملين في المصارف التجارية بأهمية الالتزام بممارسات حوكمة الأمن السيبراني، بالإضافة إلى التوصيات التي يقدمها لتعزيز دقة التقارير المالية في المصارف التجارية.

8.1 منهجية البحث

في ضوء طبيعة مشكلة البحث ولتحقيق أهدافه تم إتباع المنهج الوصفي التحليلي ذو الطابع الاستكشافي، ويتمثل ذلك في إطاره النظري الذي يتم فيه الحصول على المعلومات المختلفة الخاصة بجوانبه النظرية وذلك من خلال الاطلاع المراجع المتعلقة بموضوع البحث، ومن ثم البحث

في الجانب الميداني بتوزيع استبانات على عينة البحث وتجميعها لاستكشاف واقع حوكمة الأمن السيبراني من وجهة نظر العاملين بالمصارف التجارية ، ومن ثم تفريغها وتحليلها واستخدام البرنامج الإحصائي Statistical (Package for Social Science) SPSS وإجراء الاختبارات الإحصائية المناسبة بهدف الوصول لدلالات ذات قيمة ومؤشرات تدعم موضوع البحث واستخلاص وصياغة التوصيات اللازمة بناء على النتائج التي تم التوصل إليها.

9.1 حدود البحث:

الحدود المكانية: المصارف التجارية الليبية العامة العاملة في مدينة صبراتة، حيث تم إجراء البحث ميدانياً على مصرف الجمهورية، ومصرف الوحدة، ومصرف الصحاري، ومصرف شمال أفريقيا، والمصرف التجاري الوطني.

الحدود الزمنية: تم توزيع وتجمع صحيفة الاستبيان خلال الفترة من 2025/9/3 – 2025/9/20.

الحدود الموضوعية: تحليل واستكشاف دور حوكمة الأمن السيبراني في تعزيز دقة التقارير المالية من وجهة نظر العاملين بالمصارف التجارية.

ثانياً: الإطار النظري للبحث:

1.2 حوكمة الأمن السيبراني

تعد الحوكمة السيبرانية في العلاقات الدولية من أبرز القضايا في السنوات الأخيرة، فقد بحثت المنظمات الدولية عن حلول فيما يتعلق بتحديات الحوكمة السيبرانية، وفي هذا الصدد، تم اتخاذ الخطوات الأولى من خلال التوقيع على "اتفاقية الجرائم الإلكترونية" من قبل مجلس أوروبا (Önok 2013)، بالإضافة إلى ذلك، تم اعتماد التقييس الدولي في هذا المجال فعلى سبيل المثال، يوفر معيار ISO/IEC 38500:2015 مبادئ توجيهية لأعضاء مجالس إدارة المؤسسات بشأن الاستخدام الفعال والكفء والمقبول لتكنولوجيا المعلومات داخل مؤسساتهم، وتغطي هذه الحوكمة أيضًا عمليات الإدارة والقرارات المتعلقة باستخدام تكنولوجيا المعلومات، علاوة على ذلك، يحدد معيار ISO/IEC 38500:2015 حوكمة تكنولوجيا المعلومات باعتبارها مجموعة فرعية أو مجالًا للحوكمة التنظيمية ، وعلى الرغم من وجود بعض الخطوات لتوحيد معايير حوكمة السيبرانية وتوحيد معايير تكنولوجيا المعلومات مثل ISO 22301 و ISO/IEC 27001 و27002 و27031 و27032 و27701، إلا أنه لا يوجد حتى الآن معيار إطاري يتكون من حوكمة الأمن السيبراني و تكنولوجيا المعلومات كموضوعين منفصلين (Savaş & Karataş, 2022).

والحوكمة في سياق الأمن السيبراني تشير إلى المبادئ والقواعد والأساليب الإدارية التي تتبعها المؤسسات لتنظيم سلطات اتخاذ القرار وتحديد المسؤوليات وفرض المساءلة في تنفيذ المهام والواجبات المتعلقة بحماية المؤسسة من الهجمات السيبرانية أو إساءة استخدام الأصول المعلوماتية مع ضمان استمرارية العمليات التشغيلية في حالة وقوع حوادث أو كوارث (Al-Rawashdeh et AL., 2024). فالحوكمة السيبرانية تعمل على تشغيل عمليات صنع القرار بطريقة تزيد من المشاركة والشفافية والمساءلة في اتخاذ التدابير المتعلقة بالفضاء السيبراني، إلى جانب آلية الاتفاقيات والاستراتيجيات والقوانين والتدابير واللوائح والمعايير الدولية وتنفيذها بأفضل الطرق (Savaş & Karataş, 2022).

وتُعرف الحوكمة السيبرانية على أنها عملية توجيه إجراءات الأمن السيبراني ، وتحديد تدابير التحكم في المخاطر ، ومعالجة التهديدات السيبرانية ، وضمان الامتثال للتشريعات ومعايير التشغيل والإجراءات (Chundu et al., P1, 2025)، وبالتالي، تهدف حوكمة الأمن السيبراني إلى توجيه ومراقبة وإرشاد وتعزيز وتسهيل تنسيق الجهود بين الجهات ذات الصلة، بما يتماشى مع مصالح وتطلعات أصحاب المصلحة ، دون انتهاك الاتفاقيات والقوانين التي تكون المؤسسة طرفًا فيها (Al-

(Rawashdeh et AL., 2024، كما أن وجود الحوكمة السيبرانية يركز على حماية الأصول الرقمية المملوكة للمؤسسات المالية من المخاطر الأمنية المحتملة(Lisnawati, 2024) ، **وتتمثل آليات الحوكمة السيبرانية في العناصر التالية:**

أولا: التزام مجلس الإدارة بالأمن السيبراني

يُعد هيكلية عمل المؤسسات المصرفية وهيكلية عملها عنصرًا أساسيًا في إطار حوكمة المؤسسات المصرفية الفعّاله، فيما يتعلق بالسيطرة على المخاطر المصرفية (Alnor et AL., 2024)، فيجب أن تتم الموافقة على سياسة الأمن السيبراني من أعلى سلطة متاحة قبل تطبيقها وتوفر موافقة أعلى سلطة في مؤسسة معينة بالتفويض المناسب لتطبيق السياسة على جميع المستويات داخل تلك المؤسسة، فمجلس الإدارة (أو الإدارة العليا في المؤسسات الحكومية) مسؤول عن مراجعة السياسة واعتمادها، وتُضفي موافقة مجلس الإدارة شعورًا بالمسؤولية على بقية الموظفين، بمن فيهم من هم في مستوى الإدارة العليا(Lubua & Pretorius, 2019).

ويجب أن يكون قد طور مجلس الإدارة ووافق على الضوابط الداخلية والإجراءات والسياسات لإدارة المخاطر، وكذلك يجب أن تغطي هذه اللوائح جميع جوانب إدارة المخاطر، مثل تقييم المخاطر وتقنيات التخفيف من المخاطر ومراقبتها، ويتأكد مجلس الإدارة من مشاركة هذه السياسات بشكل مناسب في جميع أنحاء المؤسسة وأنها تلتزم بأفضل الممارسات والمتطلبات القانونية فيما يتعلق بإدارة المخاطر، كما يضمن مجلس الإدارة التزام المصرف بجميع القوانين والقواعد والمعايير المعمول بها في الصناعة ، كما يراقب التطورات التنظيمية ويعدل إجراءات إدارة المخاطر في المصارف حسب الضرورة ، بالإضافة إلى ذلك، يعزز مجلس الإدارة ثقافة الامتثال في جميع أنحاء المؤسسة من خلال تسليط الضوء على أهمية السلوك الأخلاقي والامتثال للوائح والمساءلة على جميع المستويات (Alnor et AL., 2024).

ثانيا: سياسات الأمن السيبراني

السياسات هي وثائق تُسجل أساس رفيع المستوى أو مسار عمل يُشير إلى النية والاتجاه الذي حددته الإدارة، وتعرف سياسة الأمن السيبراني بأنها وثيقة تُحدد المتطلبات أو القواعد المحددة التي يجب استيفاؤها، والتي عادةً ما تكون محددة بنقاط محددة (Harris & Martin, 2019)، ومن الضروري أن تكون سياسات الأمن السيبراني شاملة ومحدثة بانتظام لمواكبة التطورات السيبرانية الجديدة، ولذلك تقوم بعض المؤسسات بمراجعة السياسة بمجرد ملاحظة التغييرات الخارجية (قد يتم إدخال التغييرات من خلال الهيئات التنظيمية المحلية والدولية، أو حتى التغيير في التكنولوجيا). وتتفق مؤسسات أخرى على الوقت المسموح به لتشغيل السياسة قبل أن تخضع لمراجعة شاملة في حال التزام المؤسسة بإطار زمني محدد، فمن الضروري مواكبة وتيرة التغيرات التكنولوجية لضمان استمرارية الأعمال، وأن الحد الأقصى هو ثلاث سنوات، على أن تخضع سياسة الأمن السيبراني خلالها لمراجعة شاملة، ومن المسلّم به أن تحديات مثل نقص المعرفة بالسياسات ذات الصلة، والدعم الإداري، والتمويل، تعيق عملية المراجعة (Lubua & Pretorius, 2019).

وغالبًا ما تحتوي السياسات على بنود مصممة لحماية مصالح العملاء وضمان العمليات المصرفية الصادقة والمفتوحة (Alnor et AL., 2024)، وبمجرد أن تضع المؤسسة سياسات للأمن السيبراني، يُطلب من المستخدمين الالتزام بها، وعادةً ما يكون المستخدمون هم موظفو المؤسسة والعمال المتعاقدون معها، وغالبًا ما يتم إعلام المستخدمين بسياسات الأمن السيبراني للمؤسسة من خلال برنامج تعليمي وتدريبي وتوعوي أمني، قد تتضمن هذه البرامج تدريبات وجهاً لوجه، وتدريبات عبر الإنترنت، وملصقات توعية أمنية، وغيرها، والتي تُعقد وفقًا لجدول زمني دوري، وبمجرد وضع السياسات ووعي

المستخدمين بها، تحتاج المؤسسات إلى ضمان الامتثال(Harris & Martin, 2019).

ثالثا: الامتثال لمتطلبات الأمن السيبراني

يعرف الامتثال بأنه الالتزام بالمتطلبات الإلزامية التي تُحددها القوانين واللوائح، والقدرة على إثبات الالتزام بها، بالإضافة إلى المتطلبات الطوعية الناتجة عن الالتزامات التعاقدية والسياسات الداخلية، وتُثبت المؤسسة امتثالها لمتطلبات الأمن السيبراني المعمول بها من خلال وضع سياسات الأمن السيبراني ونشرها وتطبيقها، وللمساعدة في تنفيذ السياسات واسعة النطاق، غالبًا ما تُطوّر المؤسسات معايير وإرشادات وإجراءات مُصاحبة، ينص المعيار SP 800-12 من المعهد الوطني للمعايير والتكنولوجيا (NIST) على أن المعايير والإرشادات تُحدد التقنيات والمنهجيات، وأن الإجراءات تُفصّل خطوات إنجاز المهام، وإن معايير السياسات والإرشادات والإجراءات خاصة بالمؤسسة، ولكنها غالبًا ما تكون مُستنيرة بالمعايير والأطر المعترف بها خارجيًا(Harris & Martin, 2019). ويتطلب الامتثال التنظيمي أن تتخذ المؤسسات تدابير استباقية لحماية البيانات المالية والحفاظ على الشفافية في تقاريرها لضمان المساءلة المؤسسية، والحفاظ على ثقة أصحاب المصلحة، والامتثال للمتطلبات التنظيمية، ويجب على المؤسسات إعطاء الأولوية لدمج الحوكمة القوية والتقنيات المتقدمة وممارسات الأمن القوية، إذ سيكون التطور المستمر لهذه الممارسات أمرًا بالغ الأهمية للتنقل عبر تحديات العصر الرقمي وحماية مستقبل التقارير المالية (Jumble & Mirza, 2025).

2.2 دقة التقارير المالية

يتم الإفصاح عن التقارير المالية الدقيقة، التي تُظهر الوضع المالي للمؤسسة ونتائج التشغيل في نهاية الفترة وفقًا لمبادئ المحاسبة للتقارير المالية، ويتم استخدام المعلومات التي يتم إنتاجها من خلال التقارير المالية الدقيقة لأنها تحتوي على معلومات ذات سمات عالية الجودة، مثل المعلومات المالية (Kagiri, 2023). وتعتبر سلامة البيانات أمرًا بالغ الأهمية لموثوقية ودقة التقارير المالية في عالم رقمي متزايد، تضمن المؤسسات أن تكون البيانات المالية التي تفصح عنها كاملة ودقيقة وغير معدلة، وبدون تدابير سلامة البيانات القوية، تخاطر المؤسسات بتقديم بيانات مالية غير دقيقة، مما قد يؤدي إلى خسائر مالية كبيرة وغرامات تنظيمية وإلحاق الضرر بسمعتها. **وللحفاظ على دقة البيانات في التقارير المالية يكون بالآتي (Jumble & Mirza, 2025):**

1. ضمان الدقة والاتساق: إن ضمان دقة البيانات المالية وتناسقها طوال دورة حياتها أمر أساسي للحفاظ على سلامتها، ويتطلب هذا تنفيذ ضوابط داخلية قوية وعمليات آلية لتقليل احتمالية الخطأ البشري والتلاعب بالبيانات، حيث يساعد إعداد التقارير المالية الآلية باستخدام أنظمة برمجية متقدمة في القضاء على التناقضات وضمان تسجيل البيانات بشكل صحيح في كل مرحلة من مراحل عملية إعداد التقارير، وكذلك من خلال إنشاء ضوابط لضمان الأمن السيبراني تزيد المؤسسات بشكل كبير من دقة البيانات وتقليل مخاطر الأخطاء.
2. التحقق من صحة البيانات والتحقق منها: يعد التحقق من صحة البيانات من المكونات الرئيسة للحفاظ على دقة البيانات، وتحتاج المؤسسات إلى التحقق من صحة بياناتها المالية بانتظام من خلال الرجوع إلى المعلومات من مصادر مختلفة لتحديد التناقضات وتصحيحها. يمكن أن تساعد طرق التحقق من البيانات مثل عمليات المصادقة ومسارات التدقيق والفحوصات الآلية في ضمان اتساق البيانات ودقتها. وتسهم هذه الممارسات أيضًا في تسهيل الشفافية من خلال توفير مسار تدقيق واضح،

وهو أمر ضروري لإثبات الامتثال للوائح وتعزيز الثقة بين أصحاب المصلحة.

3. منع التلاعب بالبيانات والاحتيال: من بين التهديدات الكبيرة التي تهدد دقة البيانات في التقارير المالية الاحتيال المتعمد، وللحماية من هذه المخاطر يجب على الشركات تنفيذ ضوابط وصول صارمة، ومراقبة مستمرة للكشف عن التغييرات غير المصرح بها على البيانات المالية ومنعها، بالإضافة إلى ذلك يجب على المؤسسات إنشاء آليات تدقيق قوية توفر الشفافية وتسهل تحديد أي تناقضات أو علامات على النشاط الاحتيالي.

3.2 دور حوكمة الأمن السيبراني في تحسين دقة التقارير المالية

إن حجر الزاوية لمساعدة المديرين على اتخاذ قرارات عمل سليمة وتوجيه العمليات المناسبة بانتظام وتشغيل وإدارة المؤسسة بكفاءة، والحفاظ على رقابة داخلية ممتازة هو المعلومات المحاسبية الدقيقة(Halasa, 2024)، ويساعد استخدام أدوات البرمجيات المتقدمة في التحقق من صحة البيانات وتحديد الأخطاء وتصحيحها بكفاءة أكبر، مما يؤدي في النهاية إلى تحسين الدقة في إعداد هذه البيانات (Ghanem & Al-Shammari, 2024) ، وأن المؤسسات التي لديها ضوابط أمنية سيبرانية ضعيفة شهدت ارتفاعًا في حالات الاحتيال المالي والتلاعب بالبيانات والعقوبات التنظيمية(Emmanuel, 2025)، ولا ترغب العديد من المؤسسات في تقبّل المخاطر المرتبطة بعدم الامتثال، وتلجأ بدلاً من ذلك إلى إجراء تقييمات ذاتية متكررة لتحديد وضعها فيما يتعلق باللوائح التنظيمية(Harris & Martin, 2019)،

وتعد أطر الحوكمة القوية ضرورية للإشراف على تنفيذ استراتيجيات التحول الرقمي في التقارير المالية، وضمان توافقها مع أهداف المنظمة ومتطلبات الامتثال واستراتيجيات إدارة المخاطر، حيث تضمن الحوكمة الفعالة أن تتبنى المؤسسات أفضل ممارسات الأمن السيبراني ودمجها عبر جميع جوانب إدارة البيانات المالية، من عمليات إعداد التقارير إلى أنظمة تخزين البيانات ونقلها (Jumble & Mirza, 2025)، وأن المستثمرين ينظرون إلى المؤسسات ذات التقارير الدقيقة على أنها أقل خطورة، بالإضافة إلى ذلك تُمكن التقارير المالية الدقيقة من تعزيز كفاءة السوق، حيث يمكن للمستثمرين الاعتماد على المعلومات المبلغ عنها لاتخاذ خيارات استثمارية فعالة (Johri, 2024).

ثالثاً: الدراسة الميدانية

1.3 مجتمع الدراسة

يشمل مجتمع البحث العاملين بالمصارف التجارية الليبية العامة العاملة داخل النطاق الجغرافي لمدينة صبراتة، حيث اقتصرت الدراسة على عدد من فروع المصارف التجارية الموجودة داخل المدينة، والمتمثلة في مصرف الجمهورية، ومصرف الوحدة، ومصرف الصحارى، ومصرف شمال أفريقيا، والمصرف التجاري الوطني، حيث تم الاعتماد على أسلوب العينة القصدية متمثلة في أعضاء مجلس الإدارة ومديري إدارات تقنية المعلومات، والشؤون المالية، والمراجعة الداخلية، ونظراً لمحدودية عدد الموظفين المختصين في هذه المجالات داخل هذه المصارف، تم توزيع (35) استبيانه واسترجاع (35) استمارة واستبعاد(3) استمارات، وإخضاع (32) استمارة للتحليل الإحصائي من خلال الحزمة الإحصائية للعلوم الاجتماعية Spss.

2.3 أداة البحث:

لتحقيق أهداف البحث، استخدمت الاستبانة كأداة لجمع البيانات، والتي اشتملت على محورين: تضمن المحور الأول المتغير المستقل حوكمة الأمن السيبراني بإبعاده والمتمثلة في التزام مجلس الإدارة بالأمن السيبراني وتضمن (7) عبارات، والبعد الثاني السياسات المعتمدة للأمن السيبراني وتضمن (7) عبارات، والبعد الثالث الامتثال لمتطلبات الأمن

السيبراني وتضمن (7) عبارات، والمحور الثاني المتغير التابع دقة التقارير المالية وتضمن (7) عبارات.

3.3 الصدق الظاهري للاستبانة:

للتأكد من صدق مقياس البحث قامت الباحثة بعرض استمارة الاستبانة على مجموعة من المحكمين من ذوي الخبرة والاختصاص في الجامعات الليبية والعاملين بالمصارف التجارية الليبية، وذلك لإبداء رأيهم وتقديم مقترحاتهم حول استمارة الاستبانة، والاستفادة من خبراتهم في الحكم على المقاييس المستخدمة ومدى ملامتها للتطبيق في البحث، وبناء على الملاحظات القيمة الواردة من المحكمين تم إجراء التعديلات على استمارة الاستبانة بشكلها النهائي.

1. صدق المقياس (الاتساق الداخلي):

يقصد بصدق المقياس (الاتساق الداخلي) مدى اتساق كل فقرة من فقرات الاستبانة مع المجال الذي تنتمي إليه هذه الفقرة وقد تم حساب الاتساق الداخلي للاستبانة، وذلك من خلال حساب معاملات الارتباط (معامل ارتباط سيبرمان) بين كل فقرة من فقرات مجالات الاستبانة والدرجة الكلية للمجال نفسه.

أولا: صدق المقياس للمتغير المستقل: حوكمة الأمن السيبراني.

ا–بعد التزام مجلس الإدارة بالأمن السيبراني .

يوضح الجدول (1) معامل الارتباط بين كل فقرة من فقرات البعد الأول والدرجة الكلية له، والذي يبين أن معاملات الارتباط المبينة بالجدول دالة إحصائية أقل من مستوى معنوية0.05 وبذلك يعتبر البعد صادق لما وضع لقياسه.

جدول (1) معامل الارتباط بين كل فقرة من فقرات البعد الأول والدرجة الكلية

ت	العبارات	معامل الارتباط	مستوى الدلالة
1	يحرص مجلس الإدارة على وضع سياسات واضحة للأمن السيبراني.	0.675	0.000
2	يُشرف مجلس الإدارة على تنفيذ ضوابط الأمن السيبراني بانتظام.	0.845	0.000
3	يهتم مجلس الإدارة بتخصيص ميزانية للأمن السيبراني.	0.731	0.001
4	يحرص مجلس الإدارة على مراجعة تقارير الأمن السيبراني بشكل دوري.	0.678	0.000
5	يقوم مجلس الإدارة بتقييم المخاطر السيبرانية وتأثيرها على التقارير المالية.	0.564	0.000
6	يشارك مجلس الإدارة في تحديد مسؤوليات الأمن السيبراني.	0.693	0.000
7	يتم تدريب أعضاء مجلس الإدارة على قضايا الأمن السيبراني.	0.771	0.000

المصدر: إعداد الباحثة اعتماداً على مخرجات البرنامج الإحصائي spss.

ب–بعد السياسات المعتمدة للأمن السيبراني.

يوضح الجدول (2) معامل الارتباط بين كل فقرة من فقرات البعد الثاني والدرجة الكلية للبعد، والذي يبين أن معاملات الارتباط المبينة بالجدول دالة إحصائية عند مستوى دلالة أقل من مستوى معنوية0.05 وبذلك يعتبر البعد صادق لما وضع لقياسه.

جدول (2) معامل الارتباط بين كل فقرة من فقرات البعد الثاني والدرجة الكلية

ت	العبارات	معامل الارتباط	مستوى الدلالة
1	توجد سياسات مكتوبة وواضحة للأمن السيبراني في المصرف.	0.821	0.000
2	يتم تحديث السياسات السيبرانية باستمرار وفقًا للتطورات.	0.881	0.000
3	السياسات الحالية تغطي حماية البيانات المالية بالكامل.	0.730	0.001
4	يتم تطبيق السياسات بشكل موحد على جميع الأقسام.	0.669	0.000
5	تُبلغ السياسات لجميع الموظفين بوضوح تام.	0.708	0.000
6	تُسهم السياسات في الكشف عن محاولات التلاعب بالبيانات المالية.	0.634	0.001
7	تسهم السياسات في تعزيز الرقابة على إعداد التقارير المالية.	0.894	0.000

المصدر: إعداد الباحثة اعتماداً على مخرجات البرنامج الإحصائي spss.

ج–بعد الامتثال لمتطلبات الأمن السيبراني

يوضح الجدول (3) معامل الارتباط بين كل فقرة من فقرات البعد الثالث والدرجة الكلية للبعد، والذي يبين أن معاملات الارتباط المبينة بالجدول دالة إحصائية عند مستوى دلالة أقل من مستوى معنوية0.05 وبذلك يعتبر البعد صادق لما وضع لقياسه.

جدول (3) معامل الارتباط بين كل فقرة من فقرات البعد الثالث والدرجة الكلية

ت	العبارات	معامل الارتباط	مستوى الدلالة
1	يلتزم المصرف بالمعايير المحلية والدولية للأمن السيبراني.	0.832	0.000
2	يخضع المصرف لمراجعة دورية حول تطبيق متطلبات الأمن السيبراني.	0.637	0.000
3	يتم التعامل بجدية مع ملاحظات الجهات الرقابية حول الأمن السيبراني.	0.844	0.000
4	يوجد فريق مختص يتابع تنفيذ متطلبات الامتثال السيبراني.	0.709	0.000
5	الامتثال السيبراني جزء من استراتيجية المصرف.	0.884	0.000
6	يتم التبليغ عن الحوادث السيبرانية وفق سياسات معتمدة.	0.716	0.001
7	تُوثق كل خطوات الامتثال المؤثرة على التقارير المالية.	0.891	0.000

المصدر: إعداد الباحثة اعتماداً على مخرجات البرنامج الإحصائي spss.

أولا: صدق المقياس للمتغير التابع: دقة التقارير المالية

يوضـــح الجدول (4) معامل الارتباط بين كل فقرة من فقرات بعد المتغير التابع والدرجة الكلية للبعد، والذي يبين أن معاملات الارتباط المبينة بالجدول دالة إحصـــائية عند مستوى دلالة أقل من مستوى معنوية0.05 وبذلك يعتبر البعد صادق لما وضع لقياسه

جدول (4) معامل الارتباط بين كل فقرة من فقرات بعد المتغير التابع والدرجة الكلية

ت	العبارات	معامل الارتباط	مستوى الدلالة
1	تعكس التقارير المالية الواقع المالي الحقيقي للمصرف.	0.698	0.000
2	يتم إعداد التقارير المالية وفقًا للمعايير المحاسبية الدولية.	0.746	0.000
3	تُراجع التقارير المالية داخليًا قبل إصدارها.	0.773	0.000
4	تتسم التقارير المالية بالوضوح والدقة في العرض.	0.802	0.000
5	تُفصح التقارير المالية عن جميع المعلومات الجوهرية.	0.589	0.000
6	تُعد التقارير المالية في الوقت المناسب.	0.725	0.000
7	يتم مراجعة التقارير المالية من قبل جهة خارجية مستقلة.	0.588	0.000

المصـــدر: إعداد البـاحثـة اعتمـاداً على مخرجـات البرنامج الإحصائي spss.

4.3 ثبات أداة البحث:

-يقصـد بثبات أداة جمع البيانات دقتها واتسـاقها. بمعنى أن تعطي أداة جمع البيانات نفس النتائج إذا تم استخدامها أو إعادتها مرة أخرى تحت ظروف مماثلة، وتم اســتخدم معامل (ألفا كرونباخ)، لقياس درجة تناســق إجابات المستقصي منهم على كل الأسئلة الموجودة بالمقياس، وإلى المدى الذي يقيس فيه كل ســؤال نفس المفهوم، وتكون قيمة معامل كرونباخ ألفا ما بين(0،1)، ليبين مدى الارتباط بين إجابات مفردات عينة البحث ، فعندما تكون قيمة معامل كرونباخ ألفا صـــفراً فيدل ذلك على عدم وجود ارتباط مطلق ما بين إجابات مفردات عينة البحث، أما إذا كانت قيمة معامل كرونباخ ألفا واحد صـــحيح فهذا يدل على أن هناك ارتباط تام بين إجابات مفردات عينة البحث، ومن المعروف أن أصغر قيمة مقبولة لمعامل كرونباخ ألفا هي(0.6) وأفضـــل قيمة تتراوح بين(0.7 إلى 0.8) وكلما زادت قيمته عن(0.8) كان ذلك أفضـــل، والجدول التالي رقم (5) يبين معامل ثبات محاور البحث.

جدول رقم (5) نتائج اختبار ألفا كرونباخ لمحاور الدراسة

المتغيرات	المجموع	
	عدد العبارات	ألفا كرونباخ
بعد: التزام مجلس الإدارة بالأمن السيبراني	**7**	**0.805**
بعد: السياسات المعتمدة للأمن السيبراني	**7**	**0.795**
بعد: الامتثال لمتطلبات الأمن السيبراني	**7**	**0.804**
المتغير المستقل: حوكمة الأمن السيبراني.	**21**	**0.837**
المتغير التابع: دقة التقارير المالية	**7**	**0.902**
الثبات الكلي لمتغيرات البحث	28	0.894

المصدر: إعداد الباحثة اعتماداً على مخرجات البرنامج الإحصائي spss.

يتضح من الجدول رقم (5) أن معامل ثبات محاور البحث (معامل ألفا كرونباخ) كانت (0.837) للمتغير المستقل (حوكمة الأمن السيبراني)، و(0.902) للمتغير التابع دقة التقارير المالية، وكان الثبات الكلي لمتغيرات البحث (0.894) وهي نسبة ثبات جيد جدا. وبذلك يكون قد تأكد من صدق وثبات مقياس البحث مما يجعله على ثقة بصحة المقياس وصلاحيته لتحليل النتائج والإجابة على فرضية البحث.

5.3 وصف متغيرات البحث

توصف متغيرات البحث في هذا الجزء بمقاييس النزعة المركزية ممثلة بالوسط الحسابي، ومقاييس التشتت المطلق ممثلة بالانحراف المعياري، كما يأتي:

اولاً: وصف المتغير المستقل: حوكمة الأمن السيبراني.

أ- بعد التزام مجلس الإدارة بالأمن السيبراني.

تم قياس بعد **التزام مجلس الإدارة بالأمن السيبراني** بسبع عبارات والجدول التالي يبين فقرات قياس هذا المتغير والوسط الحسابي والانحراف المعياري ومستوى اتجاه أفراد العينة.

الجدول (6) الوسط الحسابي والانحراف المعياري لفقرات بعد: التزام مجلس الإدارة بالأمن السيبراني

الفقرات	الوسط الحسابي	الانحراف المعياري	الأهمية النسبية	اتجاه أفراد العينة
يحرص مجلس الإدارة على وضع سياسات واضحة للأمن السيبراني.	**2.90**	**1.043**	4	إيجابي
يُشرف مجلس الإدارة على تنفيذ ضوابط الأمن السيبراني بانتظام.	**3.03**	**1.009**	3	إيجابي
يهتم مجلس الإدارة بتخصيص ميزانية للأمن السيبراني.	**2.85**	**1.037**	5	إيجابي
يحرص مجلس الإدارة على مراجعة تقارير الأمن السيبراني بشكل دوري.	**3.11**	**1.104**	2	إيجابي
يقوم مجلس الإدارة بتقييم المخاطر السيبرانية وتأثيرها على التقارير المالية.	**2.78**	**1.005**	7	إيجابي
يشارك مجلس الإدارة في تحديد مسؤوليات الأمن السيبراني.	**3.19**	**1.102**	1	إيجابي
يتم تدريب أعضاء مجلس الإدارة على قضايا الأمن السيبراني.	**2,84**	**1.006**	6	إيجابي
الالتزام مجلس الإدارة بالأمن السيبراني	**2.69**	**1.210**		إيجابي

المصدر: إعداد الباحثة بالاعتماد على نتائج برنامج spss

يتضح من الجدول رقم (6) أن الفقرة التي تنص على مشاركة مجلس الإدارة في تحديد مسؤوليات الأمن السيبراني حصلت على المرتبة الأولى بمتوسط حسابي (**3.19**) وانحراف معياري (**1.102**)، مما يدل على أن مشاركة مجلس الإدارة في تحديد مسؤوليات الأمن السيبراني. في حين حصلت الفقرة التي تنص على قيام مجلس الإدارة بتقييم المخاطر السيبرانية وتأثيرها على التقارير المالية حصلت على المرتبة الأخيرة من بين جميع فقرات هذا المتغير، بمتوسط حسابي (2.78) وانحراف معياري (**1.005**)، وبمقارنة المتوسطات الحسابية لجميع فقرات متغير **التزام مجلس الإدارة بالأمن السيبراني** بالوسط النظري المعتمد في البحث نلاحظ أن اتجاهات أفراد عينة البحث حول المتغير كانت إيجابية، وأخيراً بلغ المتوسط الحسابي الكلي لمتغير **التزام مجلس الإدارة بالأمن السيبراني** (**2.69**) وبانحراف معياري (**1.210**)، مما يؤكد أن اتجاهات أفراد العينة حول بعد **التزام مجلس الإدارة بالأمن السيبراني** كانت إيجابية .

ب- بعد السياسات المعتمدة للأمن السيبراني.

تم قياس بعد **السياسات المعتمدة للأمن السيبراني** بسبع عبارات والجدول التالي يبين فقرات قياس هذا المتغير والوسط الحسابي والانحراف المعياري ومستوى اتجاه أفراد العينة.

الجدول (7) الوسط الحسابي والانحراف المعياري لفقرات بعد: السياسات المعتمدة للأمن السيبراني

الفقرات	الوسط الحسابي	الانحراف المعياري	الأهمية النسبية	اتجاه أفراد العينة
توجد سياسات مكتوبة وواضحة للأمن السيبراني في المصرف.	**2.53**	**1.005**	7	إيجابي
يتم تحديث السياسات السيبرانية باستمرار وفقًا للتطورات.	**2.89**	**1.118**	2	إيجابي
السياسات الحالية تغطي حماية البيانات المالية بالكامل.	**2.75**	**1.033**	4	إيجابي
يتم تطبيق السياسات بشكل موحد على جميع الأقسام.	**2.69**	**1.038**	5	إيجابي
تُبلغ السياسات لجميع الموظفين وتُوضح بوضوح.	**2.77**	**1.109**	3	إيجابي
تُسهم السياسات في الكشف عن محاولات التلاعب بالبيانات المالية.	**2.63**	**1.007**	6	إيجابي
تسهم السياسات في تعزيز الرقابة على إعداد التقارير المالية.	**2.90**	**1.031**	1	إيجابي
السياسات المعتمدة للأمن السيبراني	**2.69**	**1.102**		إيجابي

المصدر: إعداد الباحثة بالاعتماد على نتائج برنامج spss

يتضح من الجدول رقم (7) أن الفقرة التي تنص على تسهم السياسات في تعزيز الرقابة على إعداد التقارير المالية. حصلت على المرتبة الأولى بمتوسط حسابي (**2.90**) وانحراف معياري (**1.031**)، مما يدل على أن السياسات تسهم في تعزيز الرقابة على إعداد التقارير المالية. في حين حصلت الفقرة التي تنص على في رأيك، توجد سياسات مكتوبة وواضحة للأمن السيبراني في المصرف. المرتبة الأخيرة. من بين جميع فقرات هذا المتغير، بمتوسط حسابي (2.53) وانحراف معياري (1.005)، وبمقارنة المتوسطات الحسابية لجميع فقرات متغير **السياسات المعتمدة للأمن السيبراني** بالوسط النظري المعتمد في البحث نلاحظ أن اتجاهات أفراد عينة البحث

حول المتغير **السياسات المعتمدة للأمن السيبراني** كانت إيجابية، وأخيراً بلغ المتوسط الحسابي الكلي لمتغير **السياسات المعتمدة للأمن السيبراني (2.69)** وبانحراف معياري **(1.102)**، مما يؤكد أن اتجاهات أفراد العينة حول بعد **السياسات المعتمدة للأمن السيبراني** كانت إيجابية.

ج- بعد الامتثال لمتطلبات الأمن السيبراني.

تم قياس بعد **الامتثال لمتطلبات الأمن السيبراني بسبع** عبارات والجدول التالي يبين فقرات قياس هذا البعد والوسط الحسابي والانحراف المعياري ومستوى اتجاه أفراد العينة.

الجدول (8) الوسط الحسابي والانحراف المعياري لفقرات متغير: الامتثال لمتطلبات الأمن السيبراني.

الفقرات	الوسط الحسابي	الانحراف المعياري	الأهمية النسبية	اتجاه أفراد العينة
يلتزم المصرف بالمعايير المحلية والدولية للأمن السيبراني.	**3.19**	**1.032**	1	إيجابي
يخضع المصرف لمراجعة دورية حول تطبيق متطلبات الأمن السيبراني.	**2.94**	**1.011**	4	إيجابي
يتم التعامل بجدية مع ملاحظات الجهات الرقابية حول الأمن السيبراني.	**3.04**	**1.103**	3	إيجابي
يوجد فريق مختص يتابع تنفيذ متطلبات الامتثال السيبراني.	**2.83**	**1.006**	6	إيجابي
الامتثال السيبراني جزء من استراتيجية المصرف.	**3.11**	**1.017**	2	إيجابي
يتم التبليغ عن الحوادث السيبرانية وفق سياسات معتمدة.	**2.76**	**1.044**	7	إيجابي
تُوثق كل خطوات الامتثال المؤثرة على التقارير المالية.	**2.91**	**1.015**	5	إيجابي
-بعد الامتثال لمتطلبات الأمن السيبراني.	**2.80**	**1.100**		إيجابي

المصدر: إعداد الباحثة بالاعتماد على نتائج برنامج spss

يتضح من الجدول رقم (8) أن الفقرة التي تنص على يلتزم المصرف بالمعايير المحلية والدولية للأمن السيبراني حصلت على المرتبة الأولى بمتوسط حسابي **(3.19)** وانحراف معياري **(1.032)**، مما يدل على أن يلتزم المصرف في رأيك بالمعايير المحلية والدولية للأمن السيبراني من بين جميع فقرات هذا البعد، في حين حصلت الفقرة التي تنص على يتم التبليغ عن الحوادث السيبرانية وفق سياسات معتمدة. على المرتبة الأخيرة، بمتوسط حسابي (2.76) وانحراف معياري **(1.044)**، وبمقارنة المتوسطات الحسابية لجميع فقرات متغير **الامتثال لمتطلبات الأمن السيبراني** بالوسط النظري المعتمد في البحث نلاحظ أن اتجاهات أفراد عينة البحث حول المتغير **الامتثال لمتطلبات الأمن السيبراني** كانت إيجابية، وأخيراً بلغ المتوسط الحسابي الكلي لمتغير **الامتثال لمتطلبات الأمن السيبراني (2.80)** وبانحراف معياري **(1.100)**، مما يؤكد أن اتجاهات أفراد العينة حول بعد **الامتثال لمتطلبات الأمن السيبراني** كانت إيجابية.

ثانياً: وصف المتغير التابع: دقة التقارير المالية.

تم قياس المتغير التابع **دقة التقارير المالية بسبع** عبارات والجدول التالي يبين فقرات قياس هذا المتغير والوسط الحسابي والانحراف المعياري ومستوى اتجاه أفراد العينة.

الجدول (9) الوسط الحسابي والانحراف المعياري لفقرات متغير: دقة التقارير المالية

الفقرات	الوسط الحسابي	الانحراف المعياري	الأهمية النسبية	اتجاه أفراد العينة
تعكس التقارير المالية الواقع المالي الحقيقي للمصرف.	2.96	1.331	5	إيجابي
يتم إعداد التقارير المالية وفقًا للمعايير المحاسبية الدولية.	3.01	1.216	3	إيجابي
تُراجع التقارير المالية داخليًا قبل إصدارها.	2.81	1.099	7	إيجابي
تتسم التقارير المالية بالوضوح والدقة في العرض.	3.19	1.108	1	إيجابي
تُفصح التقارير المالية عن جميع المعلومات الجوهرية.	2.99	1.026	4	إيجابي
تُعد التقارير المالية في الوقت المناسب.	2.87	1.078	6	إيجابي
يتم مراجعة التقارير المالية من قبل جهة خارجية مستقلة.	3.11	1.133	2	إيجابي
دقة التقارير المالية	3.07	1.034		إيجابي

المصدر: إعداد الباحثة بالاعتماد على نتائج برنامج spss

يتضح من الجدول رقم (9) أن الفقرة التي تنص على تتسم التقارير المالية بالوضوح والدقة في العرض حصلت على المرتبة الأولى بمتوسط حسابي (3.19) وانحراف معياري (**1.108**)، مما يدل على أن تتسم التقارير المالية بالوضوح والدقة في العرض، في حين حصلت الفقرة التي تنص على تُراجع التقارير المالية داخليًا قبل إصدارها حصلت على المرتبة الأخيرة، من بين جميع فقرات هذا المتغير، بمتوسط حسابي (2.81) وانحراف معياري (1.009). وبمقارنة المتوسطات الحسابية لجميع فقرات متغير التابع التي تتعلق **دقة التقارير المالية بالوسط** النظري المعتمد في البحث نلاحظ أن اتجاهات أفراد عينة البحث حول المتغير كانت إيجابية، وأخيراً بلغ المتوسط الحسابي الكلي لمتغير **دقة التقارير المالية** (**3.07**) وبانحراف معياري (**1.034**)، مما يؤكد أن اتجاهات أفراد العينة حول **دقة التقارير المالية كانت** إيجابية.

3.6 اختبار فرضيات البحث.

-الفرضية الرئيسة للبحث.

- يوجد أثر ذو دلالة إحصائية وعلى مستوى الدلالة ≤ 0.05 بين حوكمة الأمن السيبراني بأبعادها وتعزيز دقة التقارير المالية في المصارف التجارية.

ولاختبار الفرضية فقد تم استخدام اختبار الانحدار واختبار F الناتج عنه، لمعرفة أن كان هناك فروق ذات دلالة بين متوسطات تقديرات أفراد عينة البحث للعلاقة بين حوكمة الأمن السيبراني وتعزيز دقة التقارير المالية في المصارف التجارية محل البحث، على مستوى الدلالة الإحصائية (0.05=) ويبين الجدول رقم (10) النتائج المتعلقة بتحليل هذه العلاقة.

الجدول رقم (**10**) نتائج اختبار الانحدار واختبار **F** الناتج عنه

Rالارتباط	الارتباط المصحح R^2	**F**	مستوى الدلالة	نتيجة الفرضية
0.834	0.695	131.883	0.000	قبول

المصدر: إعداد الباحثة بالاعتماد على نتائج برنامج spss

لقد جاءت قيمة اختبار (F) مساوياً إلى (131.883) بقيمة احتمالية (0.000) وهي أقل من القيمة المحددة (0.05) مما يشير إلى وجود علاقة ذات دلالة إحصائية بين حوكمة الأمن السيبراني وتعزيز دقة التقارير المالية في المصارف التجارية ي مجتمع البحث, وبالتالي نقبل الفرضية والتي تنص على وجود اثر ذو دلالة إحصائية بين حوكمة الأمن السيبراني وتعزيز دقة التقارير المالية في المصارف التجارية ويتضح من الجدول نفسه أن المتغير المستقل (حوكمة الأمن السيبراني) في هذا النموذج يفسر ما مقداره (70%) من التباين في المتغير التابع (دقة التقارير المالية) وهي قوة تفسيرية جيدة ، مما يدل على أن هناك أثراً للمتغير المستقل حوكمة الأمن السيبراني على المتغير التابع دقة التقارير المالية.

-الفرضية الفرعية الأولى.

- يوجد أثر ذو دلالة إحصائية وعلى مستوى الدلالة ≤ 0.05 بين التزام مجلس الإدارة بالأمن السيبراني وتعزيز دقة التقارير المالية في مجتمع البحث.

ولاختبار الفرضية فقد تم استخدام اختبار الانحدار واختبار F الناتج عنه، لمعرفة أن كان هناك فروق ذات دلالة بين متوسطات تقديرات أفراد عينة البحث للعلاقة بين التزام مجلس الإدارة بالأمن السيبراني وتعزيز دقة التقارير المالية محل البحث ، على مستوى الدلالة الإحصائية (0.05= α) ويبين الجدول رقم (11) النتائج المتعلقة بتحليل هذه العلاقة.

الجدول رقم (11)

نتائج اختبار الانحدار واختبار F الناتج عنه

R الارتباط	الارتباط المصحح R^2	F	مستوى الدلالة	نتيجة الفرضية
0.758	0.574	99.794	0.000	قبول

المصدر: إعداد الباحثة بالاعتماد على نتائج برنامج spss

لقد جاءت قيمة اختبار (F) مساوياً إلى (99.794) بقيمة احتمالية (0.000) وهي أقل من القيمة المحددة (0.05) مما يشير إلى وجود علاقة ذات دلالة إحصائية بين التزام مجلس الإدارة بالأمن السيبراني وتعزيز دقة التقارير المالية في مجتمع البحث, وبالتالي نقبل الفرضية والتي تنص على وجود اثر ذو دلالة إحصائية بين التزام مجلس الإدارة بالأمن السيبراني و تعزيز دقة التقارير المالية ويتضح من الجدول نفسه أن المتغير المستقل (التزام مجلس الإدارة بالأمن السيبراني) في هذا النموذج يفسر ما مقداره (57%) من التباين في المتغير التابع (تعزيز دقة التقارير المالية) وهي قوة تفسيرية جيدة ، مما يدل على أن هناك أثراً للمتغير المستقل التزام مجلس الإدارة بالأمن السيبراني على المتغير التابع تعزيز دقة التقارير المالية.

-الفرضية الفرعية الثانية.

- يوجد أثر ذو دلالة إحصائية وعلى مستوى الدلالة ≤ 0.05 بين وجود سياسات للأمن السيبراني وتعزيز دقة التقارير المالية في المصارف التجارية.

ولاختبار الفرضية فقد تم استخدام اختبار الانحدار واختبار F الناتج عنه، لمعرفة أن كان هناك فروق ذات دلالة بين متوسطات تقديرات أفراد عينة الدراسة للعلاقة وجود سياسات للأمن السيبراني وتعزيز دقة التقارير المالية في المصارف التجارية محل البحث، على مستوى الدلالة الإحصائية (0.05=) ويبين الجدول رقم (12) النتائج المتعلقة بتحليل هذه العلاقة.

الجدول رقم (12) نتائج اختبار الانحدار واختبار F الناتج عنه

R الارتباط	الارتباط المصحح R^2	F	مستوى الدلالة	نتيجة الفرضية
0.703	0.494	122.832	0.000	قبول

المصدر: إعداد الباحثة بالاعتماد على نتائج برنامج spss

لقد جاءت قيمة اختبار (F) مساوياً إلى (122.832) بقيمة احتمالية (0.000) وهي أقل من القيمة المحددة (0.05) مما يشير إلى وجود علاقة ذات دلالة إحصائية بين وجود سياسات للأمن السيبراني و تعزيز دقة التقارير المالية في المصارف التجارية في مجتمع البحث, وبالتالي نقبل الفرضية التي تنص على وجود اثر ذو دلالة إحصائية بين وجود سياسات للأمن السيبراني وتعزيز دقة التقارير المالية في المصارف التجارية ويتضح من الجدول نفسه أن المتغير المستقل (وجود سياسات للأمن السيبراني) في هذا النموذج يفسر ما مقداره (49%) من التباين في المتغير التابع (تعزيز دقة التقارير المالية) وهي قوة تفسيرية جيدة ، مما يدل على أن هناك أثراً للمتغير المستقل وجود سياسات للأمن السيبراني على المتغير التابع تعزيز دقة التقارير المالية.

-الفرضية الفرعية الثالثة.

-يوجد أثر ذو دلالة إحصائية وعلى مستوى الدلالة ≤ 0.05 بين بعد الامتثال لمتطلبات الأمن السيبراني وتعزيز دقة التقارير المالية في المصارف التجارية.

ولاختبار الفرضية فقد تم استخدام اختبار الانحدار واختبار F الناتج عنه، لمعرفة أن كان هناك فروق ذات دلالة بين متوسطات تقديرات أفراد عينة البحث للعلاقة بين الامتثال لمتطلبات الأمن السيبراني وتعزيز دقة التقارير المالية في المصارف التجارية محل البحث، على مستوى الدلالة الإحصائية (0.05=) ويبين الجدول رقم (13) النتائج المتعلقة بتحليل هذه العلاقة.

الجدول رقم (13) نتائج اختبار الانحدار واختبار F الناتج عنه

R الارتباط	الارتباط المصحح R^2	F	مستوى الدلالة	نتيجة الفرضية
0.770	0.592	95.362	0.000	قبول

المصدر: إعداد الباحثة بالاعتماد على نتائج برنامج spss

لقد جاءت قيمة اختبار (F) مساوياً إلى (95.362) بقيمة احتمالية (0.000) وهي أقل من القيمة المحددة (0.05) مما يشير إلى وجود علاقة ذات دلالة إحصائية بين الامتثال لمتطلبات الأمن السيبراني وتعزيز دقة التقارير المالية في المصارف التجارية في مجتمع البحث, وبالتالي نقبل الفرضية والتي تنص على وجود اثر ذو دلالة إحصائية بين الامتثال لمتطلبات الأمن السيبراني و تعزيز دقة التقارير المالية في المصارف التجارية ويتضح من الجدول نفسه أن المتغير المستقل (الامتثال لمتطلبات الأمن السيبراني) في هذا النموذج يفسر ما مقداره (59%) من التباين في المتغير التابع (تعزيز دقة التقارير المالية) وهي قوة تفسيرية جيدة ، مما يدل على أن هناك أثراً للمتغير المستقل الامتثال

لمتطلبات الأمن السيبراني على المتغير التابع تعزيز دقة التقارير المالية.

4. النتائج والتوصيات

1.4 النتائج:

بعد تحليل البيانات التي تم جمعها، توصل البحث إلى مجموعة من النتائج أهمها:

1-أنه يوجد أثر ذو دلالة إحصائية وعلى مستوى الدلالة ≤ 0.05 بين حوكمة الأمن السيبراني بأبعادها وتعزيز دقة التقارير المالية في المصارف التجارية محل البحث، مما يدل على أن تطبيق حوكمة الأمن السيبراني يسهم بشكل فعال في تحسين وتعزيز دقة التقارير المالية. (وهذه النتيجة تعتبر النتيجة الرئيسة للبحث).

2-من نتائج التحليل الإحصائي المتحصل عليها تبين أنه يوجد أثر ذو دلالة إحصائية وعلى مستوى الدلالة ≤ 0.05 بين بعد التزام مجلس الإدارة بالأمن السيبراني وتعزيز دقة التقارير المالية، مما يشير إلى أهمية دور الإدارة العليا في دعم تطبيق الحوكمة السيبرانية وتحسين جودة التقارير المالية.

3-من نتائج التحليل الإحصائي المتحصل عليها تبين أنه يوجد أثر ذو دلالة إحصائية وعلى مستوى الدلالة ≤ 0.05 بين وجود سياسات للأمن السيبراني وتعزيز دقة التقارير المالية، مما يؤكد أن وجود سياسات وإجراءات واضحة يسهم في تعزيز موثوقية ودقة المعلومات المالية.

4-من نتائج التحليل الإحصائي المتحصل عليها تبين أنه يوجد أثر ذو دلالة إحصائية وعلى مستوى الدلالة ≤ 0.05 بين بعد الامتثال لمتطلبات الأمن السيبراني وتعزيز دقة التقارير المالية، مما يدل على أن الالتزام بالمتطلبات والإجراءات السيبرانية يسهم في تحسين جودة التقارير المالية وتقليل الأخطاء والمخاطر المرتبطة بها.

2.4 التوصيات:

في ضوء النتائج التي تم التوصل إليها يوصي البحث بالآتي:

1-تعزيز حوكمة الأمن السيبراني بإنشاء هيئة/لجنة لها، وذلك لتأثيرها على دقة التقارير المالية.

2-تعزيز التزام مجلس الإدارة بالأمن السيبراني من خلال تحديد وتوثيق مسؤولياته في مراجعة سياسات الأمن السيبراني واعتماد الميزانيات وتتبّع تطبيقها وتفعيلها كعنصر مركزي في الحوكمة والشفافية المالية.

3-وضع وتنفيذ سياسات أمن سيبراني متكاملة وتوثيقها وفق أطر دولية مع تحديثها، تصنيفها حسب مخاطرها على البيانات المالية وتحديد إجراءات معالجة مخصصة لكل فئة.

4-تعزيز الامتثال والتنظيم الداخلي من خلال تعزيز الشفافية مع الجهات التنظيمية حول مستويات الامتثال والجهود التحسينية، بما يعزز الثقة ويدعم جودة التقارير.

5-توصي الباحثة بإجراء دراسات مماثلة على قطاعات أخرى غير القطاع المصرفي، مثل شركات التأمين والمؤسسات المالية الأخرى، وذلك للتعرف على دور الحوكمة السيبرانية في تحسين جودة التقارير المالية في مختلف القطاعات.

المراجع

أولا: المراجع باللغة العربية

- شقلوف، محمد فرج. (2024). الحوكمة وأثرها على الإفصاح المحاسبي وجودة التقارير المالية: دراسة تطبيقية على المصارف التجارية بمدينة طرابلس. *مجلة جامعة الزيتونة، العدد 49*، ص130-169.
- عبد الله، وفاء إمحمد. (2023). الأمن السيبراني في القطاع المالي مع الإشارة لواقع الأمن السيبراني في ليبيا. *مجلة الأستاذ خريف، 25*. ص111 -137.
- محمد، حسناء عطية (2023). المقدرة التقييمية للالتزام بضوابط حوكمة الأمن السيبراني وتأثيره على قرارات المستثمرين: دراسة تطبيقية على شركات الاتصالات السعودية (زين -STC)، *المجلة المصرية للدراسات التجارية. العدد 47*، ص1-54.
https://doi.org/10.21608/alat.2023.331416

- شـــوران، عمر (2025). الأمن الســـيبراني في ليبيا: تحديات تواجه المؤسسات الحكومية. *وكالة الأنبـــاء الـــليـــبـــيـــة، 17 يـــنـــايـــر/2025.* https://lana.gov.ly/post.php?lang=ar&id=324291 تم الاطلاع بتاريخ 2025/4/30.
- عبد الله، وليد (2024). الهجمات الســـيبرانية المتكررة تقلق المؤســـســـــات المالية في ليبيا، *Independent عربية، 9 أبريل 2024،* [independentarabiya.com/node/566346] (https://independentarabiya.com/node/566346/تاريخ الاطلاع في 2025/5/1.
- مصـــرف ليبيا المركزي. (2023). *دليل حوكمة تـكـنـولـوجـيـا الـمـعـلـومـات* (المنشـــور رقم 21/2023)، تاريخ الإصـــــدار 10 يوليو 2023.

ثانيا: المراجع باللغة الإنجليزية

- Alnor, N. H. A., Mohammed, O. A., Al-Matari, E. M., Ahmed, A., Benlaria, H., Elhefni, A. H. M., Kouki, F., & Elshaabany, M. M. (2024). The role of bank governance in managing the risks associated with banking institutions. *International Journal of Advanced and Applied Sciences*, 11(4), 194-206. http://www.science-gate.com/IJAAS.html
- Al-Mohaerb, M. (2025). The Impact of Cyber Governance Quality on Dividend Policy in Mitigating Cybersecurity Breaches. *Risks, 13,* 34. https://doi.org/10.3390/risks13020034
- Al-Rawashdeh, H., Rabie, A., Abdul-Munim Ali, O., Rabie, H., & Al-Sraheen, D. (2024). the impact of cyber governance on financial technology implementation: The mediating role of internal control effectiveness. *Kurdish Studies, 12*(1), 3556-3568. https://doi.org/10.58262/ks.v12i1.252
- Basiouny, M. M. M., Elnagar, S. M. A., & Ahmed, A. S. A. (2024). The Impact of Cybersecurity Risk Disclosure on the Quality of Financial Reporting and Market Value: Evidence from Egyptian Stock Market. *Educational Administration: Theory and Practice, 30*(5), 2504-2516. https://doi.org/10.53555/kuey.v30i5.3310
- Chundu, B., Masamhha, T., & Sifile, O. (2025). Cyber-security governance framework pillars for Zimbabwean local authorities. *Cogent Social Sciences, 11*(1), Article 2453094. https://doi.org/10.1080/23311886.2025.2453094
- Ghanem, M. B., & Al-Shammari, A. J. (2024). The impact of accounting information systems on ensuring the accuracy and reliability of financial. *ZAC Conference Series: Social Sciences and Humanities, 1* (1), 100–125. https://doi.org/10.70516/zaccsssh.v1i1.29
- Jumble, E., & Mirza, D. (2025). Cybersecurity and Data Integrity in Financial Reporting: The Role of Digital Transformation and Governance in Integrated Reporting and Corporate Accountability.

ResearchGate. https://doi.org/10.13140/RG.2.2.17035.81443

- Johri, Amar. 2024. Examining the Impact of International Financial Reporting Standards Adoption on Financial Reporting Quality of Multinational Companies. *International Journal of Financial Studies 12*: 96. https://doi.org/10.3390/ ijfs12040096
- **Harris**, **M**. **A**., **& Martin**, **R**. (**2019**). Promoting cyber security compliance. In *Cybersecurity frameworks* (Chapter 4). IGI Global. https://doi.org/10.4018/978-1-5225-7847-5.ch004
- Halasa, S. Y. B. (2024). *Factors affecting the accounting information system usage in Jordanian SMEs, and the role of experience as a moderating variable* [*Master's thesis*]. *Middle East University.*
- Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cyber security: an overview of cyber security governance. *Into Cybersecurity Law Rev*, DOI: 10.1365/s43439-021-00045-4.
- Kagiri, B. (2023). Internal audit report quality and financial statement accuracy of savings and credit cooperative societies in Kenya. *African Journal of Commercial Studies, 3*(1), 75-85. (http://ijcsacademia.com/index.php/journal/)
- Lisnawati, L. (2024). How financial performance is influenced by adaptation to financial technology and cyber governance. *Journal Akuntansi, Keuangan, Pajak dan Informasi (JAKPI), 4*(2), 90-98. https://journal.moestopo.ac.id/index.php/jakpi
- Lubua, E. W., & Pretorius, P. D. (2019). Cyber-security policy framework and procedural compliance in public organizations. In Proceedings of the International Conference on Industrial Engineering and Operations Management, Pilsner, *Czech Republic,* July 23-26, 2019. https://www.researchgate.net/publication/334971399