The North African Journal of Scientific Publishing (NAJSP)
مجلة شمال إفريقيا للنشر العلمي (NAJSP)
E-ISSN: 2959-4820
Volume 4, Issue 4, 2026
Page No: 123-143
Website: https://najsp.com/index.php/home/index
SJIFactor 2024: 5.49 معامل التأثير العربي (AIF) 2025: 0.69 ISI 2024: 0.696

The Impact of Investment in Cybersecurity Technology on the Reliability of Accounting Systems and the Effectiveness of Internal Control: A Field Study on Libyan Banks

Ekhwira Salih Abdelkader[1*], Iman Salih Abdelkader[2]
[1]Department of Accounting, Faculty of Economics, Omar Al-Mukhtar University, Libya.
[2]Department of Finance and Banking, Faculty of Economics, Omar Al-Mukhtar University, Libya.

أثر الاستثمار في تكنولوجيا الأمن السيبراني على فاعلية وموثوقية النظم المحاسبية والرقابة الداخلية: دراسة ميدانية على المصارف الليبية

إخويره صالح عبد القادر محمد[1*]، ايمان صالح عبد القادر محمد[2]
[1]قسم المحاسبة، كلية الاقتصاد، جامعة عمر المختار، ليبيا
[2]قسم التمويل والمصارف، كلية الاقتصاد، جامعة عمر المختار، ليبيا

*Corresponding author: Akhweerah.salih@omu.edu.ly

Received: August 16, 2026	Accepted: October 26, 2026	Published: November 11, 2026

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

Abstract:
This study aimed to measure the impact of investing in cybersecurity technology on the effectiveness of internal control and the reliability of accounting systems in Libyan commercial banks. The study is contextualized within the accelerating digital transformation and its accompanying cyber threats that affect the integrity and reliability of accounting information. The research adopted a descriptive-analytical approach, utilizing a questionnaire as a data collection tool from a sample of specialized professional personnel, which included financial department managers, heads of accounting departments, information technology managers, and internal auditors. The data were processed using SPSS software. The study concluded that there is a statistically significant positive impact of investing in cybersecurity technology on the effectiveness of internal control. This impact was also proven regarding the qualitative characteristics of information and the reliability of banking accounting systems; consequently, the main null hypothesis and its two sub-hypotheses were rejected. Furthermore, the results revealed a disparity in opinions concerning the adequacy of budgets allocated for cybersecurity infrastructure, a relative weakness in adopting cyber risk management strategies in accordance with international standards (ISO 27001, NIST, COBIT), and a skills gap among some human resources. Accordingly, the study recommended establishing a mandatory governance framework for cyber expenditure that links it to international standards and periodic risk assessments. It also recommended setting a minimum threshold for cybersecurity budgets as a fixed percentage of the total information technology budget, shifting towards continuous auditing based on intelligent analysis for early fraud detection, and implementing sustainable cyber training programs across all functional levels.

Keywords: Cybersecurity, Internal control, Accounting Systems Reliability.

الملخص:
هدفت هذه الدراسة إلى قياس أثر الاستثمار في تكنولوجيا الأمن السيبراني على فاعلية الرقابة الداخلية وموثوقية النظم المحاسبية في المصارف التجارية الليبية. وتأتي الدراسة في ظل تسارع التحول الرقمي وما يرافقه من تهديدات سيبرانية تمس سلامة المعلومات المحاسبية وموثوقيتها. واعتمدت الدراسة المنهج الوصفي التحليلي، واستخدمت الاستبانة أداةً لجمع البيانات من عينة من الكوادر المهنية المتخصصة، شملت مديري الإدارات المالية ورؤساء أقسام المحاسبة ومديري تقنية المعلومات والمراجعين الداخليين، وعولجت البيانات باستخدام برنامج.(SPSS) وتوصلت الدراسة إلى وجود أثر إيجابي ذي دلالة إحصائية للاستثمار في تكنولوجيا الأمن السيبراني على فاعلية الرقابة الداخلية، كما ثبت الأثر ايضا على خصائص المعلومات وموثوقية النظم المحاسبية المصرفية، وعليه رُفضت الفرضية الصفرية الرئيسة وفرضيتاها الفرعيتان. وكشفت النتائج كذلك عن تفاوت في الآراء حول كفاية الميزانيات المخصصة للبنية التحتية للأمن السيبراني، وعن ضعف نسبي في تبني استراتيجيات لإدارة المخاطر السيبرانية وفق المعايير الدولية(ISO 27001 ، NIST، COBIT)، إضافة إلى فجوة مهارية لدى بعض الكوادر البشرية، هذا وقد أوصت الدراسة بتأسيس إطار إلزامي لحوكمة الإنفاق السيبراني يربطه بالمعايير الدولية وتقييمات المخاطر الدورية، وتحديد حد أدنى لميزانيات الأمن السيبراني بنسبة ثابتة من إجمالي ميزانية تقنية المعلومات، وكذلك التحول نحو الرقابة المستمرة القائمة على التحليل الذكي للكشف المبكر عن الاحتيال، و إرساء برامج تدريب سيبراني مستدامة لكافة المستويات الوظيفية.

الكلمات المفتاحية: الأمن السيبراني، الرقابة الداخلية، موثوقية النظم المحاسبية.

المقدمة:

شهد القطاع المصرفي العالمي تحولاً جذرياً نحو الرقمنة الشاملة، فلم يعد الاعتماد على التكنولوجيا مجرد خيار للحصول على التميز، ولكنه بات خيار أساسي لاستمرار عمل هذا القطاع. ومع انتقال الأصول وكافة البيانات المالية من السجلات المادية إلى الشبكات الافتراضية، بدأ ظهور أنواع معقدة من التهديدات السيبرانية التي تتجاوز مخاطر السرقة المتعارف عليها لتستهدف سلامة وموثوقية المعلومات المحاسبية ذاتها. الأمر الذي أخذ يفرض على المصارف التجارية العاملة في البيئة الليبية، ضرورة الانتقال من الإنفاق الخجول والتقليدي إلى الاستثمار الاستراتيجي في تكنولوجيا الأمن السيبراني لضمان حماية قواعد البيانات المالية من التلاعب أو الاختراق. ووجب عليها النظر إلى هذه الخطوة ليس كمجرد تكلفة تقنية، بل كصمام أمان لتعزيز الموثوقية التي تعد من أهم الخصائص النوعية للمعلومات المحاسبية، والتي قد يتسبب إهمالها في فقدان القوائم المالية قيمتها في اتخاذ القرارات الاقتصادية الرشيدة. كما أن دمج تقنيات الحماية المتقدمة يساهم في تدعيم أنظمة الرقابة الداخلية، مما يقلص من فرص الاحتيال المالي الناتجة عن نقاط الضعف التقنية، الأمر الذي من شأنه تدعيم عمل المصارف الليبية وتسريع التحاقها بالركب العالمي التكنولوجي المالي في قطاع المصارف.

مشكلة البحث:

على الرغم من التطور المتسارع في التكنولوجيا المالية، إلا أن البيئة المصرفية الليبية لا تزال تواجه تحديات جسيمة في إنجاز متطلبات التحول الرقمي وتوحيد البيئة الإلكترونية، وإن كانت قد سعت إلى اللحاق بهذا الركب إلا أن وتيرة هذا الالتحاق جدا بطيئة وتقليدية . وبالنظر إلى ما أشار اليه تقرير ديوان المحاسبة الليبي الصادر في (2022) بوجود فجوات تقنية وقصور في تدريب الموظفين على استخدام المنظومات الحديثة، الأمر الذي أتاح الفرصة أمام التحايل والاختراق لبعض الحسابات المصرفية (ميلاد وابوشعفة،2025، ص.492). وهذه المشكلة تكمن في عدم الاهتمام بالاستثمار الكافي في تقنيات الأمن السيبراني الأمر الذي يؤدي إلى انخفاض جودة المعلومات المحاسبية وتراجع مستوى المصداقية في السجلات، مما يسبب ضعفاً في فاعلية الرقابة الداخلية وتعريض المؤسسات لأخطار اقتصادية. وبناءً على ذلك، تبرز الحاجة لدراسة مدى انعكاس هذا الاستثمار على الجوانب المحاسبية والرقابية، ويمكن صياغة مشكلة الدراسة في التساؤل الرئيس التالي:

- هل يوجد أثر ذو دلالة إحصائية إيجابية للاستثمار في تكنولوجيا الأمن السيبراني على فاعلية وموثوقية النظم المحاسبية والرقابة الداخلية؟

أهمية الدراسة:

تنبع هذه الاهمية للدراسة في المساهمة بإثراء الأدبيات المحاسبية المحلية حول دور الأمن السيبراني في حماية جودة التقارير المالية، والمحاولة لسد الفجوة البحثية في البيئة الليبية التي تفتقر للدراسات المعمقة في هذا الجانب. وقد أصبح لزوما تدارك هذه الفجوة في ظل التطور السريع للتكنولوجيا والاعتماد على التقنيات الرقمية وما يواجهها من مشكلات أمنية وتقنية، هذا وتسعى الدراسة للفت انتباه المصارف الليبية وجهات الاختصاص بشكل عام إلى أهمية تخصيص الموارد المالية والتقنية لتعزيز البنية التحتية السيبرانية، بما ينعكس إيجاباً على دقة الرقابة في المصارف الليبية محليا ودوليا، وثقة المودعين والمستثمرين.

أهداف الدراسة:

- تقييم واقع الاستثمار في تقنيات الأمن السيبراني في المصارف الليبية.
- قياس أثر الأدوات التقنية الحديثة (مثل التشفير والمصادقة البيومترية) في تفعيل إجراءات الرقابة الداخلية والحد من الاحتيال.

- بيان أثر الاستثمار في تكنولوجيا الأمن السيبراني على موثوقية النظم المحاسبية والرقابة الداخلية في المصارف.

فرضيات الدراسة:

استنادًا إلى مشكلة الدراسة تم صياغة فرضية رئيسية للدراسة على الوجه التالي:

- لا يوجد أثر ذو دلالة إحصائية للاستثمار في تكنولوجيا الأمن السيبراني على فاعلية وموثوقية النظم المحاسبية والرقابة الداخلية.

وقد تم اشتقاق فرضيتين فرعيتين من هذه الفرضية:

1. لا يوجد أثر ذو دلالة إحصائية للاستثمار في تكنولوجيا الأمن السيبراني على خصائص المعلومات وموثوقية النظم المحاسبية المصرفية.
2. لا يوجد أثر ذو دلالة إحصائية للاستثمار في تكنولوجيا الأمن السيبراني على فاعلية الرقابة الداخلية وزيادة تعزيزها.

منهج ومنهجية الدراسة:

اعتمدت الدراسة المنهج الوصفي التحليلي من خلال الرجوع للدراسات السابقة والاطلاع على أدبيات الموضوع، وتم تصميم استبانة كأداة للدراسة الميدانية لجمع البيانات موجهة لعينة الدراسة التي تم اختيارها. وقد تم معالجة البيانات باستخدام البرنامج الإحصائي SPSS.

مجتمع وعينة الدراسة:

يتمثل المجتمع في المصارف التجارية الليبية داخل مدينة البيضاء، مع اختيار عينة ممثلة من الكوادر المهنية المتخصصة. والمتمثلة في مديري الإدارات المالية، ورؤساء أقسام المحاسبة، ومديري تقنية المعلومات، والمراجعين الداخليين في المصارف التجارية الليبية.

الدراسات السابقة:

الدراسة	الهدف	المنهج والأسلوب المستخدم	النتيجة
علي (2026)	دور الحوكمة الرقمية في تعزيز النزاهة ومكافحة الفساد بالمؤسسات الحكومية.	مناهج تحليلية كمية نوعيًا، حيث شملت الدراسات السابقة العربية والأجنبية، بهدف دعم نتائج البحث وتوضيح أبعاده	الحوكمة الرقمية تساهم في تيسير الاطلاع على المعلومات والخدمات، وتعزيز ثقة المواطنين بالمؤسسات، وتحسين آليات الرقابة والتدقيق.
(تواتي وبوحفص، 2025)	تحليل أثر استخدام الأنظمة السحابية على العمليات المحاسبية في المصارف الإسلامية،	. واعتمدت الدراسة على المنهج الوصفي التحليلي، ومجموعة من الأساليب الإحصائية، من بينها اختبار (Shapiro–Wilk).	تطبيق الأنظمة السحابية يسهم بدرجة كبيرة في تحسين كفاءة العمليات المحاسبية، والحد من الأخطاء البشرية،
(علي.2025)	دور الذكاء الاصطناعي، من خلال الشبكات العصبية الاصطناعية والرؤية الحاسوبية، في تعزيز جودة المعلومات المحاسبية.	مزيج من المناهج البحثية مثل المنهج التاريخي، والوصفي والتحليلي، والاستقرائي، بهدف تقييم أثر التقنيات الحديثة على النظم المحاسبية التقليدية.	هناك علاقة طردية ذات دلالة إيجابية بين فاعلية تطبيقات تكنولوجيا الذكاء الاصطناعي وجودة المعلومات المحاسبية في البنك.
(ميلاد وأبو شعفة ،2025)	دور الإفصاح المحاسبي عن الأمن السيبراني في تحسين جودة المعلومات المحاسبية في المصارف التجارية الليبية العاملة في مدينة مسلاته وفروعها.	المنهج الوصفي التحليلي، الاستبانة لجمع البيانات من عينة مكوّنة من القيادات الإدارية بمستوياتها المختلفة بالمصارف محلّ الدراسة، وتحليل البيانات باستخدام برنامج (SPSS).	وتوصلت النتائج إلى وجود أثر ذي دلالة إحصائية للإفصاح عن حوكمة الأمن السيبراني والإفصاح عن الاستراتيجية الأمنية في تحسين جودة المعلومات المحاسبية.
(حداوي،2024)	دور قيادة التحول الرقمي واهتمام المصارف بتعزيز ثقافة وسلوك العاملين في مجال الأمن السيبراني.	بالتحليل الوصفي بالاعتماد على استبيان تم توزيعه على موظفي المصارف.	وجود علاقة ذات إثر إيجابي بين قيادة التحول الرقمي وبين السلوك الأمني السيبراني للموظفين.
Chahrazed) (2025،	استكشاف العلاقة بين أمن البيانات المالية وثقة المستثمرين في القطاع المصرفي.	اعتمدت المنهج الكمي، وتم استخدام استبانة وُزّعت على موظفي (10) مصارف تجارية.	وجود علاقة إيجابية ذات دلالة إحصائية بين قوة أمن البيانات المالية وارتفاع ثقة المستثمرين.
(Shafa & Islam 2025)	أثر خصوصية البيانات والأمن السيبراني في نظم المعلومات المحاسبية.	المنهج الكميومراجعة شملت (135) دراسة علمية محكّمة منشورة خلال الفترة من 2010 إلى 2024.	وجود أثر إيجابي لخصوصية البيانات والأمن السيبراني على الشفافية المالية.
(Morshed & Khrais 2025)،	دراسة تأثير ممارسات الأمن السيبراني، والمساءلة الأخلاقية، والإطار التنظيمي، والتقنيات الناشئة على اعتماد أنظمة المحاسبة الرقمية.	المنهج الكمي، حيث تم جمع عينة عشوائية وتم إجراء التحليل التجريبي باستخدام نمذجة المعادلات الهيكلية عبر طريقة المربعات الصغرى الجزئي.	أن تطبيق إجراءات قوية للأمن السيبراني، تسهل بشكل كبير اعتماد أنظمة المعلومات المحاسبية الرقمية وتعزيز الثقة فيه.
(Hossen & Ayedh، 2016)	تحديد المخاطر التي تهدد نظم المعلومات المحاسبية في مصرف ليبيا المركزي، والتعرّف على أسباب تلك المخاطر.	المنهج التطبيقي في تحليل مخاطر أمن المعلومات المرتبطة بنظم المعلومات المحاسبية، وتم تحليل البيانات باستخدام برنامج (SPSS)،	وأوضحت الدراسة أن هذا التطور المتسارع صاحَبَه ظهور مجموعة من المخاطر والمشكلات التي تمس أمن المعلومات المحاسبية.
(Al-Laith، 2012)	تحديد أهمية الرقابة الداخلية ومدى توافقها مع تطور استخدام تكنولوجيا المعلومات، وتأثير ذلك على موثوقية البيانات المالية للمصارف التجارية.	تم توزيع استبيانات على المديرين الماليين، والمراجعين الداخليين، وموظفي قسم الحاسوب العاملين في هذه المصارف.	وان توافق أنظمة الرقابة الداخلية مع تطور استخدام تكنولوجيا المعلومات في المصارف التجارية يؤدي الى الحصول على بيانات مالية موثوقة بدرجة عالية.

الإطار النظري للدراسة:

أولاً: الاستثمار في تكنولوجيا الأمن السيبراني:

يُقصد بالاستثمار في تكنولوجيا الأمن السيبراني ما تخصصه المصارف من موارد مالية وبشرية لاقتناء وتشغيل الأدوات والضوابط التقنية التي تحمي نظمها وبياناتها من الهجمات الرقمية. وقد شهدت السنوات الأخيرة زيادة واضحة في الميزانيات والاستثمارات الموجهة للأمن السيبراني، بوصفها انعكاساً مباشراً لتغير الاستراتيجيات المؤسسية وإدراك الحاجة إلى حماية الأصول الرقمية (Ferreira et al. 2025, p. 1). وتُبرر المؤسسات هذه الزيادة بتعاظم تعقيد التهديدات وتكرارها، وبضغوط الامتثال لتشريعات حماية البيانات.(Ferreira et al. 2025, p. 2)

ويعبّر مفهوم الأمن السيبراني في النظام المالي عن درجة الحماية والتأمين التي توفرها التقنيات والبرمجيات للعمليات المحاسبية والمالية، بما يصون خصوصيتها ويمنع اختراق البيانات والأجهزة والبرمجيات داخلياً وخارجياً (عثمان، 2023، كما ورد في يوسف وخلف، 2025، ص. 273). ويرتبط ذلك بقطاع المصارف ارتباطاً خاصاً؛ إذ يُعد القطاع المالي من أعلى القطاعات تكلفةً في حوادث اختراق البيانات وأكثرها عرضة للهجمات المعقدة.(Ferreira et al.) ،2025 ، p. 8).

ثانياً: خصائص المعلومات المحاسبية وموثوقية النظم المحاسبية المصرفية:

تستمد المعلومات المحاسبية فائدتها من خصائصها النوعية؛ إذ يحدد الإطار المفاهيمي لمجلس معايير المحاسبة الدولية (International Accounting Standards Board [IASB]، 2018، para. 2.5) ، وأربع خصائص معززة هي القابلية للمقارنة والقابلية للتحقق والتوقيت المناسب والقابلية للفهم (IASB، 2018). ولا تتحقق هذه الخصائص في البيئة المصرفية الإلكترونية ما لم تكن النظم التي تنتجها موثوقاً بها.

وفي هذا الإطار، حدد المعهد الأمريكي للمحاسبين القانونيين والمعهد الكندي للمحاسبين القانونيين خمسة مبادئ رئيسة لموثوقية النظم الإلكترونية، هي: الأمن، والسرية، والخصوصية، وسلامة المعالجات، والجاهزية (شوكت وطه، 2022، ص. 113). ويعني مبدأ الأمن حماية النظام من الوصول والاستخدام غير المشروع (شوكت وطه، 2022، ص. 113–114)، وتعني السرية حماية المعلومات المصنفة سرية في مراحل جمعها ومعالجتها وتخزينها، بينما تنصرف الخصوصية إلى حماية البيانات الشخصية للعملاء (شوكت وطه، 2022، ص. 114). أما سلامة المعالجات فتعني دقة عمليات معالجة البيانات واكتمالها وتوقيتها وشرعيتها (شوكت وطه، 2022، ص. 114–115)، وتعني الجاهزية قدرة المستخدم على استخدام النظام في الوقت المناسب لتنفيذ متطلبات العمل (شوكت وطه، 2022، ص. 115).

ويتضح من ذلك أن مبادئ الموثوقية أهداف للأمن السيبراني؛ وهي تأتي من توفير الحماية اللازمة بالضوابط الرقابية اللازمة. وقد توصلت دراسة حديثة على المصارف التجارية العراقية إلى وجود علاقة قوية وإيجابية بين جودة نظم المعلومات المحاسبية بأبعادها (الملاءمة والموثوقية والتوقيت والقابلية للمقارنة) والأمن السيبراني(Abu Kallal ، 2025).

وبناءً على ما سبق، يُتوقع أن يسهم الاستثمار في تكنولوجيا الأمن السيبراني في رفع موثوقية النظم المحاسبية المصرفية، وبالتالي تحسين خصائص المعلومات التي تنتجها، وهو ما يختبره الفرض الأول للدراسة.

ثالثاً: فاعلية الرقابة الداخلية في ظل الأمن السيبراني:

تُعرّف لجنة المنظمات الراعية (COSO) الرقابة الداخلية بأنها عملية ينفذها مجلس الإدارة والإدارة وسائر العاملين، وتُصمم لتوفير تأكيد معقول بشأن تحقيق الأهداف المتعلقة بالعمليات والتقارير والامتثال (Committee of Sponsoring Organizations of the Treadway Commission [COSO]، 2013، p. 3). وتزداد أهمية هذا التعريف في المصارف الرقمية، لأن جانباً كبيراً من الأنشطة الرقابية أصبح مدمجاً في النظم الإلكترونية ذاتها. ويؤكد يوسف وخلف أن فعالية مواجهة المخاطر السيبرانية لا تعتمد فقط على الأدوات التقنية، بل على وجود إجراءات رقابة داخلية فعّالة (يوسف وخلف، 2025، ص. 269). ومن الإجراءات الرقابية المقترحة لمواجهة هذه المخاطر: تحديد الأصول الحيوية الواجب حمايتها، ووضع سياسات أمن سيبراني تُحدّث دورياً، وتدريب الموظفين، وإجراء تدقيق أمني دوري، وتوظيف التقنيات الحديثة كالذكاء الاصطناعي وتحليل البيانات (منصور، 2021، كما ورد في يوسف وخلف، 2025، ص. 276).

وبهذا يمكن القول أن الاستثمار في تكنولوجيا الأمن السيبراني يرتبط نظرياً بمتغيري الدراسة عبر مسارين يمر الأول بمبادئ موثوقية النظم المحاسبية (الأمن والسرية والخصوصية وسلامة المعالجات والجاهزية) التي تحفظ للمعلومات ملاءمتها وتمثيلها الصادق، والثاني يمر بالضوابط الرقابية التقنية التي ترفع فاعلية نظام الرقابة الداخلية وقدرته على توفير تأكيد معقول. وتبرز الحاجة إلى اختبار هذين المسارين في المصارف الليبية، في ظل ما رصدته الدراسات المحلية من تحديات تواجه تطبيق الأمن السيبراني المحاسبي فيها(Eltaeb & Elsayih ،2025).

الدراسة الميدانية:

ولتحقيق أهداف الدراسة والإجابة عن تساؤلها تم الاعتماد على الاستبيان كأداةً لجمع البيانات الأولية من العاملين بالمصارف التجارية المستهدفة داخل مدينة البيضاء. وقد تكون الاستبيان من ثلاثة محاور رئيسية؛ يتناول المحور الأول الاستثمار في تكنولوجيا الأمن السيبراني في المصارف، ويركز المحور الثاني على أثر الأمن السيبراني على خصائص

المعلومات وموثوقية النظم المحاسبية المصرفية، أما المحور الثالث فيتناول دور الأمن السيبراني في تعزيز فاعلية الرقابة الداخلية.

أولا: اختبار ثبات أداة الدراسة باستخدام معامل ألفا كرونباخ:

للتأكد من مدى ثبات أداة الدراسة ودرجة الاتساق الداخلي بين فقرات الاستبيان، تم استخدام معامل ألفا كرونباخ (Cronbach's Alpha)، وقد تم حساب معامل ألفا كرونباخ لكل محور من محاور الاستبيان على حدة، بالإضافة إلى الاستبيان ككل، باستخدام برنامج الحزمة الإحصائية للعلوم الاجتماعية (SPSS)، وقد بلغ عدد الحالات الصالحة للتحليل الإحصائي (90)حالة من أصل (94) حالة، في حين استُبعدت أربع حالات (4.3%) لوجود بيانات مفقودة في متغير واحد أو أكثر من المتغيرات الداخلة في التحليل .ويوضح الجدول (1) نتائج معاملات الثبات لمحاور الاستبيان والاستبيان ككل.

الجدول رقم (1): يبين معاملات الثبات باستخدام معامل ألفا كرونباخ لمحاور الاستبيان والاستبيان ككل

م	المحور	عدد الفقرات	معامل ألفا كرونباخ	معامل الصدق
1	الاستثمار في تكنولوجيا الأمن السيبراني	12	0.803	0.896
2	أثر الأمن السيبراني على خصائص المعلومات وموثوقية النظم المحاسبية والمصرفية	13	0.843	0.918
3	دور الأمن السيبراني في تعزيز فاعلية الرقابة الداخلية	14	0.759	0.871
	الاستبيان ككل	39	0.900	0.949

يتضح من نتائج الجدول أن أداة الدراسة تتمتع بدرجة مرتفعة من الثبات والاتساق الداخلي، إذ بلغ معامل ألفا كرونباخ للاستبيان ككل (0.900)، وهي قيمة تعكس مستوى جيدًا من التجانس بين فقرات الاستبيان في قياس الأبعاد التي صُممت لتمثيلها.

وعلى مستوى محاور الاستبيان، أظهرت النتائج تفاوتًا نسبيًا في معاملات الثبات، مع تجاوزها جميعا للحد المقبول إحصائيًا، والمقدر عادةً بـ(0.70).

وبوجه عام، تؤكد النتائج أن معاملات الثبات للمحاور الثلاثة تتراوح بين (0.759)و(0.843)، في حين بلغ معامل الثبات الكلي (0.900)، وهو ما يوفر دليلًا إحصائيًا مناسبًا على الاتساق الداخلي لأداة الدراسة.

ثانيا: تحديد معيار تفسير المتوسطات الحسابية وفق مقياس ليكرت الخماسي:

جدول رقم (2): يبين قيم المتوسطات الحسابية والتقدير اللفظي والاتجاه وفق مقياس ليكرت الخماسي

قيم المتوسط الحسابي	التقدير اللفظي	الاتجاه أو المستوى	المتوسط الفرضي
1.00 – 1.80	غير موافق بشدة	منخفض جدًا / سلبي جدًا	3
1.81 – 2.60	غير موافق	منخفض / سلبي	
2.61 – 3.40	محايد	متوسط	
3.41 – 4.20	موافق	مرتفع / إيجابي	
4.21 – 5.00	موافق بشدة	مرتفع جدًا / إيجابي جدًا	

يتضح أن مقياس ليكرت الخماسي يتيح تصنيف المتوسطات الحسابية لفقرات الاستبانة، وقسم الاستبانة ومحاورها إلى خمسة مستويات متدرجة، وقد تم تحديد حدود هذه المستويات اعتمادًا على تقسيم المدى الكلي للمقياس، الذي يتراوح بين(1) و(5). إلى خمس فئات متساوية الطول، بما يوفر معيارًا موحدًا لتفسير المتوسطات الحسابية ومقارنة نتائج محاور الدراسة، وبهذا فإن المتوسطات التي تقع ضمن المستويات المرتفعة تشير إلى اتجاهات إيجابية لدى أفراد العينة نحو موضوع الدراسة.

جدول رقم (3): المتوسطات الحسابية والانحرافات المعيارية لمحاور الدراسة

م	المحور	المتوسط الحسابي	الانحراف المعياري	التقدير اللفظي
1	الاستثمار في تكنولوجيا الأمن السيبراني	3.9194	0.57984	موافق
2	أثر الأمن السيبراني على خصائص المعلومات وموثوقية النظم المحاسبية والمصرفية	4.1436	0.47477	موافق
3	دور الأمن السيبراني في تعزيز فاعلية الرقابة الداخلية	4.0976	0.42325	موافق

يتضح هنا أن المتوسطات الحسابية لمحاور الدراسة الثلاثة جاءت جميعها ضمن مستوى (موافق) وفقًا لمقياس ليكرت الخماسي المعتمد في الدراسة، مما يشير إلى اتجاه إيجابي لدى أفراد العينة نحو محاور الدراسة.

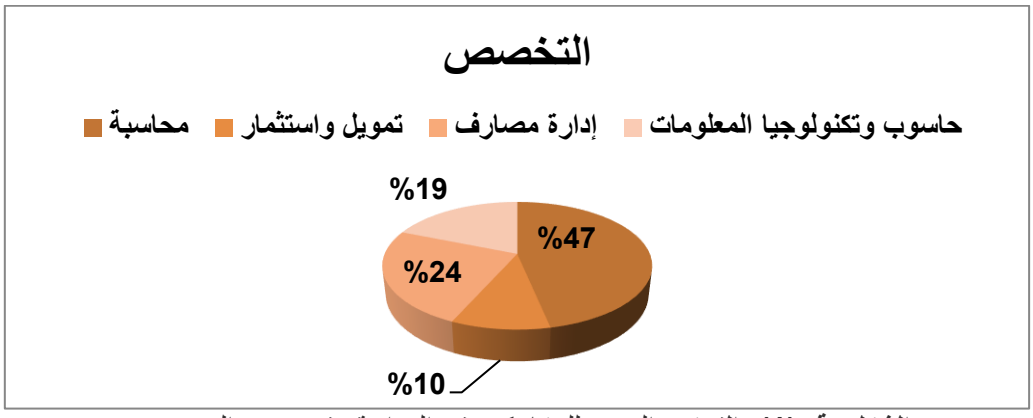
وتشير النتائج في الجدول السابق إلى أن أعلى متوسط حسابي كان للمحور الثاني، في حين كان أقل متوسط للمحور الأول، مع بقاء المحاور الثلاثة ضمن مستوى الموافقة .كما يُلاحظ أن الانحرافات المعيارية منخفضة نسبيًا، مما يشير إلى تقارب استجابات أفراد العينة حول المتوسطات الحسابية.

ثالثا: التحليل الوصفي للمتغيرات الأولية:

1. وصف عينة الدراسة وفق متغير التخصص:

جدول رقم (4): توزيع المشاركين في الدراسة وفق متغير التخصص

التخصص	التكرار	النسبة المئوية%
محاسبة	42	46.7%
تمويل واستثمار	9	10%
إدارة مصارف	22	24.4%
حاسوب وتكنولوجيا المعلومات	17	18.9%
المجموع	90	100%



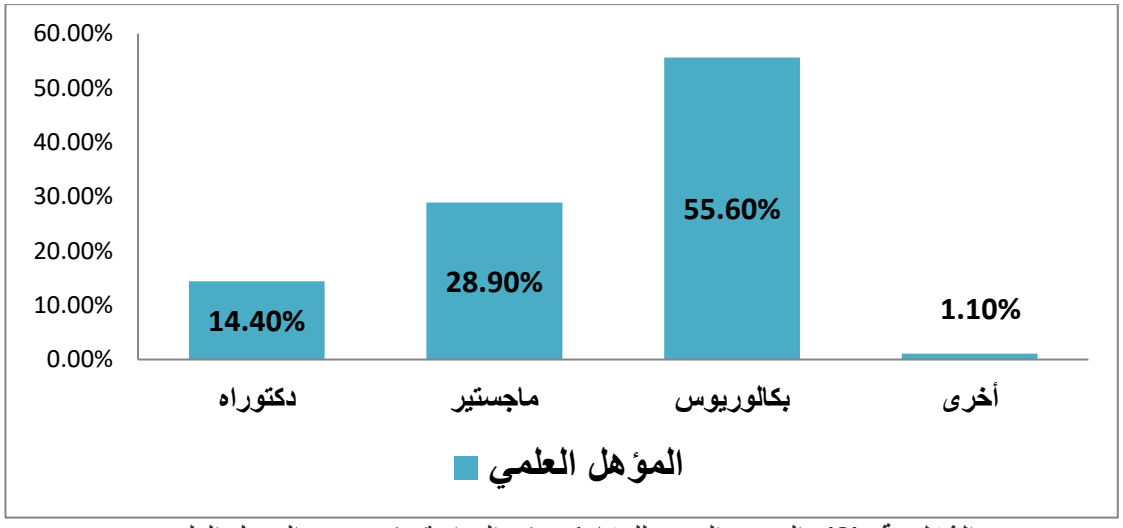
الشكل رقم (1): التوزيع النسبي للمشاركين في الدراسة وفق متغير التخصص.

يشير الجدول إلى تنوع توزيع المشاركين في الدراسة من حيث التخصصات العلمية، مع ارتفاع نسبة المشاركين من تخصص المحاسبة، يليه تخصص إدارة المصارف، وهما تخصصان يرتبطان بصورة مباشرة بالعمل المصرفي والنظم المحاسبية والرقابة الداخلية، بينما يسهم وجود مشاركين من تخصص الحاسوب وتكنولوجيا المعلومات في إثراء الدراسة بالخبرات المرتبطة بالجوانب التقنية للأمن السيبراني.

2. وصف عينة الدراسة وفق متغير المؤهل العلمي:

الجدول رقم (5): توزيع المشاركين في الدراسة وفق متغير المؤهل العلمي

المؤهل العلمي	التكرار	النسبة المئوية%
دكتوراه	13	14.4%
ماجستير	26	28.9%
بكالوريوس	50	55.6%
أخرى	1	%1.1
المجموع	90	100%



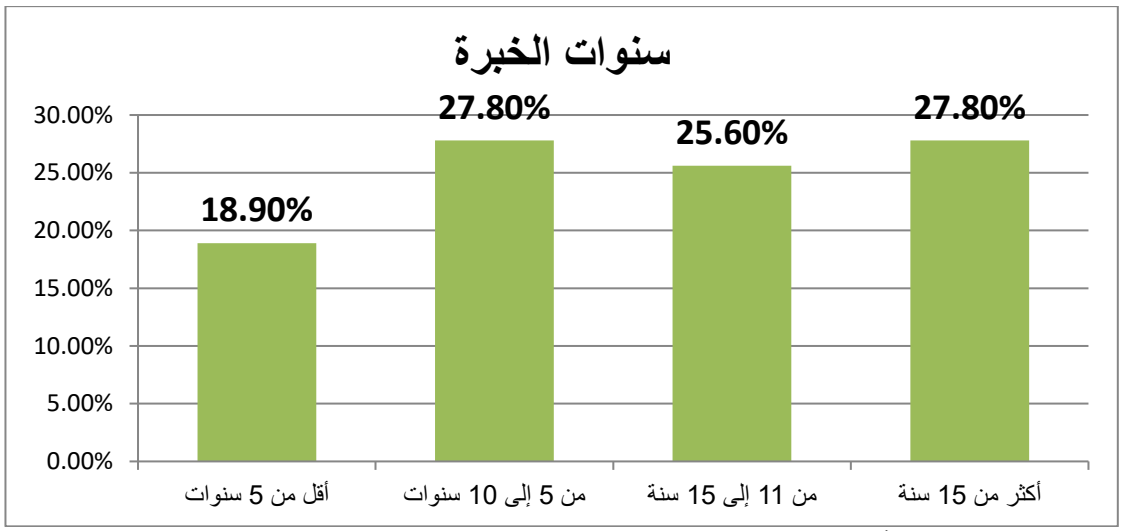
الشكل رقم (2): التوزيع النسبي للمشاركين في الدراسة وفق متغير المؤهل العلمي.

ويشير التوزيع في الجدول إلى أن غالبية المشاركين في الدراسة يحملون مؤهل البكالوريوس، مع وجود نسبة ملحوظة من الحاصلين على درجتي الماجستير والدكتوراه، مما يعكس تنوع المستويات العلمية والخلفية المناسبة للمشاركين.

3. **وصف عينة الدراسة وفق متغير سنوات الخبرة:**

الجدول رقم (6): توزيع المشاركين في الدراسة وفق متغير سنوات الخبرة.

سنوات الخبرة	التكرار	النسبة المئوية%
أقل من 5 سنوات	17	%18.9
من 5 إلى 10 سنوات	25	%27.8
من 11 إلى 15 سنة	23	%25.6
أكثر من 15 سنة	25	%27.8
المجموع	90	%100



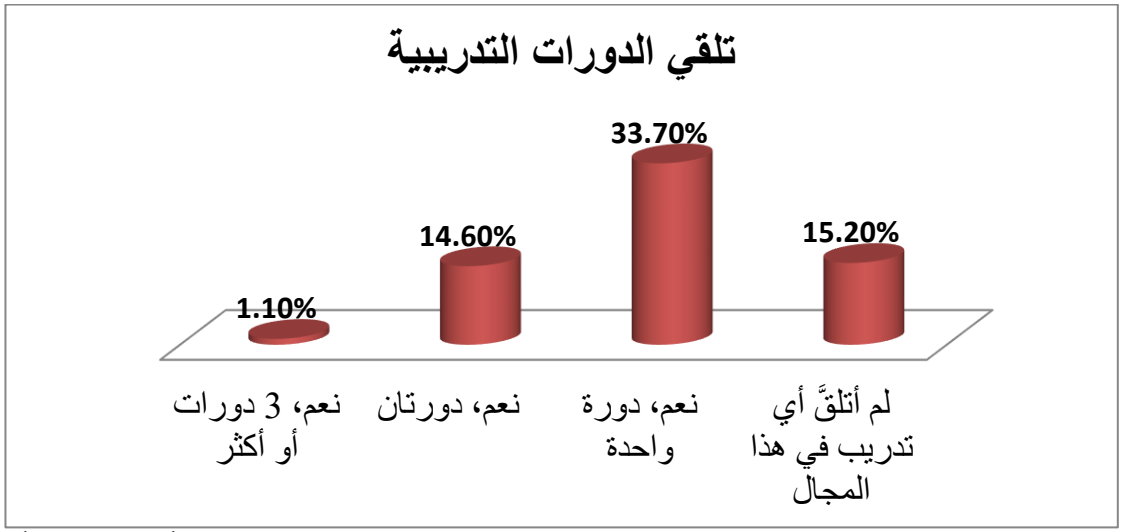
الشكل رقم (3): التوزيع النسبي للمشاركين في الدراسة وفق متغير سنوات الخبرة.

ويشير التوزيع في الجدول إلى أن عينة الدراسة تضم مشاركين بمستويات متنوعة من الخبرة العملية، مع تمثيل ملحوظ للفئات ذات الخبرة المتوسطة والطويلة، الأمر الذي يوفر خلفية مهنية متنوعة تساعد على فهم آراء المشاركين.

4. **وصف عينة الدراسة وفق متغير تلقي الدورات التدريبية المتخصصة:**

جدول رقم (7): توزيع المشاركين في الدراسة وفق تلقي دورات تدريبية متخصصة في الأمن السيبراني أو أمن المعلومات خلال السنوات الأربع الماضية.

تلقي الدورات التدريبية	التكرار	النسبة المئوية%
نعم، 3 دورات أو أكثر	33	%36.7
نعم، دورتان	37	%41.1
نعم، دورة واحدة	13	%14.4
لم أتلقَّ أي تدريب في هذا المجال	7	%7.8
المجموع	90	100%



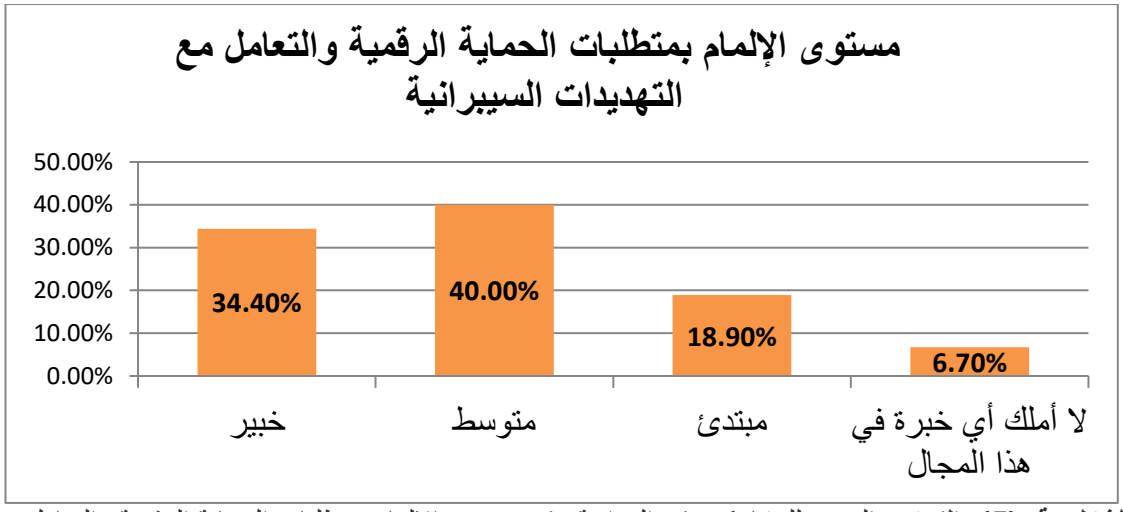
الشكل رقم (4): التوزيع النسبي للمشاركين في الدراسة وفق تلقي دورات تدريبية متخصصة في الأمن السيبراني أو أمن المعلومات خلال السنوات الأربع الماضية.

وهنا تشير النتائج إلى أن غالبية المشاركين في الدراسة سبق لهم تلقي دورات تدريبية متخصصة في الأمن السيبراني أو أمن المعلومات خلال السنوات الأربع الماضية، وهو ما يعكس وجود مستوى من الاهتمام بالتدريب والتأهيل في هذا المجال، مع استمرار الحاجة إلى تعزيز البرامج التدريبية لضمان تطوير مهارات العاملين ورفع مستوى استعدادهم للتعامل مع التهديدات السيبرانية في بيئة العمل المصرفي.

5. **وصف عينة الدراسة وفق متغير مستوى الإلمام بمتطلبات الحماية الرقمية:**

جدول رقم (8): توزيع المشاركين في الدراسة وفق مستوى الإلمام بمتطلبات الحماية الرقمية والتعامل مع التهديدات السيبرانية.

مستوى الإلمام بمتطلبات الحماية الرقمية والتعامل مع التهديدات السيبرانية	التكرار	النسبة المئوية%
خبير	31	%34.4
متوسط	36	%40.0
مبتدئ	17	%18.9
لا أملك أي خبرة في هذا المجال	6	%6.7
المجموع	90	%100



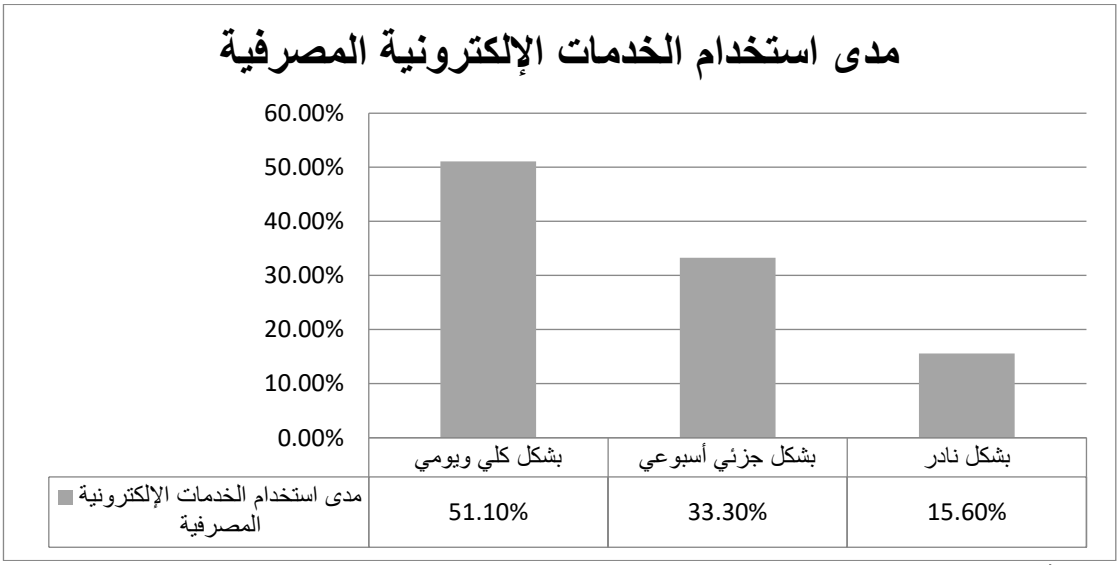
الشكل رقم (5): التوزيع النسبي للمشاركين في الدراسة وفق مستوى الإلمام بمتطلبات الحماية الرقمية والتعامل مع التهديدات السيبرانية.

تشير النتائج إلى أن معظم المشاركين لديهم مستوى من الإلمام بمتطلبات الحماية الرقمية والتعامل مع التهديدات السيبرانية، سواء كان متوسطًا أو متقدمًا، مما يوفر خلفية معرفية تساعدهم على إبداء آرائهم بشأن الاستثمار في تكنولوجيا الأمن السيبراني ودوره في دعم موثوقية النظم المحاسبية والمصرفية وتعزيز فاعلية الرقابة الداخلية .ومع ذلك، فإن وجود مشاركين بمستوى مبتدئ أو دون خبرة يؤكد أهمية استمرار التدريب والتوعية بالأمن السيبراني داخل المصارف التجارية الليبية.

6. وصف عينة الدراسة وفق متغير استخدام الخدمات الإلكترونية المصرفية:

جدول رقم (9): توزيع المشاركين في الدراسة وفق مدى استخدام الخدمات الإلكترونية المصرفية في العمل اليومي.

مدى استخدام الخدمات الإلكترونية المصرفية	التكرار	النسبة المئوية%
بشكل كلي ويومي	46	51.1%
بشكل جزئي أسبوعي	30	33.3%
بشكل نادر	14	15.6%
المجموع	90	100%



الشكل رقم (6): التوزيع النسبي للمشاركين في الدراسة وفق مدى استخدام الخدمات الإلكترونية المصرفية في العمل اليومي.

وتشير هذه النتائج إلى أن أكثر من نصف المشاركين في الدراسة وبنسبة 51.1 %من إجمالي العينة يستخدمون الخدمات الإلكترونية المصرفية بصورة يومية، و33،3% يستخدمونها بشكل جزئي الأمر الذي يعكس أهمية هذه الخدمات

في إنجاز الأعمال المصرفية .كما يبرز هذا الاستخدام أهمية الاستثمار في تكنولوجيا الأمن السيبراني لحماية المعاملات والبيانات المصرفية، والحد من المخاطر والتهديدات الإلكترونية، وتعزيز موثوقية النظم المصرفية وفاعلية الرقابة الداخلية.

رابعا: نتائج تحاليل البيانات الخاصة بمحاور الدراسة:

المحور الأول :الاستثمار في تكنولوجيا الأمن السيبراني:

يهدف هذا المحور إلى التعرّف على واقع الاستثمار في تكنولوجيا الأمن السيبراني في المصارف التجارية الليبية، ولتحقيق ذلك، تم تحليل استجابات المشاركين باستخدام التكرارات والنسب المئوية والمتوسطات الحسابية والانحرافات المعيارية، بهدف تحديد مستوى الموافقة على فقرات المحور والتعرّف على اتجاهات المشاركين نحو واقع الاستثمار في تكنولوجيا الأمن السيبراني.

جدول رقم (10): التوزيع التكراري والنسب المئوية لاستجابات المشاركين حول فقرات الاستثمار في تكنولوجيا الأمن السيبراني.

ر.م	العبارات	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة	المتوسط الحسابي	الانحراف المعياري
1	يحرص المصرف على تخصيص ميزانيات واستثمارات مالية استباقية كافية لتحديث وتطوير البنية التحتية للأمن السيبراني	35 (38.9%)	22 (24.4%)	10 (11.1%)	21 (23.3%)	2 (2.2%)	3.74	1.259
2	يحرص المصرف على تخصيص ميزانية كافية لتحديث برمجيات الحماية والجدران النارية بصفة دورية	16 (17.8%)	44 (48.9%)	19 (21.1%)	10 (11.1%)	1 (1.1%)	3.71	0.927
3	ينفذ المصرف برامج تدريبية ودورات توعوية سيبرانية دورية لجميع الموظفين للحد من مخاطر الهندسة الاجتماعية والأخطاء البشرية	27 (30.0%)	43 (47.8%)	14 (15.6%)	6 (6.7%)	0 (0.0%)	4.01	0.855
4	تستثمر المصارف في تقنيات التشفير المتقدمة لحماية البيانات المحاسبية أثناء التبادل الإلكتروني	35 (38.9%)	27 (30.0%)	13 (14.4%)	13 (14.4%)	2 (2.2%)	3.89	1.146
5	يعتمد المصرف على سياسات صارمة للوصول والمصادقة المتعددة (MFA) لتقييد الوصول إلى قواعد البيانات المالية.	23 (25.6%)	45 (50.0%)	15 (16.7%)	5 (5.6%)	2 (2.2%)	3.91	0.920
6	يتوفر لدى المصرف نظام النسخ الاحتياطي السحابي المحمي كجزء من استراتيجية الاستثمار التقني.	21 (23.3%)	38 (42.2%)	24 (26.7%)	7 (7.8%)	0 (0.0%)	3.81	0.886
7	يمتلك المصرف استراتيجية واضحة ومحدثة بانتظام لإدارة وتقييم المخاطر السيبرانية بالتوافق مع المعايير الدولية (مثلISO 27001، COBIT، NIST)	24 (26.7%)	34 (37.8%)	15 (16.7%)	17 (18.9%)	0 (0.0%)	3.72	1.060
8	تحرص الإدارة على الاستثمار في تدريب الكوادر المحاسبية على كيفية التعامل مع التهديدات السيبرانية	41 (45.6%)	24 (26.7%)	19 (21.1%)	6 (6.7%)	0 (0.0%)	4.11	0.965
9	تؤدي الاستثمارات الاستباقية في تكنولوجيا الأمن السيبراني إلى تقليل الخسائر والتكاليف المباشرة والخفية للحوادث والاختراقات السيبرانية بأسلوب ملموس.	44 (48.9%)	24 (26.7%)	13 (14.4%)	9 (10.0%)	0 (0.0%)	4.14	1.012
10	تساهم تقنيات الحماية الرقمية في تعزيز أمن المعلومات وإدارة العمليات الرقمية من جهة ونضج بيئة الرقابة الداخلية المصرفية من جهة أخرى	30 (33.3%)	36 (40.0%)	12 (13.3%)	10 (11.1%)	2 (2.2%)	3.91	1.056
11	يُحقق التكامل الهيكلي بين الاستثمار السيبراني والرقابة الداخلية والنظم المحاسبية حماية شاملة للبيانات المصرفية ويرفع ثقة المودعين والمستثمرين.	28 (31.1%)	48 (53.3%)	4 (4.4%)	10 (11.1%)	0 (0.0%)	4.04	0.898
12	يُساهم دمج الوظيفة المحاسبية ضمن أطر حوكمة المخاطر السيبرانية بالمصرف في استدامة الأعمال واستقرار الملاءة المالية للمؤسسة.	28 (31.1%)	45 (50.0%)	8 (8.9%)	9 (10.0%)	0 (0.0%)	4.02	0.899

يتضح من البيانات أعلاه أن استجابات المشاركين حول فقرات الاستثمار في تكنولوجيا الأمن السيبراني اتجهت بصفة عامة نحو الموافقة، إذ تراوحت المتوسطات الحسابية للفقرات بين (3.71–4.14)، وجميعها تقع ضمن مستوى مرتفع (إيجابي) وفقًا لمقياس ليكرت الخماسي المعتمد في الدراسة .ويشير ذلك إلى وجود اتجاه إيجابي لدى المشاركين نحو أهمية الاستثمار في تكنولوجيا الأمن السيبراني في المصارف التجارية، ودوره في دعم حماية البيانات وتعزيز كفاءة العمليات المصرفية والرقابة الداخلية. ولعل ما يزيد هذا التفسير قوة هو تصدر الفقرة (تؤدي الاستثمارات الاستباقية في تكنولوجيا الأمن السيبراني إلى تقليل الخسائر والتكاليف المباشرة والخفية للحوادث والاختراقات السيبرانية بأسلوب ملموس)، المرتبة الأولى بمتوسط حسابي بلغ (4.14)، وانحراف معياري (1.012)، حيث بلغت نسبة الموافقين بشدة (48.9%)، والموافقين (26.7%)، بإجمالي موافقة قدره (75.6%)، وتعكس هذه النتيجة إدراك المشاركين لأهمية الاستثمار الاستباقي في الأمن السيبراني في الحد من الخسائر والتكاليف المرتبطة بالحوادث والاختراقات السيبرانية.

ومجيئ الفقرة المتعلقة (باستثمار الإدارة في تدريب الكوادر المحاسبية على التعامل مع التهديدات السيبرانية)، في المرتبة الثانية بمتوسط حسابي بلغ (4،11)، وانحراف معياري (0.965)، وأظهرت النتائج أن (45.6%) من المشاركين موافقون بشدة، و(26.7%) موافقون، بإجمالي موافقة بلغ (72.3%)، وهذا يبرز الأهمية البالغة للعنصر البشري والتدريب المتخصص في تعزيز قدرة المصارف على التعامل مع المخاطر السيبرانية والحد من الأخطاء البشرية.

هذا وجاءت الفقرة المتعلقة (بالتكامل بين الاستثمار السيبراني والرقابة الداخلية والنظم المحاسبية)، بمتوسط حسابي بلغ (4.04)وانحراف معياري (0.898)، حيث بلغ إجمالي الموافق والموافق بشدة (84.4%)، وهي أعلى نسبة موافقة إجمالية بين جميع الفقرات. ويعكس ذلك اتفاقًا واسعًا بين المشاركين على أهمية التكامل بين الأنظمة التقنية والمحاسبية وإجراءات الرقابة الداخلية في حماية البيانات المصرفية وتعزيز الثقة لدى المودعين والمستثمرين.

كما أن الفقرة المتعلقة (بالاستثمار في تقنيات التشفير المتقدمة لحماية البيانات المحاسبية أثناء التبادل الإلكتروني)، فقد بلغ المتوسط الحسابي (3.89)والانحراف المعياري .(1.146)وبلغت نسبة الموافقة بشدة (38.9%)والموافقة (30.0%)، بإجمالي (68.9%)، الأمر الدال على وجود اتجاه إيجابي نحو أهمية التشفير في حماية البيانات المحاسبية، مع ملاحظة وجود نسبة من المشاركين لا توافق على مستوى تطبيق هذه التقنيات أو تظل محايدة بشأنه.

وبالنسبة إلى الفقرة المتعلقة بدور تقنيات الحماية الرقمية في تعزيز أمن المعلومات وإدارة العمليات الرقمية ونضج بيئة الرقابة الداخلية المصرفية، فقد بلغ المتوسط الحسابي (3.91)والانحراف المعياري (1.056)وبلغت نسبة الموافقة بشدة (33.3%)والموافقة (40.0%)، بإجمالي (73.3%)، وتدل هذه النتيجة على إدراك المشاركين لأهمية تقنيات الحماية الرقمية في دعم أمن المعلومات وتطوير بيئة الرقابة الداخلية.

وفيما يخص الفقرة السابعة، المتعلقة بامتلاك المصرف استراتيجية واضحة ومحدثة لإدارة وتقييم المخاطر السيبرانية وفقًا للمعايير الدولية، فقد بلغ المتوسط الحسابي (3.72) والانحراف المعياري (1.060)وبلغت نسبة الموافقة بشدة (26.7%)والموافقة (37.8%)، بإجمالي (64.5%)، وتكشف هذه النتيجة عن اتجاه إيجابي عام، إلا أن ارتفاع نسبة عدم الموافقة نسبيًا مقارنةً ببعض الفقرات الأخرى يشير إلى أهمية تعزيز وضوح استراتيجيات إدارة المخاطر السيبرانية وتحديثها بصورة منتظمة.

هذا ويتم ملاحظة أن الفقرة المتعلقة بتخصيص ميزانيات واستثمارات مالية استباقية كافية لتحديث وتطوير البنية التحتية للأمن السيبراني، فقد بلغ المتوسط الحسابي (3.74)والانحراف المعياري .(1.259)وبلغت نسبة الموافقة بشدة (38.9%)والموافقة (24.4%)، بإجمالي (63.3%)، بينما بلغت نسبة المحايدين (11.1%)، وغير الموافقين (23.3%)، وغير الموافقين بشدة .(2.2%)وعلى الرغم من وقوع متوسط الفقرة ضمن المستوى المرتفع، فإنها سجلت أعلى انحراف معياري بين الفقرات (1.259)، كما بلغت نسبة عدم الموافقة الإجمالية (25.5%)، الأمر الذي يعكس تفاوتًا ملحوظًا في آراء المشاركين بشأن كفاية الميزانيات المخصصة لتطوير البنية التحتية للأمن السيبراني.

واستكمالًا للتحليل الوصفي لفقرات المحور الأول، تم استخدام اختبار(T) لعينة واحدة للتحقق من الدلالة الإحصائية لاستجابات المشاركين، وذلك بمقارنة المتوسط الحسابي لكل فقرة بالقيمة المحكية المعتمدة في الدراسة، وهي(3) وفق مقياس ليكرت الخماسي، كما تم ترتيب الفقرات تنازليًا وفقًا لمتوسطاتها الحسابية، وتحديد اتجاه كل فقرة وفق مستويات التقدير اللفظي المعتمدة، ويهدف هذا التحليل إلى تحديد الجوانب التي حظيت بأعلى وأدنى مستويات الموافقة، بما يساعد على تقييم واقع الاستثمار في تكنولوجيا الأمن السيبراني في المصارف التجارية الليبية.

جدول رقم (11): نتائج اختبار(T) لعينة واحدة وترتيب فقرات الاستثمار في تكنولوجيا الأمن السيبراني حسب المتوسطات الحسابية.

ر.م	العبارات	المتوسط الحسابي	الانحراف المعياري	قيمة تي	قيمة الدالة	ترتيب الفقرات	اتجاه الفقرة
1	يحرص المصرف على تخصيص ميزانيات واستثمارات مالية استباقية كافية لتحديث وتطوير البنية التحتية للأمن السيبراني	3.74	1.259	5.609	0.000	10	مرتفع
2	يحرص المصرف على تخصيص ميزانية كافية لتحديث برمجيات الحماية والجدران النارية بصفة دورية	3.71	0.927	7.277	0.000	12	مرتفع
3	ينفذ المصرف برامج تدريبية ودورات توعوية سيبرانية دورية لجميع الموظفين للحد من مخاطر الهندسة الاجتماعية والأخطاء البشرية	4.01	0.855	11.225	0.000	5	مرتفع
4	تستثمر المصارف في تقنيات التشفير المتقدمة لحماية البيانات المحاسبية أثناء التبادل الإلكتروني	3.89	1.146	7.358	0.000	8	مرتفع
5	يعتمد المصرف على سياسات صارمة للوصول والمصادقة المتعددة (MFA) لتقييد الوصول إلى قواعد البيانات المالية.	3.91	0.920	9.398	0.000	6	مرتفع
6	يتوفر لدى المصرف نظام النسخ الاحتياطي السحابي المحمي كجزء من استراتيجية الاستثمار التقني.	3.81	0.886	8.690	0.000	9	مرتفع
7	يمتلك المصرف استراتيجية واضحة ومحدثة بانتظام لإدارة وتقييم المخاطر السيبرانية بالتوافق مع المعايير الدولية (مثلISO 27001)، COBIT، NIST	3.72	1.060	6.462	0.000	11	مرتفع
8	تحرص الإدارة على الاستثمار في تدريب الكوادر المحاسبية على كيفية التعامل مع التهديدات السيبرانية	4.11	0.965	10.923	0.000	2	مرتفع

9	تؤدي الاستثمارات الاستباقية في تكنولوجيا الأمن السيبراني إلى تقليل الخسائر والتكاليف المباشرة والخفية للحوادث والاختراقات السيبرانية بأسلوب ملموس.	4.14	1.012	10.730	0.000	1	مرتفع
10	تساهم تقنيات الحماية الرقمية في تعزيز أمن المعلومات وإدارة العمليات الرقمية من جهة ونضج بيئة الرقابة الداخلية المصرفية من جهة أخرى	3.91	1.056	8.183	0.000	7	مرتفع
11	يُحقق التكامل الهيكلي بين الاستثمار السيبراني والرقابة الداخلية والنظم المحاسبية حماية شاملة للبيانات المصرفية ويرفع ثقة المودعين والمستثمرين.	4.04	0.898	11.030	0.000	3	مرتفع
12	يُساهم دمج الوظيفة المحاسبية ضمن أطر حوكمة المخاطر السيبرانية بالمصرف في استدامة الأعمال واستقرار الملاءة المالية للمؤسسة.	4.02	0.899	10.785	0.000	4	مرتفع

يتضح من نتائج الجدول أن المتوسطات الحسابية لفقرات محور الاستثمار في تكنولوجيا الأمن السيبراني تراوحت بين (3.71–4.14)، وجاءت جميعها ضمن مستوى مرتفع وفقًا لمقياس ليكرت الخماسي المعتمد في الدراسة. كما أظهرت النتائج أن قيم اختبار(T). لجميع الفقرات موجبة، وتراوحت بين (5.609–11.225)، في حين ظهرت قيمة الدلالة الإحصائية في مخرجات البرنامج (0.000)لجميع الفقرات، وهو ما يُعرض علميًا على أنه (\p<0.001)\، وليس أن قيمة الاحتمال تساوي صفرًا. وبما أن هذه القيم أقل من مستوى الدلالة المعتمد (0.05)، فإن متوسطات الفقرات تختلف دالًّا إحصائيًا عن المتوسط الفرضي للمقياس، البالغ (3)، وذلك لصالح المتوسطات الأعلى منه.

وعلى مستوى ترتيب الفقرات، فانه سوف يتم تبيان أعلى الفقرات و أهمها، بدأ بالفقرة التاسعة، التي تنص على (تؤدي الاستثمارات الاستباقية في تكنولوجيا الأمن السيبراني إلى تقليل الخسائر والتكاليف المباشرة والخفية للحوادث والاختراقات السيبرانية بأسلوب ملموس)، التي جاءت في المرتبة الأولى بمتوسط حسابي بلغ (4.14)، وانحراف معياري (1.012)، وقيمة اختبار(T) بلغت (10.730)، ودلالة إحصائية أقل من(0.001)، ويشير ذلك إلى ارتفاع مستوى موافقة المشاركين على أهمية الاستثمار الاستباقي في الأمن السيبراني للحد من الخسائر والتكاليف الناجمة عن الحوادث والاختراقات السيبرانية. وتلتها الفقرة المتعلقة باستثمار الإدارة في تدريب الكوادر المحاسبية على كيفية التعامل مع التهديدات السيبرانية، في المرتبة الثانية، بمتوسط حسابي بلغ (4.11)، وانحراف معياري (0.965)، وقيمة (T)بلغت (10.923)، ودلالة إحصائية أقل من (0.001)وتعكس هذه النتيجة أهمية التدريب والتأهيل المستمر للكوادر المحاسبية في تعزيز قدرتها على التعامل مع التهديدات السيبرانية والحد من المخاطر المرتبطة بالعنصر البشري. ثم الفقرة المتعلقة بالتكامل بين الاستثمار السيبراني والرقابة الداخلية والنظم المحاسبية، فقد احتلت المرتبة الثالثة بمتوسط حسابي بلغ (4.04)، وانحراف معياري (0.898)، وقيمة (T)بلغت (11.030)، ودلالة إحصائية أقل من .(0.001)وتوضح هذه النتيجة ارتفاع مستوى موافقة المشاركين على أهمية التكامل بين الجوانب التقنية والمحاسبية والرقابية في حماية البيانات المصرفية وتعزيز الثقة لدى المودعين والمستثمرين.

هذا وتحصلت الفقرة المتعلقة بتخصيص ميزانيات واستثمارات مالية استباقية كافية لتحديث وتطوير البنية التحتية للأمن السيبراني، بمتوسط حسابي بلغ (3.74)، وانحراف معياري (1.259)، وقيمة (T)بلغت (5.609)، ودلالة إحصائية أقل من .(0.001)وعلى الرغم من وقوع متوسطها ضمن المستوى المرتفع، فإنها سجلت أعلى انحراف معياري بين الفقرات، بما يشير إلى تباين أكبر في استجابات المشاركين بشأن كفاية الميزانيات المخصصة لتطوير البنية التحتية للأمن السيبراني. هذا وجاءت بقية الفقرات متأخرة في المراتب مع احتفاظها بالمستوى المرتفع، وبذلك تشير النتائج إلى وجود اتجاه إيجابي عام لدى المشاركين نحو الاستثمار في تكنولوجيا الأمن السيبراني في المصارف التجارية الليبية.

المحور الثاني :أثر الأمن السيبراني على خصائص المعلومات وموثوقية النظم المحاسبية والمصرفية:

هدف هذا المحور إلى التعرّف على دور تكنولوجيا الأمن السيبراني في دعم خصائص المعلومات وتعزيز موثوقية النظم المحاسبية والمصرفية في المصارف التجارية الليبية، وتم تحليل استجابات المشاركين باستخدام التكرارات والنسب المئوية والمتوسطات الحسابية والانحرافات المعيارية، بهدف تحديد مستوى الموافقة على فقرات المحور والتعرّف على اتجاهات المشاركين بشأن هذا المحور.

جدول رقم (12): التوزيع التكراري والنسب المئوية لاستجابات المشاركين حول فقرات أثر الأمن السيبراني على خصائص المعلومات وموثوقية النظم المحاسبية والمصرفية

ر.م	العبارات	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة	المتوسط الحسابي	الانحراف المعياري
1	يساهم الاستثمار في الأمن السيبراني في ضمان عدم تعديل أو تحريف البيانات المحاسبية من قبل أطراف غير مصرح لها.	38 (42.2%)	42 (46.7%)	10 (11.1%)	0 (0.0%)	0 (0.0%)	4.31	0.664
2	تزداد ثقة الأطراف الخارجية (المودعين، المستثمرين) في المخرجات المحاسبية نتيجة قوة النظام السيبراني.	33 (36.7%)	51 (56.7%)	6 (6.7%)	0 (0.0%)	0 (0.0%)	4.30	0.589
3	تنعكس قوة الأمن السيبراني على دقة التقارير المالية وخلوها من الأخطاء الناتجة عن الاختراقات	37 (41.1%)	46 (51.1%)	7 (7.8%)	0 (0.0%)	0 (0.0%)	4.33	0.618

4	توفر تكنولوجيا الأمن السيبراني آليات متطورة للتحقق من هوية العملاء والموردين إلكترونياً، مما يمنع تسجيل عمليات مالية وهمية.	32 (35.6%)	54 (60.0%)	4 (4.4%)	0 (0.0%)	0 (0.0%)	4.31	0.554
5	يسمح الاستثمار السيبراني بربط الأنظمة الفرعية (الخزينة، الائتمان، المقاصة) بالنظام المحاسبي المركزي بشكل آمن، مما يقلل من أخطاء الإدخال اليدوي.	29 (32.2%)	50 (55.6%)	10 (11.1%)	1 (1.1%)	0 (0.0%)	4.19	0.669
6	يقلل الاستثمار في جدران الحماية القوية من مخاطر توقف النظام(Downtime) ، مما يضمن استخراج التقارير المالية في مواعيدها القانونية دون تأخير ناتج عن هجمات سيبرانية	22 (24.4%)	47 (52.2%)	17 (18.9%)	4 (4.4%)	0 (0.0%)	3.97	0.785
7	توفر تكنولوجيا الأمن السيبراني مسار مراجعة إلكتروني (Audit Trail)يسهل تتبع العمليات المالية.	29 (32.2%)	45 (50.0%)	10 (11.1%)	6 (6.7%)	0 (0.0%)	4.08	0.838
8	تضمن أنظمة الحماية استمرارية عمل نظم المعلومات المحاسبية دون توقف ناتج عن هجمات حجب الخدمة (DoS).	27 (30.0%)	42 (46.7%)	14 (15.6%)	7 (7.8%)	0 (0.0%)	3.99	0.880
9	تضمن تقنيات الأمن السيبراني عدم التلاعب بالبيانات المالية من جهات غير مخولة.	45 (50.0%)	32 (35.6%)	6 (6.7%)	7 (7.8%)	0 (0.0%)	4.28	0.900
10	تساهم أنظمة الحماية في توفير تقارير مالية دقيقة وخالية من التحريف الناتج عن الاختراق	27 (30.0%)	43 (47.8%)	13 (14.4%)	7 (7.8%)	0 (0.0%)	4.00	0.874
11	يقلل الاستثمار السيبراني من فترات توقف النظم المحاسبية نتيجة الهجمات الإلكترونية	43 (47.8%)	20 (22.2%)	20 (22.2%)	7 (7.8%)	0 (0.0%)	4.10	1.006
12	يتجاوز الاستثمار في تكنولوجيا الامن السيبراني كونه مجرد اقتناء للبرمجيات إلى كونه استراتيجية مؤسسية تعيد تشكيل البيئة التشغيلية للنظام المحاسبي الرقمي.	29 (32.2%)	43 (47.8%)	11 (12.2%)	7 (7.8%)	0 (0.0%)	4.04	0.873
13	إن الاستثمار في تكنولوجيا الامن السيبراني يساهم في رفع كفاءة مخرجات النظم المحاسبية والحد من القرصنة ورفع الخصائص النوعية للمعلومات المالية.	24 (26.7%)	45 (50.0%)	15 (16.7%)	6 (6.7%)	0 (0.0%)	3.97	0.841

توضح النتائج هنا أن المتوسطات الحسابية لفقرات هذا المحور تراوحت بين (3.97) و(4.33)، بما يعكس مستوى موافقة مرتفعًا على جميع الفقرات وفق معيار تفسير المتوسطات المعتمد في الدراسة، الأمر الذي يشير إلى إدراك المشاركين لأهمية الأمن السيبراني في دعم سلامة المعلومات المالية والحد من المخاطر التي قد تتعرض لها النظم المحاسبية.

وفيما يتعلق بحماية البيانات ودقة المعلومات، حققت الفقرة الثالثة، التي تنص على أن (تنعكس قوة الأمن السيبراني على دقة التقارير المالية وخلوها من الأخطاء الناتجة عن الاختراقات)، أعلى متوسط حسابي بلغ (4.33)، بانحراف معياري قدره (0.618). كما أظهرت النتائج أن (92.2%) من المشاركين أبدوا موافقتهم على هذه الفقرة، منهم (41.1%) موافقين بشدة و(51.1%) موافقين. ويعكس ذلك أهمية حماية الأنظمة المصرفية من الاختراقات في المحافظة على دقة التقارير المالية وسلامة المعلومات الواردة فيها .كذلك سجلت الفقرة الأولى، المتعلقة (بمنع تعديل البيانات المحاسبية أو تحريفها من أطراف غير مصرح لها)، متوسطًا حسابيًا بلغ (4.31)، وانحرافًا معياريًا قدره (0.664)، مع بلوغ نسبة الموافقة الإجمالية (88.9%)، وهو ما يؤكد أهمية حماية البيانات من التغيير غير المصرح به. كما بلغ المتوسط الحسابي للفقرة (الخاصة بالتحقق الإلكتروني من هوية العملاء والموردين والحد من تسجيل العمليات المالية الوهمية) (4.31)، بانحراف معياري قدره (0.554)، ووصلت نسبة الموافقة عليها إلى (95.6%)، وهي أعلى نسبة موافقة إجمالية بين فقرات المحور .وتشير هذه النتيجة إلى اتفاق واضح بين المشاركين بشأن أهمية آليات التحقق الإلكتروني في تعزيز موثوقية العمليات المصرفية وتقليل فرص تسجيل المعاملات غير الصحيحة، كما بلغ متوسط الفقرة المتعلقة (بتعزيز ثقة الأطراف الخارجية في المخرجات المحاسبية نتيجة قوة النظام السيبراني) (4.30)، بانحراف معياري قدره (0.589)، وبلغت نسبة الموافقة الإجمالية (93.4%)، مما يبرز ارتباط حماية المعلومات المالية بثقة المودعين والمستثمرين في مخرجات النظم المحاسبية.

أما فيما يخص منع التلاعب بالبيانات المالية، فقد بلغ متوسط الفقرة التاسعة (4.28)، بانحراف معياري قدره (0.900)، وأبدى (85.6%) من المشاركين موافقتهم عليها، وفيما يتعلق باستمرارية تشغيل النظم المحاسبية وتأمين الربط بين مكونات النظام المصرفي، بلغ المتوسط الحسابي للفقرة الخاصة بتوفير مسار مراجعة إلكتروني يسهل تتبع العمليات المالية (4.08)، بانحراف معياري قدره (0.838)، وبلغت نسبة الموافقة الإجمالية .(82.2%)بينما سجلت الفقرة المتعلقة (بضمان استمرارية عمل نظم المعلومات المحاسبية في مواجهة هجمات حجب الخدمة)، متوسطًا قدره (3.99)، بانحراف معياري بلغ (0.880)، مع نسبة موافقة إجمالية بلغت (76.7%) أما الفقرة (بربط الأنظمة الفرعية بالنظام المحاسبي المركزي بصورة آمنة وتقليل أخطاء الإدخال اليدوي)، فقد بلغ متوسطها (4.19)، بانحراف معياري قدره (0.669)، وبلغت نسبة الموافقة الإجمالية (87.8%)، مما يعكس أهمية التكامل الآمن بين الأنظمة المصرفية في الحد من الأخطاء وتعزيز كفاءة تدفق البيانات.

كما أظهرت النتائج أن الفقرة المتعلقة ب (النظر إلى الاستثمار في الأمن السيبراني بوصفه استراتيجية مؤسسية تتجاوز مجرد اقتناء البرمجيات)، سجلت متوسطًا حسابيًا قدره (4.04)، بانحراف معياري بلغ (0.873)، مع نسبة موافقة إجمالية وصلت إلى (80%).

وبصفة عامة، تشير نتائج الجدول إلى أن المشاركين ينظرون بإيجابية إلى دور الاستثمار في تكنولوجيا الأمن السيبراني في تعزيز موثوقية المعلومات المحاسبية المصرفية، ولا سيما فيما يتعلق بدقة التقارير المالية، وحماية البيانات من التحريف، والتحقق من هوية المتعاملين، وتعزيز الثقة في المخرجات المحاسبية وفي المقابل تظهر الحاجة إلى ضرورة العناية بالجوانب المرتبطة باستمرارية تشغيل النظم وتقليل فترات توقفها، نظرًا إلى انخفاض نسبة الموافقة على بعض الفقرات المرتبطة بهذه الجوانب مقارنةً بغيرها .وتوفر هذه النتائج وصفًا لاتجاهات المشاركين وتصوراتهم، على أن يُستكمل اختبار فرضية أثر الاستثمار في الأمن السيبراني على موثوقية النظم المحاسبية باستخدام التحليل الاستدلالي المناسب، مثل تحليل الارتباط والانحدار.

اختبار(T)لعينة واحدة لدلالة استجابات المشاركين وترتيبها حسب المتوسطات الحسابية :أثر الأمن السيبراني على خصائص المعلومات وموثوقية النظم المحاسبية والمصرفية:

استكمالًا للتحليل الوصفي لفقرات المحور الثاني، تم استخدام اختبار(T) لعينة واحدة للتحقق من الدلالة الإحصائية لاستجابات المشاركين، وذلك بمقارنة المتوسط الحسابي لكل فقرة بالقيمة المحكية المعتمدة في الدراسة، والبالغة (3) وفق مقياس ليكرت الخماسي .كما تم ترتيب الفقرات تنازليًا وفقًا لمتوسطاتها الحسابية، وتحديد اتجاه كل فقرة وفق مستويات التقدير اللفظي المعتمدة، ويهدف هذا التحليل إلى بيان مستوى موافقة المشاركين على دور الأمن السيبراني في دعم خصائص المعلومات وموثوقية النظم المحاسبية والمصرفية، وتحديد الجوانب التي حظيت بأعلى وأدنى مستويات الموافقة، بما يساعد على مناقشة نتائج الدراسة في ضوء أهدافها.

جدول رقم (13): نتائج اختبار (T) لعينة واحدة وترتيب فقرات أثر الأمن السيبراني على خصائص المعلومات وموثوقية النظم المحاسبية والمصرفية حسب المتوسطات الحسابية

ر.م	العبارات	المتوسط الحسابي	الانحراف المعياري	قيمة تي	قيمة الدالة	ترتيب الفقرات	اتجاه الفقرة
1	يساهم الاستثمار في الأمن السيبراني في ضمان عدم تعديل أو تحريف البيانات المحاسبية من قبل أطراف غير مصرح لها.	4.31	0.664	18.721	0.000	2	مرتفع جدا
2	تزداد ثقة الأطراف الخارجية (المودعين، المستثمرين) في المخرجات المحاسبية نتيجة قوة النظام السيبراني.	4.30	0.589	20.931	0.000	4	مرتفع جدا
3	تنعكس قوة الأمن السيبراني على دقة التقارير المالية وخلوها من الأخطاء الناتجة عن الاختراقات	4.33	0.618	20.465	0.000	1	مرتفع جدا
4	توفر تكنولوجيا الأمن السيبراني آليات متطورة للتحقق من هوية العملاء والموردين إلكترونياً، مما يمنع تسجيل عمليات مالية وهمية.	4.31	0.554	22.463	0.000	3	مرتفع جدا
5	يسمح الاستثمار السيبراني بربط الأنظمة الفرعية (الخزينة، الائتمان، المقاصة) بالنظام المحاسبي المركزي بشكل آمن، مما يقلل من أخطاء الإدخال اليدوي.	4.19	0.669	16.869	0.000	6	مرتفع
6	يقلل الاستثمار في جدران الحماية القوية من مخاطر توقف النظام(Downtime) ، مما يضمن استخراج التقارير المالية في مواعيدها القانونية دون تأخير ناتج عن هجمات سيبرانية	3.97	0.785	11.676	0.000	12	مرتفع
7	توفر تكنولوجيا الأمن السيبراني مسار مراجعة إلكتروني (Audit Trail) يسهل تتبع العمليات المالية.	4.08	0.838	12.206	0.000	8	مرتفع
8	تضمن أنظمة الحماية استمرارية عمل نظم المعلومات المحاسبية دون توقف ناتج عن هجمات حجب الخدمة.(DoS)	3.99	0.880	10.656	0.000	11	مرتفع
9	تضمن تقنيات الأمن السيبراني عدم التلاعب بالبيانات المالية من جهات غير مخولة.	4.28	0.900	13.472	0.000	5	مرتفع جدا
10	تساهم أنظمة الحماية في توفير تقارير مالية دقيقة وخالية من التحريف الناتج عن الاختراق	4.00	0.874	10.853	0.000	10	مرتفع
11	يقلل الاستثمار السيبراني من فترات توقف النظم المحاسبية نتيجة الهجمات الإلكترونية	4.10	1.006	10.372	0.000	7	مرتفع
12	يتجاوز الاستثمار في تكنولوجيا الامن السيبراني كونه مجرد اقتناء للبرمجيات إلى كونه استراتيجية مؤسسية تعيد تشكيل البيئة التشغيلية للنظام المحاسبي الرقمي.	4.04	0.873	11.351	0.000	9	مرتفع
13	إن الاستثمار في تكنولوجيا الامن السيبراني يساهم في رفع كفاءة مخرجات النظم المحاسبية والحد من القرصنة ورفع الخصائص النوعية للمعلومات المالية.	3.97	0.841	10.909	0.000	13	مرتفع

هنا يتضح لنا نتائج اختبار(T) لعينة واحدة، والذي استُخدم للتحقق من دلالة الفروق بين المتوسطات الحسابية لاستجابات المشاركين والقيمة المحايدة للمقياس البالغة (3)، إلى جانب ترتيب فقرات المحور وفق متوسطاتها الحسابية .وتشير النتائج إلى أن المتوسطات الحسابية للفقرات تراوحت بين (3.97) (4.33) وجاءت جميعها ضمن مستوى الاتجاه المرتفع أو

المرتفع جدًا وفقًا لمعيار تفسير المتوسطات المعتمد في الدراسة، بما يعكس اتجاهًا إيجابيًا لدى المشاركين نحو دور الأمن السيبراني في تعزيز خصائص المعلومات وموثوقية النظم المحاسبية والمصرفية.

وعلى مستوى ترتيب الفقرات، جاءت الفقرة الثالثة، التي تنص على أن (تنعكس قوة الأمن السيبراني على دقة التقارير المالية وخلوها من الأخطاء الناتجة عن الاختراقات)، في المرتبة الأولى، بمتوسط حسابي بلغ(4.33)، وانحراف معياري قدره (0.618)، تلتها الفقرة الأولى المتعلقة بضمان عدم تعديل البيانات المحاسبية أو تحريفها من أطراف غير مصرح لها، بمتوسط حسابي بلغ(4.31)، وانحراف معياري قدره (0.664)، ثم الفقرة الرابعة الخاصة بالتحقق الإلكتروني من هوية العملاء والموردين والحد من تسجيل العمليات المالية الوهمية، بمتوسط حسابي بلغ (4.31)وانحراف معياري قدره(0.554) ويشير تقدم هذه الفقرات إلى أن المشاركين يولون أهمية كبيرة لحماية سلامة البيانات المالية، وضمان دقة التقارير المحاسبية، والتحقق من صحة العمليات المصرفية.

كما جاءت الفقرة الثانية المتعلقة بتعزيز ثقة الأطراف الخارجية في المخرجات المحاسبية في المرتبة الرابعة، بمتوسط حسابي بلغ (4.30)، وانحراف معياري قدره (0.589)، والفقرة الخاصة بمنع التلاعب بالبيانات المالية من جهات غير مخولة، المرتبة الخامسة، بمتوسط حسابي بلغ (4.28)وانحراف معياري قدره .(0.900)وتبرز هذه النتائج أهمية الدور المتوقع لتقنيات الأمن السيبراني في حماية المعلومات المالية وتعزيز الثقة في مخرجات النظم المحاسبية والمصرفية.

وفي المراتب التالية، جاءت الفقرة المتعلقة بربط الأنظمة الفرعية بالنظام المحاسبي المركزي بصورة آمنة في المرتبة السادسة، بمتوسط حسابي قدره (4.19)، تلتها الفقرة الخاصة بتقليل فترات توقف النظم المحاسبية نتيجة الهجمات الإلكترونية، بمتوسط (4.10)، ثم الفقرة المتعلقة بتوفير مسار مراجعة إلكتروني لتتبع العمليات المالية، بمتوسط .(4.08) أما الفقرة التي تناولت النظر إلى الاستثمار السيبراني باعتباره استراتيجية مؤسسية تتجاوز مجرد اقتناء البرمجيات، فقد جاءت في المرتبة التاسعة بمتوسط حسابي بلغ (4.04)، تلتها الفقرة المتعلقة بتوفير تقارير مالية دقيقة وخالية من التحريف الناتج عن الاختراق، بمتوسط (4.00)، ثم الفقرة الخاصة باستمرارية عمل نظم المعلومات المحاسبية في مواجهة هجمات حجب الخدمة، بمتوسط .(3.99)

أما فيما يتعلق بنتائج اختبار (T)، فقد تراوحت قيمته بين (10.372)و(22.463)، وظهرت قيمة الدلالة في مخرجات البرنامج (0.000)لجميع الفقرات .وتُفسَّر هذه النتيجة إحصائيًا على أنها دالة عند مستوى (\p<0.001)، وليست قيمة احتمالية تساوي صفرًا حرفيًا .وبذلك توجد فروق ذات دلالة إحصائية بين متوسطات استجابات المشاركين والقيمة المحايدة للمقياس (3)، وجاء اتجاه هذه الفروق لصالح المتوسطات الأعلى من القيمة المحايدة، نظرًا إلى أن جميع المتوسطات الحسابية تجاوزت .(3)

وبناءً على ما سبق، يتضح أن استجابات المشاركين تعكس اتجاهًا إيجابيًا نحو دور الأمن السيبراني في تعزيز موثوقية النظم المحاسبية والمصرفية، مع بروز حماية البيانات ودقة التقارير والتحقق من العمليات في مقدمة الجوانب التي حظيت بأعلى المتوسطات .ومع ذلك، فإن هذه النتائج تعبّر عن مستوى الموافقة المدركة لدى المشاركين.

التحليل الوصفي لفقرات المحور الثالث: دور الأمن السيبراني في تعزيز فاعلية الرقابة الداخلية:

يهدف هذا المحور إلى التعرّف على دور تكنولوجيا الأمن السيبراني في تعزيز فاعلية الرقابة الداخلية في المصارف التجارية الليبية، وبهذا تم تحليل استجابات المشاركين باستخدام التكرارات والنسب المئوية والمتوسطات الحسابية والانحرافات المعيارية، بهدف تحديد مستوى الموافقة على فقرات المحور والتعرّف على اتجاهات المشاركين بشأن دور الأمن السيبراني في تعزيز فاعلية الرقابة الداخلية.

جدول رقم (14): التوزيع التكراري والنسب المئوية لاستجابات المشاركين حول فقرات دور الأمن السيبراني في تعزيز فاعلية الرقابة الداخلية.

ر.م	العبارات	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة	المتوسط الحسابي	الانحراف المعياري
1	تساهم تكنولوجيا الأمن السيبراني في تفعيل مبدأ الفصل بين الوظائف عبر الصلاحيات الرقمية.	37 (41.1%)	39 (43.3%)	10 (11.1%)	4 (4.4%)	0 (0.0%)	4.21	0.814
2	توفر الأنظمة السيبرانية رقابة تلقائية (Automated Controls) تمنع تنفيذ العمليات المشبوهة فوراً.	28 (31.1%)	44 (48.9%)	16 (17.8%)	2 (2.2%)	0 (0.0%)	4.09	0.759
3	يساعد الاستثمار السيبراني في تحسين بيئة الرقابة من خلال الكشف المبكر عن محاولات الاحتيال الداخلي.	40 (44.4%)	38 (42.2%)	12 (13.3%)	0 (0.0%)	0 (0.0%)	4.31	0.697
4	تعزز التكنولوجيا المستخدمة من قدرة المدققين الداخليين على الوصول الفوري والآمن للبيانات الحساسة.	24 (26.7%)	58 (64.4%)	8 (8.9%)	0 (0.0%)	0 (0.0%)	4.18	0.572
5	يساهم الاستثمار في الحوسبة السحابية المؤمنة في حماية الأصول المعلوماتية للمصرف من الكوارث المادية أو الهجمات التخريبية، مما يعزز استمرارية الرقابة.	20 (22.2%)	48 (53.3%)	22 (24.4%)	0 (0.0%)	0 (0.0%)	3.98	0.687
6	تسمح تكنولوجيا الأمن السيبراني بفرض رقابة صارمة على مقدمي الخدمات الإلكترونية الخارجيين الذين يرتبطون بأنظمة المصرف، لضمان عدم اختراق الرقابة من خلالهم.	28 (31.1%)	47 (52.2%)	14 (15.6%)	1 (1.1%)	0 (0.0%)	4.13	0.706

7	يعتمد نظام الرقابة الداخلية في المصرف على تقارير دورية ناتجة عن أنظمة الأمن السيبراني لتحديد نقاط الضعف المحتملة في العمليات المالية.	37 (41.1%)	37 (41.1%)	12 (13.3%)	4 (4.4%)	0 (0.0%)	4.19	0.833
8	يقلل الاستثمار في الأمن السيبراني من مخاطر تجاوز الإدارة للضوابط الرقابية عبر الأنظمة الرقمية.	34 (37.8%)	41 (45.6%)	12 (13.3%)	3 (3.3%)	0 (0.0%)	4.18	0.787
9	تعزز تكنولوجيا الأمن السيبراني من قدرة المصرف على الرصد الفوري للعمليات المشبوهة.	14 (15.6%)	53 (58.9%)	20 (22.2%)	1 (1.1%)	2 (2.2%)	3.84	0.778
10	تساعد أدوات الأمن السيبراني المدققين الداخليين في أداء مهامهم بفاعلية وموثوقية.	28 (31.1%)	48 (53.3%)	10 (11.1%)	3 (3.3%)	1 (1.1%)	4.10	0.808
11	تُساهم أتمتة الرقابة باستخدام تقنيات التحليل الذكي في الاكتشاف المبكر للمخاطر والسلوكيات الشاذة والاحتيال المالي قبل تفاقمه.	34 (37.8%)	46 (51.1%)	9 (10.0%)	1 (1.1%)	0 (0.0%)	4.26	0.680
12	تلتزم الرقابة الداخلية بمعايير أمنية صارمة تتماشى مع متطلبات التحول الرقمي.	32 (35.6%)	40 (44.4%)	10 (11.1%)	3 (3.3%)	5 (5.6%)	4.01	1.055
13	يُساهم الاستثمار في التشفير وأدوات الحماية في دعم فعاليات الرقابة الداخلية لحماية الأصول المالية وإدارة المخاطر المباشرة.	19 (21.1%)	50 (55.6%)	14 (15.6%)	3 (3.3%)	4 (4.4%)	3.86	0.943
14	تُعزز حوكمة الرقابة الداخلية بالتعاون مع الأمن السيبراني من امتثال المصرف للتشريعات المالية وتجنب الغرامات والمسؤوليات القانونية.	32 (35.6%)	43 (47.8%)	8 (8.9%)	0 (0.0%)	7 (7.8%)	4.03	1.075

اختبار(T) لعينة واحدة لدلالة استجابات المشاركين وترتيبها حسب المتوسطات الحسابي لدور الأمن السيبراني في تعزيز فاعلية الرقابة الداخلية:

استكمالًا للتحليل الوصفي لفقرات المحور الثالث، تم استخدام اختبار(T) لعينة واحدة للتحقق من الدلالة الإحصائية لاستجابات المشاركين بشأن دور الأمن السيبراني في تعزيز فاعلية الرقابة الداخلية، وتم ترتيب الفقرات تنازليًا وفقًا لمتوسطاتها الحسابية، وتحديد اتجاه كل فقرة وفق مستويات التقدير اللفظي المعتمدة، بما يساعد على مناقشة نتائج الدراسة في ضوء أهدافها وتساؤلها الرئيس.

جدول رقم (15): نتائج اختبار (T)لعينة واحدة وترتيب فقرات دور الأمن السيبراني في تعزيز فاعلية الرقابة الداخلية حسب المتوسطات الحسابية.

ر.م	العبارات	المتوسط الحسابي	الانحراف المعياري	قيمة تي	قيمة الدالة	ترتيب الفقرات	اتجاه الفقرة
1	تساهم تكنولوجيا الأمن السيبراني في تفعيل مبدأ الفصل بين الوظائف عبر الصلاحيات الرقمية.	4.21	0.814	14.113	0.000	3	مرتفع جدا
2	توفر الأنظمة السيبرانية رقابة تلقائية (Automated Controls) تمنع تنفيذ العمليات المشبوهة فوراً.	4.09	0.759	13.608	0.000	9	مرتفع
3	يساعد الاستثمار السيبراني في تحسين بيئة الرقابة من خلال الكشف المبكر عن محاولات الاحتيال الداخلي.	4.31	0.697	17.835	0.000	1	مرتفع جدا
4	تعزز التكنولوجيا المستخدمة من قدرة المدققين الداخليين على الوصول الفوري والآمن للبيانات الحساسة.	4.18	0.572	19.522	0.000	5	مرتفع
5	يساهم الاستثمار في الحوسبة السحابية المؤمنة في حماية الأصول المعلوماتية للمصرف من الكوارث المادية أو الهجمات التخريبية، مما يعزز استمرارية الرقابة.	3.98	0.687	13.510	0.000	12	مرتفع
6	تسمح تكنولوجيا الأمن السيبراني بفرض رقابة صارمة على مقدمي الخدمات الإلكترونية الخارجيين الذين يرتبطون بأنظمة المصرف، لضمان عدم اختراق الرقابة من خلالهم.	4.13	0.706	15.222	0.000	7	مرتفع
7	يعتمد نظام الرقابة الداخلية في المصرف على تقارير دورية ناتجة عن أنظمة الأمن السيبراني لتحديد نقاط الضعف المحتملة في العمليات المالية.	4.19	0.833	13.536	0.000	4	مرتفع
8	يقلل الاستثمار في الأمن السيبراني من مخاطر تجاوز الإدارة للضوابط الرقابية عبر الأنظمة الرقمية.	4.18	0.787	14.193	0.000	6	مرتفع
9	تعزز تكنولوجيا الأمن السيبراني من قدرة المصرف على الرصد الفوري للعمليات المشبوهة.	3.84	0.778	10.302	0.000	14	مرتفع
10	تساعد أدوات الأمن السيبراني المدققين الداخليين في أداء مهامهم بفاعلية وموثوقية.	4.10	0.808	12.916	0.000	8	مرتفع
11	تُساهم أتمتة الرقابة باستخدام تقنيات التحليل الذكي في الاكتشاف المبكر للمخاطر والسلوكيات الشاذة والاحتيال المالي قبل تفاقمه.	4.26	0.680	17.523	0.000	2	مرتفع جدا

12	تلتزم الرقابة الداخلية بمعايير أمنية صارمة تتماشى مع متطلبات التحول الرقمي.	4.01	1.055	9.095	0.000	11	مرتفع
13	يُساهم الاستثمار في التشفير وأدوات الحماية في دعم فعاليات الرقابة الداخلية لحماية الأصول المالية وإدارة المخاطر المباشرة.	3.86	0.943	8.608	0.000	13	مرتفع
14	تُعزز حوكمة الرقابة الداخلية بالتعاون مع الأمن السيبراني من امتثال المصرف للتشريعات المالية وتجنب الغرامات والمسؤوليات القانونية.	4.03	1.075	9.117	0.000	10	مرتفع

هنا يعرض الجدول نتائج اختبار(T) لعينة واحدة لفقرات دور الأمن السيبراني في تعزيز فاعلية الرقابة الداخلية، مع ترتيب هذه الفقرات وفقًا لمتوسطاتها الحسابية .وتوضح النتائج أن المتوسطات الحسابية تراوحت بين (3.84)و(4.31)، بما يشير إلى أن اتجاه المشاركين نحو جميع فقرات المحور جاء مرتفعًا أو مرتفعًا جدًا وفقًا لمعيار تفسير المتوسطات المعتمد في الدراسة .كما جاءت قيم اختبار(T) موجبة لجميع الفقرات، وتراوحت بين (8.608)و(19.522)، في حين ظهرت قيمة الدلالة الإحصائية في مخرجات SPSSعلى صورة (0.000)لجميع الفقرات، وهو ما يُعبَّر عنه علميًا بـ (\p<0.001\)، بما يدل على وجود فروق ذات دلالة إحصائية بين متوسطات الاستجابات والقيمة المحايدة للمقياس البالغة (3)، لصالح المتوسطات الأعلى منها.

ونلاحظ أن الفقرة الثالثة، المتعلقة (بدور الاستثمار السيبراني في تحسين بيئة الرقابة من خلال الكشف المبكر عن محاولات الاحتيال الداخلي)، جاءت في المرتبة الأولى، بمتوسط حسابي بلغ (4.31)وانحراف معياري قدره (0.697)، وهو ما يعكس أهمية الكشف المبكرعن الممارسات غير المشروعة في تعزيز الرقابة الداخلية والحد من المخاطر التي قد تؤثر في سلامة العمليات المالية .تلتها الفقرة التي تناولت (مساهمة أتمتة الرقابة وتقنيات التحليل الذكي في الاكتشاف المبكر للمخاطر والسلوكيات الشاذة والاحتيال المالي)، بمتوسط حسابي بلغ (4.26)، وانحراف معياري قدره (0.680)، وجاءت في المرتبة الثانية .وتشير هاتان النتيجتان إلى أن المشاركين يمنحون أهمية واضحة للقدرات التقنية التي تساعد على اكتشاف المخاطر والاحتيال في مراحل مبكرة.

هذا واحتلت الفقرة المتعلقة بتفعيل مبدأ الفصل بين الوظائف عبر الصلاحيات الرقمية، المرتبة الثالثة بمتوسط حسابي قدره (4.21)وانحراف معياري بلغ (0.814)، تلتها الفقرة الخاصة باستخدام التقارير الدورية الناتجة عن أنظمة الأمن السيبراني لتحديد نقاط الضعف المحتملة في العمليات المالية، بمتوسط حسابي بلغ (4.19)وانحراف معياري قدره (0.833).كما جاءت الفقرتان الرابعة والثامنة في المرتبتين الخامسة والسادسة على التوالي، بمتوسط حسابي بلغ (4.18) لكل منهما؛ إذ تتعلق الأولى بتمكين المدققين الداخليين من الوصول الفوري والآمن إلى البيانات الحساسة، بينما تتناول الثانية الحد من مخاطر تجاوز الإدارة للضوابط الرقابية عبر الأنظمة الرقمية .وتبرز هذه النتائج أهمية الصلاحيات الرقمية والتقارير الرقابية وتأمين الوصول إلى المعلومات في دعم فاعلية إجراءات الرقابة الداخلية، هذا وجاءت باقي الفقرات في المراتب الأخيرة ولكن وعلى الرغم من حصول هذه الفقرات على أدنى متوسط في المحور، فإن اتجاهها لا يزال مرتفعًا وفقًا للمقياس المعتمد، مما يعني أن المشاركين ما زالوا يميلون إلى الموافقة على مضمونها، وإن كان القبول بدرجة أقل نسبيًا من بقية الفقرات.

وبوجه عام، تشير نتائج الجدول إلى أن المشاركين ينظرون بإيجابية إلى دور الأمن السيبراني في تعزيز فاعلية الرقابة الداخلية، ولا سيما في مجال الكشف المبكر عن الاحتيال والمخاطر، وتفعيل الصلاحيات الرقمية، واستخدام التحليل الذكي والتقارير الرقابية .كما توضح النتائج أن جميع المتوسطات الحسابية تجاوزت القيمة المحايدة للمقياس، وظهرت فروق دالة إحصائيًا عند مقارنتها بهذه القيمة .ومع ذلك، فإن اختبار (T)لعينة واحدة يثبت اختلاف متوسطات الاستجابات عن القيمة المحايدة، ولا يثبت بمفرده وجود أثر إحصائي مباشر للاستثمار في الأمن السيبراني على فاعلية الرقابة الداخلية؛ إذ يتطلب اختبار هذا الأثر إجراء تحليل الارتباط أو الانحدار بين المحورين.

والتساؤلات العامة التي يجب أن تطرح بعد هذه التفسيرات كالتالي:

1. **ما أثر الاستثمار في تكنولوجيا الأمن السيبراني على فاعلية وموثوقية الرقابة الداخلية في المصارف التجارية الليبية؟**

يرتبط هذا التساؤل بالهدف الثالث للدراسة، المتمثل في **بيان أثر الاستثمار في تكنولوجيا الأمن السيبراني على موثوقية النظم المحاسبية والرقابة الداخلية في المصارف**، ويُختبر في ضوء **الفرضية الرئيسة** التي تنص على أنه: «لا يوجد أثر ذا دلالة إحصائية للاستثمار في تكنولوجيا الأمن السيبراني على فاعلية أنظمة الرقابة الداخلية في المصارف الليبية». وللإجابة عن التساؤل، سيتم استخدام تحليل الانحدار الخطي البسيط لاختبار أثر الاستثمار في تكنولوجيا الأمن السيبراني في المصارف على دور الأمن السيبراني في تعزيز فاعلية الرقابة الداخلية.

جدول رقم (16): يوضح نتائج تحليل الانحدار الخطي البسيط لأثر الاستثمار في تكنولوجيا الأمن السيبراني على فاعلية الرقابة الداخلية

المتغير التابع	ملخص النموذج Model summary		تحليل التباين ANOVA		جدول المعاملات Coefficient				
	معامل الارتباط R	R^2	Fالمحسوبة	Sig F	البيان	B	الخطأ المعياري	T	Sig t
فاعلية الرقابة الداخلية	0.610[a]	0.373	52.264	0.000[b]	الاستثمار في تكنولوجيا الأمن السيبراني	0.446	0.062	7.229	0.000

*يكون التأثير ذا دالة احصائية عند مستوى ($\alpha \leq 0.05$)

وهنا يتضح من النتائج أن معامل الارتباط (R) بلغ (0.610)، مما يشير إلى وجود علاقة ارتباط موجبة بين الاستثمار في تكنولوجيا الأمن السيبراني وفاعلية الرقابة الداخلية في المصارف التجارية الليبية. كما بلغ معامل التحديد (R^2) (0.373)، وهو ما يعني أن الاستثمار في تكنولوجيا الأمن السيبراني يفسر ما نسبته (37.3%) من التباين في فاعلية الرقابة الداخلية، في حين تُعزى النسبة المتبقية، والبالغة (62.7%)، إلى عوامل أخرى لم يتضمنها النموذج وإلى الخطأ العشوائي. وأظهرت نتائج تحليل التباين أن قيمة (F) المحسوبة بلغت (52.264)، بمستوى دلالة أقل من (0.001)، وهو أقل من مستوى الدلالة المعتمد في الدراسة (0.05)، مما يدل على معنوية نموذج الانحدار إحصائيًا. كذلك بلغ معامل الانحدار(0.446) (B) ، وبلغ الخطأ المعياري (0.062)، في حين بلغت قيمة (t) المحسوبة (7.229)، بمستوى دلالة أقل من (0.001). وتشير هذه النتائج إلى وجود أثر إحصائي موجب ذي دلالة للاستثمار في تكنولوجيا الأمن السيبراني على فاعلية الرقابة الداخلية.

وبناءً على ذلك، تُرفض الفرضية الصفرية التي تنص على عدم وجود أثر ذي دلالة إحصائية للاستثمار في تكنولوجيا الأمن السيبراني على فاعلية أنظمة الرقابة الداخلية في المصارف الليبية، وتُدعم الفرضية البديلة التي تفيد بوجود أثر إحصائي موجب ذي دلالة. ومع ذلك، فإن هذه النتيجة تعبّر عن الأثر الإحصائي وفق نموذج الانحدار وبيانات الدراسة، ولا تكفي وحدها لإثبات السببية بصورة قاطعة.

2. ما أثر الأدوات التقنية الحديثة، مثل التشفير والمصادقة البيومترية، في تفعيل إجراءات الرقابة الداخلية والحد من الاحتيال في المصارف التجارية الليبية؟

يرتبط هذا التساؤل بالهدف الثاني للدراسة، المتمثل في قياس أثر الأدوات التقنية الحديثة في تفعيل إجراءات الرقابة الداخلية والحد من الاحتيال، ويرتبط موضوعيًا بالفرضية الفرعية الثانية التي تنص على أنه: لا يوجد أثر ذا دلالة إح**صائية** للاستثمار في تكنولوجيا الأمن السيبراني على فاعلية الرقابة الداخلية وتعزيزها. وسيتم تحليل فقرات المحور الثالث المتعلقة بالرقابة الآلية والكشف عن الاحتيال والتشفير وأدوات الحماية، والاستفادة من اختبار أثر المحور الأول على المحور الثالث. ولا يمكن قياس الأثر المستقل للمصادقة البيومترية ما لم تكن مقاسة مباشرةً في الاستبيان.

جدول رقم (17): نتائج تحليل الانحدار الخطي البسيط لأثر الاستثمار في تكنولوجيا الأمن السيبراني على خصائص المعلومات وموثوقية النظم المحاسبية والمصرفية في المصارف التجارية الليبية.

المتغير التابع	ملخص النموذج Model summary		تحليل التباين ANOVA		جدول المعاملات Coefficient				
	معامل الارتباط R	R^2	Fالمحسوبة	Sig F	البيان	B	الخطأ المعياري	T	Sig t
خصائص المعلومات وموثوقية النظم المحاسبية والمصرفية	0.615[a]	0.378	53.514	0.000[b]	الاستثمار في تكنولوجيا الأمن السيبراني	0.504	0.069	7.315	0.000

*يكون التأثير ذا دالة احصائية عند مستوى ($\alpha \leq 0.05$)

يتضح من نتائج الجدول أن معامل الارتباط(R) بلغ (0.615)، مما يشير إلى وجود علاقة ارتباط موجبة بين الاستثمار في تكنولوجيا الأمن السيبراني وخصائص المعلومات وموثوقية النظم المحاسبية والمصرفية في المصارف التجارية الليبية. كما بلغ معامل التحديد(0.378) (R^2) ، وهو ما يعني أن الاستثمار في تكنولوجيا الأمن السيبراني يفسر ما نسبته (37.8%) من التباين في خصائص المعلومات وموثوقية النظم المحاسبية والمصرفية، في حين تُعزى النسبة المتبقية، والبالغة (62.2%)، إلى عوامل أخرى لم يتضمنها النموذج وإلى الخطأ العشوائي. وأظهرت نتائج تحليل التباين أن قيمة (F)المحسوبة بلغت (53.514)، بمستوى دلالة أقل من (0.001)، وهو أقل من مستوى الدلالة المعتمد في الدراسة (0.05)، مما يدل على معنوية نموذج الانحدار إحصائيًا. كذلك بلغ معامل الانحدار غير المعياري(0.504) (B) ، وبلغ

الخطأ المعياري (0.069)، في حين بلغت قيمة (t) المحسوبة (7.315)، بمستوى دلالة أقل من (0.001). وتشير هذه النتائج إلى وجود أثر إحصائي موجب ذي دلالة للاستثمار في تكنولوجيا الأمن السيبراني على خصائص المعلومات وموثوقية النظم المحاسبية والمصرفية.

وبناءً على ذلك، تُرفض الفرضية الصفرية الفرعية الأولى التي تنص على عدم وجود أثر ذي دلالة إحصائية للاستثمار في تكنولوجيا الأمن السيبراني على خصائص المعلومات وموثوقية النظم المحاسبية المصرفية، وتُدعم الفرضية البديلة التي تفيد بوجود أثر إحصائي موجب ذي دلالة. وتدل هذه النتيجة على أن ارتفاع مستوى الاستثمار في تكنولوجيا الأمن السيبراني يرتبط بارتفاع مستوى خصائص المعلومات وموثوقية النظم المحاسبية والمصرفية لدى أفراد عينة الدراسة.

تحليل معامل ارتباط بيرسون بين متغيرات الدراسة:

يهدف تحليل الارتباط إلى التعرف على اتجاه العلاقة وقوتها ودلالتها الإحصائية بين الاستثمار في تكنولوجيا الأمن السيبراني وكلٍّ من خصائص المعلومات وموثوقية النظم المحاسبية والمصرفية وفاعلية الرقابة الداخلية، بالإضافة إلى تحديد طبيعة العلاقة بين هذين المحورين .ويُعد هذا التحليل مكمّلًا لتحليل الانحدار الخطي البسيط الذي أُجري لاختبار فرضيات الدراسة، إذ يساعد على تقديم صورة متكاملة عن العلاقات بين متغيرات الدراسة. للتحقق من طبيعة العلاقات بين متغيرات الدراسة، تم استخدام معامل ارتباط بيرسون (Pearson Correlation Coefficient)لقياس اتجاه العلاقة الخطية وقوتها بين متوسطات محاور الدراسة الثلاثة، وذلك عند مستوى دلالة إحصائية .(0.05)ويُستخدم هذا التحليل لتحديد ما إذا كانت العلاقات بين المحاور موجبة أم سالبة، وما إذا كانت ذات دلالة إحصائية، بما يسهم في تفسير النتائج والإجابة عن تساؤلات الدراسة.

جدول رقم (18): نتائج تحليل معامل ارتباط بيرسون بين الاستثمار في تكنولوجيا الأمن السيبراني وخصائص المعلومات وموثوقية النظم المحاسبية والمصرفية وفاعلية الرقابة الداخلية في المصارف التجارية الليبية

المتغيرات (محاور الدراسة)		الاستثمار في تكنولوجيا الأمن السيبراني	أثر الأمن السيبراني على خصائص المعلومات وموثوقية النظم المحاسبية والمصرفية	دور الأمن السيبراني في تعزيز فاعلية الرقابة الداخلية
الاستثمار في تكنولوجيا الأمن السيبراني	معامل الارتباط بيرسون	1	0.615**	0.610**
	قيمة الدلالة الإحصائية	-	0.000	0.000
أثر الأمن السيبراني على خصائص المعلومات وموثوقية النظم المحاسبية والمصرفية	معامل الارتباط بيرسون		1	0.619**
	قيمة الدلالة الإحصائية		-	0.000
دور الأمن السيبراني في تعزيز فاعلية الرقابة الداخلية	معامل الارتباط بيرسون			1
	قيمة الدلالة الإحصائية			-

يتضح من نتائج الجدول، الذي يعرض معاملات ارتباط بيرسون ثنائية الطرف (Two-tailed)، وجود علاقات ارتباط موجبة ذات دلالة إحصائية عند مستوى دلالة (0.01)بين محاور الدراسة الثلاثة .فقد بلغ معامل الارتباط بين الاستثمار في تكنولوجيا الأمن السيبراني وأثر الأمن السيبراني على خصائص المعلومات وموثوقية النظم المحاسبية والمصرفية (0.615)، كما بلغ معامل الارتباط بين الاستثمار في تكنولوجيا الأمن السيبراني ودور الأمن السيبراني في تعزيز فاعلية الرقابة الداخلية .(0.610)كذلك بلغ معامل الارتباط بين أثر الأمن السيبراني على خصائص المعلومات وموثوقية النظم المحاسبية والمصرفية ودوره في تعزيز فاعلية الرقابة الداخلية .(0.619)وقد كانت مستويات الدلالة الإحصائية لجميع هذه العلاقات أقل من (0.001)، مما يشير إلى أن العلاقات موجبة ودالة إحصائيًا عند مستوى (0.01)، وبحجم عينة بلغ (90)مفردة.

وتشير هذه النتائج إلى أنه كلما ارتفع مستوى الاستثمار في تكنولوجيا الأمن السيبراني، ارتفع مستوى خصائص المعلومات وموثوقية النظم المحاسبية والمصرفية، وكذلك مستوى فاعلية الرقابة الداخلية، كما ترتبط زيادة موثوقية النظم المحاسبية والمصرفية بارتفاع مستوى فاعلية الرقابة الداخلية .وبناءً على ذلك، تدعم النتائج وجود علاقات ارتباط موجبة ودالة إحصائيًا بين محاور الدراسة، مع التأكيد على أن الارتباط لا يعني بالضرورة وجود علاقة سببية، وإنما يوضح اتجاه العلاقة وقوتها بين المتغيرات.

النتائج والتوصيات:

أولاً: النتائج:

1. أظهرت النتائج وجود أثر إيجابي و ذا دلالة إحصائية للاستثمار في تكنولوجيا الأمن السيبراني على فاعلية الرقابة الداخلية في المصارف التجارية الليبية، فقد بلغ معامل الارتباط (R = 0.610)، وفسر الاستثمار ما نسبته (37.3%) من التباين في فاعلية الرقابة الداخلية (R^2 = 0.373). وكان النموذج معنوياً (F = 52.264، Sig < 0.001)، كما بلغ معامل الانحدار (B = 0.446) بقيمة (t = 7.229) ودلالة أقل من (0.001)، كما أظهرت النتائج وجود أثر موجب ذا دلالة إحصائية للاستثمار في الأمن السيبراني على خصائص المعلومات وموثوقية النظم المحاسبية والمصرفية (R = 0.615، R^2 = 0.378، B = 0.504، Sig < 0.001). كما ظهرت علاقات ارتباط موجبة

ودالة عند مستوى (0.01) بين محاور الدراسة الثلاثة، وأقواها العلاقة بين موثوقية النظم المحاسبية وفاعلية الرقابة الداخلية (r = 0.619).

وبهذا ترفض الفرضية الصفرية التي تنص على أنه (لا يوجد أثر ذا دلالة إحصائية للاستثمار في تكنولوجيا الأمن السيبراني على فاعلية أنظمة الرقابة الداخلية في المصارف الليبية). وما نتج عنها من فرضيات فرعية صفرية. وقبول الفرضية البديلة التي مفادها (يوجد أثر ذا دلالة إحصائية للاستثمار في تكنولوجيا الأمن السيبراني على فاعلية أنظمة الرقابة الداخلية في المصارف الليبية).

2. يستخدم (51.1%) من المشاركين الخدمات المصرفية الإلكترونية بشكل يومي وكلي، ويستخدمها (33.3%) بشكل جزئي، أي (84.4%) في المجموع. يعكس هذا اعتماداً كبيراً على هذه الخدمات في إنجاز العمل المصرفي، ويؤكد أن الاستثمار في الأمن السيبراني ضرورة لحماية المعاملات والبيانات، وتعزيز موثوقية النظم وفاعلية الرقابة الداخلية.
3. جاء اتجاه بخصوص محور الاستثمار في الامن السيبراني إيجابياً بمتوسط عام بلغ (3.92)، غير أن فقرة كفاية الميزانيات المخصصة لتطوير البنية التحتية للأمن السيبراني سجّلت أعلى انحراف معياري بين الفقرات (1.259) ونسبة عدم موافقة بلغت (25.5%)، ما يكشف تفاوتاً واضحاً في الآراء حول كفاية هذه الميزانيات، ويعكس ادراكا ووعيا بأهمية الأمن السيبراني كضرورة استراتيجية، إلا أن هذا الوعي يتصادم مع التحديات العملية على ارض الواقع التي قد تكون بسبب تفاوت التمويل لمؤسسات مصرفية عن غيرها، أو بسبب شح التمويل لهذا الجانب. مما قد يتسبب في فجوة تساهم في الاختراقات.
4. . وكذلك جاءت فقرة وجود استراتيجية واضحة ومحدّثة لإدارة المخاطر السيبرانية وفق المعايير الدولية (NIST، COBIT، ISO 27001) بين أدنى الفقرات (3.72)، وبنسبة عدم موافقة مرتفعة نسبياً، وهذا التراجع لهذه الفقرة يعتبر مؤشر على خطورة عالية؛ إذ يوضح أن كثيراً من الجهات تفتقر إلى إطار مرجعي دولي يحكم إنفاقها وحمايتها، مما قد يؤدي إلى هدر الميزانيات المتاحة في حلول سيئة وغير مبنية على تقييم منهجي للمخاطر.
5. أجمع أغلبيّة المشاركين على أن الأمن السيبراني ركيزة استراتيجية ومباشرة لدعم جودة ونزاهة النظام المحاسبي المصرفي؛ حيث تجسّد ذلك في التأكيد المباشر على دور آليات التحقق الإلكتروني في منع المعاملات الوهمية بنسبة موافقة (95.6%)، وأثر قوة النظام السيبراني في تعزيز ثقة المودعين والمستثمرين بالبيانات المحاسبية بنسبة (93.4%)، فضلاً عن دور الربط الآمن بين الأنظمة الفرعية (كالخزينة والائتمان والمقاصة) للنظام المركزي في خفض الأخطاء ورفع كفاءة البيانات بنسبة (87.8%)، وصولاً إلى قناعة (80%)من المشاركين (بمتوسط 4.04) بأن الاستثمار السيبراني هو خيار استراتيجي مؤسسي شامل وليس مجرد حلول برمجية منفصلة.
6. تُظهر النتائج اتجاهاً ذا دلالة إحصائية ($p < 0.001$) نحو الدور المحوري للأمن السيبراني في تعزيز فاعلية الرقابة الداخلية؛ حيث يتجلى التفضيل الأكبر في التوجه نحو التقنيات الاستباقية بكشف الاحتيال الداخلي في المرتبة الأولى بمتوسط (4.31) وأتمتة الرقابة عبر التحليل الذكي لاكتشاف السلوكيات الشاذة بمتوسط(4.26) ، في حين جاء الرصد الفوري للعمليات المشبوهة بمتوسط (3.84) والتشفير (3.86) في المراتب الأخيرة رغم بقائهما في مستوى إيجابي مرتفع، ويساند هذا التوجه وجود ثغرة بشرية متمثلة في وجود (25.6%) من المشاركين بالمستوى المبتدئ أو بلا خبرة و(7.8%) لم يتلقوا أي تدريب سيبراني.

ثانيا: التوصيات:

1. تأسيس إطار إلزامي لحوكمة الميزانيات والاستراتيجيات السيبرانية من خلال ربط الإنفاق المالي على البنية التحتية للأمن السيبراني بالمعايير القياسية العالمية(ISO 27001 ،NIST ، COBIT) وتقييمات المخاطر الدورية، بما يضمن تقليل الفجوة التمويلية بين المؤسسات وضمان الاستخدام الأمثل للموارد المتاحة.
2. مأسسة الأمن السيبراني كخيار استراتيجي مكمل للنظام المحاسبي عبر التوسع في تطبيق آليات التحقق الرقمي المشددة وتأمين بروتوكولات الربط الآمن بين الأنظمة الفرعية والمركزية، لضمان نزاهة البيانات المالية وخفض الأخطاء وتعزيز ثقة المودعين والمستثمرين في القوائم المالية.
3. التحول نحو الرقابة المستمرة والذكية المشفوعة بالبناء المعرفي عن طريق توظيف تقنيات التحليل الذكي للكشف المبكر عن السلوكيات الشاذة والاحتيال الداخلي، بالتوازي مع إرساء برامج تدريبية وتوعوية مستدامة لسد الفجوة المهارية لدى الكوادر البشرية وضمان بيئة رقابية محصنة.
4. وضع حد أدنى إلزامي للميزانيات المخصصة للبنية التحتية للأمن السيبراني كنسبة مئوية ثابتة من ميزانية تقنية المعلومات الكلية في المؤسسة، مع تقديم دعم تمويلي أو تسهيلات للمؤسسات أو القطاعات التي تعاني من عجز في ميزانيات البنية التحتية للحد من الفجوة التي تم ملاحظتها في التشتت المعياري.
5. مواكبة التحول الرقمي المصرفي بزيادة المخصصات الاستثمارية في تكنولوجيا الأمن السيبراني للاستفادة من أثره التفسيري المباشر في رفع كفاءة منظومة الرقابة الداخلية وتعزيز موثوقية النظم المحاسبية، بما يوفر الحماية اللازمة لخدمات الصيرفة الإلكترونية التي يعتمد عليها الغالبية العظمى من المتعاملين.

6. ضرورة التعامل مع الاستثمار في الأمن السيبراني كركن أساسي ضمن الاستراتيجية الشاملة للمؤسسة المصرفية، من خلال تعزيز آليات التحقق الرقمي وتأمين الربط بين الأنظمة المحاسبية المختلفة، بما يضمن سلامة البيانات المالية ويرسخ ثقة المتعاملين والمستثمرين في مخرجات النظام المحاسبي.
7. التركيز على تعزيز تقنيات الكشف المبكر عن الاحتيال والرقابة الذكية، بالتوازي مع الاستثمار المستمر في التأهيل والتدريب السيبراني الشامل لكافة المستويات الوظيفية لسد الفجوة المعرفية وضمان فاعلية منظومة الرقابة الداخلية.

قائمة المراجع:

أولا: المراجع العربية:

1. أحمد محمد علي البديوي الرحاحله. (2026). دور الحوكمة الرقمية في تعزيز النزاهة ومكافحة الفساد. مجلة العلوم الإنسانية والطبيعية، 7(1)، 139-155.
2. ا. م. د. أميرة هاتف حداوي أ. م. د. ضرغام علي مسلم أ. د. صفاء تايه محمد. (2024). القيادة الرقمية ودورها في تعزيز سلوك الامن السيبراني في المنظمات (دراسة تحليلية لآراء عينة من العاملين في المصارف الأهلية في النجف الاشرف). مجلة العلوم الإنسانية والطبيعية، 5(1)، 681-701.
3. د. خليفة أبراهيم ميلاد، أ. فتحي منصور أبوشعفة. (2025). دور الإفصاح المحاسبي عن الأمن السيبراني في تحسين جودة المعلومات المحاسبية على المصارف التجارية الليبية-دراسة تطبيقية على فروع المصارف التجارية العاملة في مدينة مسلاته. مجلة العلوم الإنسانية والطبيعية، 6(7)، 554-583.
4. رمضان عايش البرديني. (2025). مخاطر تطبيقات التكنولوجيا المالية في المصارف الإسلامية القطرية وطرق الوقاية منها. مجلة العلوم الإنسانية والطبيعية، 6(3)، 266-276.
5. د. محمد بخيت محمد علي. (2025). أثر تكنولوجيا الذكاء الاصطناعي على جودة المعلومات المحاسبية (دراسة تطبيقية على البنك الزراعي السوداني، 2025م). مجلة العلوم الإنسانية والطبيعية، 6(6)، 56-72.
6. يوسف، حسن صالح، وخلف، برهان حسين. (2025). دور إجراءات الرقابة الداخلية في مواجهة مخاطر الأمن السيبراني: دراسة تحليلية .تنمية الرافدين، 44(147)، .295–267

ثانيا: المراجع الأجنبية:

1. Abu Kallal, S. A. A. K. (2025). The impact of accounting information systems quality on cybersecurity in Iraqi commercial banks. Raya International Journal of Business Sciences, 4(15).
2. Al-Laith, A. A. G. (2012). Adaptation of the Internal Control Systems with the Use of Information Technology and its Effects on the financial Statements Reliability: an applied study on commercial banks. International Management Review, 8(1), 12.
3. Hossin, A. M., & Ayedh, A. M. (2016). The risks of electronic accounting information system in the central bank of Libya. South East Asia Journal of Contemporary Business, Economics and Law, 10(1), 74-79.
4. Meghdouri, C., & Bouras, F. (2025). Cybersecurity in Accounting and Auditing: The Impact of Financial Data Security on Investor Confidence in the Banking Sector-A case study commercial banks in Algeria's. Journal of Economics and Finance, 298-277 , (2) 11 .
5. Morshed, A., & Khrais, L. T. (2025). Cybersecurity in digital accounting systems: Challenges and solutions in the arab gulf region. Journal of Risk and Financial Management, 18(1), 41.
6. Shafa, H., & Islam, A. (2025). Impact of Data Privacy and Cybersecurity In Accounting Information Systems On Financial Transparency. International Journal of Scientific Interdisciplinary Research, 6(1), 254-292.
7. Twaty, O. M., & Bouhafs, R. (2025). The Impact of Cloud-Based Systems on Accounting Operations in Islamic Banks: A Case Study of Al-Yaqeen Bank, Libya) NAJSP, 65-75.
8. Committee of Sponsoring Organizations of the Treadway Commission. (2013). Internal control—Integrated framework: Executive summary. COSO.
9. International Accounting Standards Board. (2018). Conceptual framework for financial reporting. IFRS Foundation.