The Role of Strengthening Cybersecurity Oversight in Financial Risk Management
(A Field Study on Social Security Institutions in Sudan)

-**Hadeel Abdulrahman Mohammed Obeid1**: *PhD researcher, Alneelain University, Sudan*
- **Abdulrahman Abdullah Abdulrahman Abdullah2**: *Professor, Alneelain University, Sudan*
- **Abdulrahman Adel Khalil Osman3**: *Associate Professor,, Alneelain University, Sudan*

Received:20 /09/2025 ***Accepted :04/11/2026*** ***Published :21/01/2026***

Abstract
The study aimed to assess the relationship between strengthening cybersecurity controls and financial risk management in these institutions. The results showed a statistically significant positive relationship between strengthening cybersecurity oversight and financial risk management. The study also revealed the development of integrated data protection systems, increased organisational awareness of the importance of cybersecurity, and the implementation of effective control measures to mitigate financial risks. Based on these findings, the study recommends developing a comprehensive cybersecurity strategy, enhancing liquidity management efficiency, improving accounting information accuracy, and promoting a culture of innovation in risk management and internal control methods.
Keywords:
Cybersecurity, oversight, financial risk management, social security institutions.
Jel Codes Classification : G32 ،G38 ،L86

1 - Hadeel Abdulrahman Mohammed Obeid : Faculty of Graduate Studies, hadeelobaid2024@gmail.com

2 - Faculty of Graduate Studies,

3 - Faculty of Graduate Studies,

دور تعزيز الرقابة على الأمن السيبراني في إدارة المخاطر المالية (دراسة ميدانية على مؤسسات الضمان الاجتماعي في السودان)

- **هديل عبد الرحمن محمد عبيد1:** باحث دكتوراة، جامعة النيلين، السودان
- **عبدالرحمن عبدالله عبدالرحمن عبدالله2:** بروفيسور، جامعة النيلين ، السودان
- **عبدالرحمن عادل خليل عثمان3:** أ.مشارك، جامعة النيلين ، السودان

تاريخ الإرسال: 2025/09/20 **تاريخ القبول: 2025/11/04** **تاريخ النشر: 2026/01/21**

ملخص

هدفت الدراسة إلى تقييم العلاقة بين تعزيز الرقابة على الأمن السيبراني وإدارة المخاطر المالية في هذه المؤسسات. أظهرت النتائج وجود علاقة إيجابية ذات دلالة إحصائية بين تعزيز الرقابة على الأمن السيبراني وإدارة المخاطر المالية. كما كشفت الدراسة عن تطوير أنظمة حماية متكاملة للبيانات، ورفع الوعي التنظيمي بأهمية الأمن السيبراني، وتطبيق إجراءات رقابية فعّالة للحد من المخاطر المالية. بناءً على هذه النتائج، توصي الدراسة بتطوير استراتيجية شاملة للأمن السيبراني، وتعزيز كفاءة إدارة السيولة، وتحسين دقة المعلومات المحاسبية، وتعزيز ثقافة الابتكار في أساليب إدارة المخاطر والرقابة الداخلية.

الكلمات المفاتيح: الأمن السيبراني، الرقابة، إدارة المخاطر المالية، مؤسسات الضمان الاجتماعي.

التصنيف JEL: G32، G38، L86

1- **هديل عبدالرحمن محمد عبيد**، كلية الدراسات العليا، *hadeelobaid2024@gmail.com*

2- كلية الدراسات العليا،

3- كلية الدراسات العليا،

- مقدّمة:

تُعتبر الرقابة على الأمن السيبراني من المفاهيم التي تطورت مع تطور التكنولوجيا والاعتماد المتزايد على الأنظمة الرقمية. في بدايات القرن الحادي والعشرين، ومع تزايد الهجمات الإلكترونية وتعقيدها، برزت الحاجة إلى تعزيز الرقابة على الأمن السيبراني لحماية المعلومات والأنظمة من التهديدات المتنوعة. يشمل هذا المفهوم مجموعة من الإجراءات والتدابير التي تهدف إلى حماية الأنظمة والشبكات من الوصول غير المصرح به، وضمان سرية وسلامة البيانات.

يشير مفهوم إدارة المخاطر المالية إلى العمليات التي تهدف إلى تحديد وتقييم ومراقبة المخاطر التي قد تؤثر على الأصول والأرباح المالية للمؤسسات. تطورت هذه الممارسات بشكل ملحوظ منذ العصور الوسطى، حيث بدأت المؤسسات في تطوير استراتيجيات للتعامل مع المخاطر المالية الناجمة عن التغيرات الاقتصادية والتجارية. مع الثورة الصناعية، ازدادت تعقيدات الأسواق المالية، مما استدعى تطوير أدوات ومنهجيات أكثر تطورًا لإدارة هذه المخاطر.

بناءً على ما سبق، تسعى هذه الدراسة إلى استكشاف دور تعزيز الرقابة على الأمن السيبراني في تحسين إدارة المخاطر المالية، مع التركيز على مؤسسات الضمان الاجتماعي في السودان. تهدف الدراسة إلى تقديم توصيات عملية لتعزيز الأمن السيبراني، مما يسهم في تقليل المخاطر المالية المحتملة في هذه المؤسسات.

مشكلة الدراسة:

تتجلى مشكلة الدراسة في التحديات التي تواجهها مؤسسات الضمان الاجتماعي في السودان نتيجة للمخاطر المالية المتزايدة، والتي قد تنجم عن الهجمات الإلكترونية أو الثغرات في أنظمة الأمن السيبراني. تاريخيًا، شهدت العديد من المؤسسات المالية حول العالم خسائر كبيرة بسبب الاختراقات الأمنية، مما أثر سلبًا على استقرارها المالي وسمعتها. في هذا السياق، يبرز التساؤل الرئيسي: كيف يمكن لتعزيز الرقابة على الأمن السيبراني أن يسهم في تحسين إدارة المخاطر المالية في مؤسسات الضمان الاجتماعي بالسودان؟

أهمية الدراسة:

تنبع الأهمية العلمية لهذه الدراسة من الحاجة إلى سد الفجوة المعرفية المتعلقة بتأثير تعزيز الرقابة على الأمن السيبراني في إدارة المخاطر المالية، خاصة في سياق مؤسسات الضمان الاجتماعي في السودان. من خلال تحليل هذا التأثير، تسهم الدراسة في إثراء الأدبيات الأكاديمية وتقديم إطار نظري يمكن الاستفادة منه في دراسات مستقبلية.

تتجلى الأهمية العملية في تقديم توصيات وإجراءات قابلة للتطبيق لمؤسسات الضمان الاجتماعي في السودان، بهدف تعزيز أنظمتها الأمنية وتقليل المخاطر المالية المحتملة. من خلال تطبيق هذه التوصيات، يمكن للمؤسسات تحسين كفاءتها التشغيلية وضمان استدامتها المالية.

أهداف الدراسة:

1. تحليل مفهوم الرقابة على الأمن السيبراني وتطوره التاريخي.
2. دراسة ممارسات إدارة المخاطر المالية في مؤسسات الضمان الاجتماعي.
3. تقييم العلاقة بين تعزيز الرقابة على الأمن السيبراني وإدارة المخاطر المالية في مؤسسات الضمان الاجتماعي بالسودان.

منهجية الدراسة:

تم الاعتماد على الاستبانة الإلكترونية كأداة رئيسية لجمع البيانات من موظفي مؤسسات الضمان الاجتماعي في السودان. تم تحليل البيانات باستخدام برنامج SPSS لإجراء التحليلات الإحصائية اللازمة، مما يساعد في اختبار فرضيات الدراسة واستخلاص النتائج.

فرضية الدراسة:

توجد علاقة ذات دلالة إحصائية بين تعزيز الرقابة على الأمن السيبراني وإدارة المخاطر المالية في مؤسسات الضمان الاجتماعي.

حدود الدراسة:

1. الحدود الزمانية :عام 2025.
2. الحدود المكانية :مؤسسات الضمان الاجتماعي في السودان.
3. الحدود البشرية :موظفو مؤسسات الضمان الاجتماعي في السودان.
4. الحدود الموضوعية :دراسة العلاقة بين تعزيز الرقابة على الأمن السيبراني وإدارة المخاطر المالية.

مصادر جمع البيانات:

1. مصادر جمع البيانات الأولية :الاستبانة الإلكترونية الموجهة لموظفي مؤسسات الضمان الاجتماعي.
2. مصادر جمع البيانات الثانوية :الكتب، المقالات العلمية، والرسائل الجامعية ذات الصلة بموضوع الدراسة.

الدراسات السابقة

Quinn et al. (2022):

هدفت الدراسة إلى وصف كيفية دمج معلومات مخاطر الأمن السيبراني المسجلة (CSRRs) ضمن نَهج إدارة مخاطر المؤسسة الشامل (ERM) لضمان أخذ المخاطر التي تهدد المعلومات والتكنولوجيا في الاعتبار بشكل صحيح في محفظة المخاطر الكلية للمؤسسة. وتوصلت الدراسة إلى أن هذا الدمج يُحقق فهمًا متماسكًا لمخاطر الأمن السيبراني يدعم بشكل مباشر سجل مخاطر المؤسسة (ERR) وملف تعريف المخاطر(ERP) ، مما يدعم بدوره تحقيق أهداف المؤسسة بشكل أكثر فعالية.

Lowry et al. (2025):

هدفت الدراسة إلى تحليل فاعلية مجالس الإدارة في الإشراف على مخاطر الأمن السيبراني في ظل محدودية الخبرة بين أعضائها. وتوصلت النتائج إلى أن جهود الأعضاء غير المتخصصين تبقى رمزية دون فعالية حقيقية على الرغم من نواياهم الجادة، بينما يدرك الخبراء بوضوح هذه الفجوة ويدعون إلى زيادة التعيينات المتخصصة. كما أظهرت الدراسة أن غير المتخصصين لا يدركون طبيعة جهودهم الرمزية، مما يفسر عدم تأكيد تعيين خبراء متخصصين في المجالس.تؤكد النتائج على أهمية الخبرة التخصصية لتحويل الإشراف من رمزي إلى جوهري.

Kanyongo & Wadesango (2025):

هدفت الدراسة إلى تحليل تأثير الأمن السيبراني على استراتيجيات تخفيف المخاطر في البنوك التجارية بالأسواق الناشئة، مع التركيز على تحديد العلاقة بين الفضاء السيبراني والتهديدات الإلكترونية، وتشخيص التحديات والمقترحات العلاجية. وتوصلت النتائج إلى أن أهم المخاطر تشمل التصيد الإلكتروني والاختراق والاحتيال المحاسبي الداخلي، فيما تمثلت

التحديات الرئيسية في ضعف الإشراف الإداري، ونقص تشفير البيانات، والاعتماد على خدمات الطرف الثالث، وغياب المعايير الوطنية البنية التحتية اللازمة. وأوصت الدراسة بضرورة تعزيز الرقابة على موظفي البنوك، وإجراء عمليات تدقيق منتظمة، ورفع وعي العملاء، وتطبيق إجراءات تقنية متقدمة مثل المصادقة المتعددة العوامل وجدران الحماية القوية.

Opdenbusch et al. (2025):

هدفت الدراسة إلى تحليل كيفية قيام مجالس الإدارة باتخاذ القرارات المتعلقة بمخاطر الأمن السيبراني بعد تلقي المعلومات من الجهات المعنية، وكيف تؤثر علاقاتهم مع أصحاب المصلحة في تلك القرارات. وتوصلت النتائج إلى وجود خلل في موازين القوة حيث يمتنع أعضاء المجالس عن طرح الأسئلة المناسبة على المديرين التنفيذيين ومسؤولي الأمن المعلوماتي خوفاً من أن يُكشف عن محدودية معرفتهم التقنية، مما يجعلهم يعتمدون بشكل كامل على مقدمي المعلومات ويفقدون دورهم الرقابي. كما كشفت النتائج أن المخاطر السيبرانية يتم اختزالها في قرارات الميزانية دون مشاركة حقيقية في الاستراتيجيات الأمنية

Metibemu (2025):

هدفت الدراسة إلى تحليل إدارة المخاطر المالية في البنوك الرقمية الخالصة من خلال فحص تهديدات الاحتيال والأمن السيبراني باستخدام منهجيات كمية. وتوصلت النتائج إلى أن التصيد الاحتيالي (35٪) وبرامج الفدية (20٪) يتسببان في أعلى الخسائر المالية بمتوسط 5.5 مليون و7.1 مليون دولار لكل حادثة على التوالي، بينما يقلل الامتثال لمعايير بازل الثالث من مخاطر الاحتيال بشكل كبير. كما أظهرت النتائج أن البنوك الخاضعة لتنظيم صارم حققت انخفاضاً أكبر بنسبة 1.90٪ في حالات الاحتيال، بينما لم تظهر أنظمة المراقبة المدعومة بالذكاء الاصطناعي الكفاءة المطلوبة.

على الرغم من مساهمة الدراسات السابقة في فهم إدارة المخاطر السيبرانية من زوايا متعددة – كدراسة (Quinn et al., 2022)لدمجها في إدارة مخاطر المؤسسة، و (Lowry et al., 2025) و (Opdenbusch et al., 2025)لتحليل إشراف المجالس وضعف الخبرة، و (Kanyongo & Wadesango, 2025)و (Metibemu, 2025)لمعالجة التهديدات في القطاع المصرفي – إلا أنها تركز بشكل رئيسي على القطاع المصرفي والسياقات المتقدمة، وتغفل عن قطاع مؤسسات الضمان الاجتماعي في الأسواق الناشئة. هنا تكمن فجوة البحث التي تملأها دراسة الباحثان، حيث تتميز بالتركيز على هذا القطاع الحيوي غير المستكشف في السودان، مع التحقق من علاقة سببية مباشرة بين تعزيز الرقابة السيبرانية وفاعلية إدارة المخاطر المالية، مما يضيف بُعداً تطبيقياً وسياقياً فريداً يتجاوز الدراسات السابقة التي اهتمت بالتحليل الوصفي أو العام.

1-الإطار النظري

1-1الرقابة على الأمن السيبراني

مع تزايد الاعتماد على التكنولوجيا الرقمية والتحول الرقمي في مختلف القطاعات، أصبح الأمن السيبراني من الأولويات الأساسية لتحقيق الاستقرار المؤسسي وحماية البيانات الحساسة. ترتكز الرقابة على الأمن السيبراني على مجموعة من الإجراءات والتقنيات التي تهدف إلى تقليل المخاطر السيبرانية وتأمين البنية التحتية الرقمية، مما يعزز ثقة العملاء ويحسن

الأداء المؤسسي. لذا، يتناول الباحثان، تعزيز الرقابة على الأمن السيبراني كركيزة أساسية لحماية المؤسسات وضمان استمرارية وفعالية العمليات الرقمية، كما يلي:

1-1-1أهمية الأمن السيبراني ودوره في تعزيز الرقابة

الأمن السيبراني يمثل أحد الركائز الأساسية لضمان استمرارية العمليات المؤسسية وحماية البيانات الحساسة من التهديدات المتزايدة التي تواجهها الأنظمة الرقمية. الرقابة السيبرانية تعتمد على مجموعة من الأدوات التنظيمية والإدارية التي تهدف إلى تقليل المخاطر وتعزيز سلامة البنية التحتية الرقمية. تتطلب هذه الرقابة تطوير استراتيجيات فعالة تمكن المؤسسات من التصدي للهجمات السيبرانية، بما في ذلك تحسين نظم المراقبة الإلكترونية وتبني سياسات واضحة لتأمين المعلومات (AbdelSalam, 2022).

1-1-2الرقابة السيبرانية وتأثيرها على الأداء المؤسسي وثقة العملاء

تعزيز الرقابة على الأمن السيبراني يسهم بشكل كبير في تحسين الأداء المؤسسي، حيث ينعكس ذلك على استقرار العمليات الرقمية وموثوقيتها. المؤسسات التي تطبق استراتيجيات رقابة سيبرانية فعالة تتمكن من تعزيز ثقة العملاء، مما يزيد من ولائهم ويقلل من المخاطر المرتبطة بالتعاملات الرقمية. كما أن تطبيق أنظمة رقابية متطورة يساعد في تحسين الكفاءة التشغيلية وتقليل الاختراقات الأمنية التي قد تؤثر على سمعة المؤسسات وأدائها (Sundas Ali Khalifa, 2025).

1-1-3تحديات تعزيز الرقابة على الأمن السيبراني

تعاني المؤسسات من تحديات متعددة في تطبيق الرقابة السيبرانية، من أبرزها نقص الكوادر المؤهلة وضعف البنية التحتية التقنية في بعض الحالات. هذه التحديات تجعل من الصعب تبني أنظمة رقابية متكاملة وقادرة على مواجهة الهجمات السيبرانية المتطورة. ومع ذلك، فإن تبني تقنيات حديثة مثل الذكاء الاصطناعي وتحليل البيانات يسهم في تحسين قدرة المؤسسات على التنبؤ بالتهديدات ومعالجتها في وقت مناسب.(M.M. Saja Fadel Abbas, 2024)

1-1-4 دور التكنولوجيا والتدريب في تعزيز الرقابة السيبرانية

التكنولوجيا الحديثة تعد أداة أساسية في دعم الرقابة السيبرانية، حيث تساعد في تحسين عملية مراقبة الأنظمة الرقمية واكتشاف التهديدات بشكل استباقي. من جهة أخرى، يلعب التدريب دورًا محوريًا في تعزيز مهارات العاملين في المجال السيبراني وتمكينهم من التعامل مع التحديات المتزايدة. تطوير الكوادر البشرية المؤهلة يعتبر جزءًا لا يتجزأ من استراتيجيات الأمن السيبراني، حيث يساهم بشكل مباشر في تنفيذ الخطط الرقابية بفعالية (سالم وآخرون, 2024).

1-1-5 أثر الإنفاق على الأمن السيبراني في تعزيز الرقابة

الاستثمار في الأمن السيبراني يعد ضرورة لضمان كفاءة الأنظمة الرقمية وتقليل التهديدات المحتملة. الإنفاق على تطوير أدوات الرقابة السيبرانية يعزز من قدرة المؤسسات على حماية بياناتها ودعم استقرار عملياتها. بالإضافة إلى ذلك، يؤدي الاستثمار في البنية التحتية التقنية إلى تحسين العمليات التشغيلية وتقليل الخسائر الناتجة عن الاختراقات الأمنية، مما يدعم الأداء المؤسسي بشكل عام (أبو الفضل, 2024؛ الفضل, 2024).

1-1-6 البعد القانوني والتنظيمي للرقابة السيبرانية

يتطلب تعزيز الرقابة على الأمن السيبراني وجود إطار قانوني وتنظيمي يدعم المؤسسات في مواجهة التهديدات السيبرانية. القوانين والسياسات التي تنظم استخدام الأنظمة الرقمية وحمايتها تعد عنصراً مهماً لتقليل المخاطر وتحقيق الامتثال للمعايير الدولية. كما أن التعاون بين الأطراف المعنية يعزز من تطبيق هذه القوانين ويؤدي إلى بناء بيئة سيبرانية آمنة ومستدامة (Widen, 2023؛ Edwards, 2019).

1-1-7 أهمية الحوكمة الرقمية في دعم الأمن السيبراني

تعتبر الحوكمة الرقمية أحد العوامل المهمة في تعزيز الرقابة السيبرانية، حيث تضمن وجود خطط واستراتيجيات واضحة لإدارة المخاطر الرقمية. الحوكمة الفعالة تمكن المؤسسات من تنسيق الجهود بين الإدارات المختلفة، مما يسهم في تحسين قدرة الأنظمة الرقمية على التعامل مع التهديدات بشكل كفؤ. كما أن الحوكمة تدعم تطبيق أفضل الممارسات لضمان استمرارية العمليات الرقمية وحمايتها من المخاطر المحتملة (السيد, 2024).

1-2 إدارة المخاطر المالية

تشكل إدارة المخاطر المالية عملية منهجية لتحديد وقياس ومعالجة مصادر المخاطر وآثارها المالية على المنشآت، بهدف تمكينها من تحقيق أهدافها بكفاءة وفعالية أعلى (محمد علي، 2005). تتسع أبعاد هذه الإدارة لتشمل عدة أنواع، أبرزها المخاطر الائتمانية ومخاطر السيولة ومخاطر السوق.

1-2-1 إدارة المخاطر الائتمانية

تركز الإدارة الفعالة للمخاطر الائتمانية على ضرورة قيام المصرف بتقييم شامل للمقترضين المحتملين قبل منح التمويل، من خلال تطبيق إجراءات "الحرص الواجب (Customer Due Diligence) "للتعرف على ملاءتهم المالية وسمعتهم وتاريخهم السابق في السداد والوضع القانوني لهم وطبيعة نشاطهم (بنك السودان المركزي، 2010). يجب أن يتجاوز التقييم الاعتماد على السمعة أو المركز المالي للعميل ليشمل الاعتماد الأساسي على جدوى المشروع وربحيته المتوقعة وتدفقاته النقدية كمصدر للسداد (بنك السودان المركزي، 2010). كما تشمل الممارسات السليمة وضع أنظمة لتصنيف العملاء وتجنب مخاطر التركيز، وتحليل العائد مقابل المخاطرة، وتكوين مخصصات كافية، وتقييم الضمانات تقييماً حقيقياً من قبل جهات متخصصة مع التأكد من سيولتها وخلوها من العوائق القانونية، على أن لا يكون الاعتماد عليها مبالغاً فيه (بنك السودان المركزي، 2010؛ صالح، 2020). وتقتضي الإدارة المتكاملة متابعة مستمرة للمخاطر من خلال مراقبة المركز المالي للعميل والظروف المحيطة بنشاطه وسير حسابه، والمتابعة الدورية للضمانات وتقييم قيمتها السوقية (نادر الفاتح صالح، 2020). ويشمل ذلك أيضاً إنشاء وحدة متخصصة لمعالجة التمويل المتعثر والتفاوض مع العملاء وإعداد خطط استراتيجية لإعادة الجدولة، إلى جانب المراجعة المستمرة لتصنيفات الائتمان وبناء المخصصات بما يتوافق مع توجيهات البنك المركزي.

1-2-2 إدارة مخاطر السيولة

تُعرف مخاطر السيولة بأنها الخسائر الناجمة عن عدم قدرة المصرف على الوفاء بالتزاماته المستحقة بسبب سحوبات الودائع المفاجئة أو انخفاض التدفقات النقدية غير المتوقع، وهي من المخاطر الجوهرية التي تهدد استقرار القطاع المصرفي (محسن ، 2019). وتتطلب إدارتها وضع سياسات وإستراتيجيات معتمدة من مجلس الإدارة تركز على ضمان سيولة كافية لمقابلة الالتزامات، ووضع خطط طوارئ لإدارة الأزمات، وتنويع مصادر الأموال (السيسي، 2000). وتشمل الإجراءات

العملية إجراء تحليلات دورية للتدفقات النقدية الداخلة والخارجة ومواعيد استحقاق الأصول والخصوم (فجوة الاستحقاقات) لتحديد العجز أو الفائض السيولي (محسن ، 2019). كما يجب مراقبة هيكل الودائع ومصادر التمويل ومراجعة نسب السيولة دورياً. إلى جانب العوامل الكمية، يجب مراعاة العوامل النوعية مثل كفاءة إدارة الخزينة، ونوعية نظم المعلومات، وسمعة المصرف، وقدرة المساهمين على تقديم الدعم المالي عند الحاجة (السيسي، 2000).

3-2-1 إدارة مخاطر السوق

تشير مخاطر السوق إلى الخسائر المحتملة الناشئة عن التقلبات في القيم السوقية للأصول بسبب تغيرات في أسعار السوق، مثل أسعار الفائدة وأسعار الصرف وأسعار الأوراق المالية والسلع (قندوز، 2018) لإدارة هذه المخاطر، يجب على المصرف تحديد أنواعها وقياسها بدقة باستخدام نماذج قياسية مثل نموذج القيمة المعرضة للخطر - (Value at Risk VaR)أو طريقة التسعير إلى السوق (Mark to Market - MTM) والتي تقيس الأرباح والخسائر المحتملة بناءً على التقلبات السوقية (قندوز، 2018). وتقتضي المتابعة الفعالة وجود نظام قوي للإبلاغ يرصد حجم التعرض للمخاطر ومستوى الالتزام بالسياسات والسقوف المحددة (مثل سقوف التعامل بالنقد الأجنبي). وأخيراً، يتطلب التحكم الفعال في هذه المخاطر وجود نظام رقابي داخلي قوي يحدد الصلاحيات والمسؤوليات بوضوح، ونظام مراجعة مستقلة للتحقق من دقة نماذج القياس وصحة البيانات والسيناريوهات المستخدمة (جي روتيد، 2020).

3-1 تعزيز الرقابة على الأمن السيبراني وتقليل المخاطر المالية

تعزيز الرقابة على الأمن السيبراني يمثل دوراً مهماً في إدارة المخاطر المالية، حيث ترتبط المخاطر المالية في العصر الرقمي ارتباطاً وثيقاً بالتهديدات السيبرانية التي قد تؤثر على استقرار المؤسسات وأدائها المالي. إدارة هذه المخاطر تتطلب تبني استراتيجيات رقابة متقدمة تعزز من حماية البيانات والمعلومات الحساسة، مما يقلل من احتمالية وقوع اختراقات تؤثر على الثقة المؤسسية والمالية. الإفصاح عن تقارير إدارة مخاطر الأمن السيبراني يعزز من جودة التقارير المالية ويسهم في تحسين شفافية العمليات، حيث تشير الدراسات إلى أن الإفصاح الواضح عن المخاطر السيبرانية يؤثر إيجاباً على قيمة المنشآت من خلال تعزيز الثقة بين المستثمرين وأصحاب المصلحة (عبدالحكيم وآخرون، 2025).

تعتمد إدارة المخاطر المالية المرتبطة بالأمن السيبراني على برامج متخصصة تعمل على تقييم التهديدات المحتملة ووضع آليات استجابة فعالة. هذه البرامج لا تسهم فقط في تقليل الخسائر الناتجة عن الهجمات السيبرانية، بل تعزز أيضاً من جودة المعلومات المحاسبية، مما يجعل المؤسسات أكثر جاذبية للمستثمرين غير المباشرين. في هذا السياق، يعتبر قطاع الاتصالات مثالاً واضحاً على أهمية تعزيز الرقابة السيبرانية في دعم الاستثمارات، حيث أثبتت الدراسات أن المؤسسات التي تطبق برامج فعالة لإدارة مخاطر الأمن السيبراني تكون أكثر قدرة على جذب رؤوس الأموال وتحقيق استدامة مالية أعلى (رشا وعلي، 2024).

وعي العملاء بالتهديدات السيبرانية يعد عاملاً أساسياً في إدارة المخاطر المالية وتحقيق الأمن السيبراني. المؤسسات التي تقوم بتوعية عملائها بالمخاطر السيبرانية وكيفية التعامل معها تتمكن من تقليل احتمالية وقوع اختراقات تؤثر على بيانات العملاء وأنظمتهم المالية. هذا الوعي يسهم في تعزيز الثقة بين العملاء والمؤسسات، خاصة في القطاع المصرفي، حيث تعتبر الثقة أحد العوامل المحورية التي تؤثر على استقرار الأداء المالي للمؤسسات. من جهة أخرى، تعد

القرصنة الإلكترونية من أبرز التهديدات التي تواجه المؤسسات المالية، مما يجعل الرقابة على الأمن السيبراني ضرورة استراتيجية لتقليل المخاطر المالية المرتبطة بها (التوني، 2023).

تؤثر حوادث الأمن السيبراني بشكل مباشر على استقرار المؤسسات وأدائها المالي، حيث تتسبب الاختراقات السيبرانية في خسائر مالية كبيرة قد تؤثر على سمعة المؤسسات وعلاقاتها مع المستثمرين. خبرة مراقبي الحسابات تلعب دوراً مهماً في تقليل تأثير هذه الحوادث من خلال تطبيق إجراءات رقابية تضمن حماية البيانات وتقليل المخاطر المالية. المؤسسات التي تعتمد على مراقبي حسابات ذوي خبرة في مجال الأمن السيبراني تكون أكثر قدرة على التعامل مع التهديدات السيبرانية بفعالية، مما يعزز من كفاءة إدارة المخاطر المالية في المؤسسات المقيدة بالبورصات (طلبة، 2024).

2-الدراسة الميدانية:

2-1وصف مجتمع وعينة الدراسة :

2-1-1 مجتمع الدراسة

يتكوَّن مجتمع الدراسة من العاملين في مؤسسات الضمان الاجتماعي، ويشمل فئات مهنية متعددة تتمثل في: المحاسبين، ورؤساء الأقسام، ورؤساء أقسام الحسابات، ومديري ورؤساء وأعضاء فرق المراجعة الداخلية، بالإضافة إلى فئات وظيفية أخرى ذات صلة. يمثل هذا التنوع المهني قاعدة بيانات غنية وشاملة تعكس تجارب وآراء الممارسين المهنيين بشكل مباشر، مما يضمن تغطية جوانب البحث المتعلقة بالرقابة الداخلية وإدارة المخاطر وتقويم الأداء المالي من وجهات نظر متخصصة ومتنوعة.

2-1-2 عينة الدراسة وخصائصها :

تم اختيار عينة البحث بالاعتماد على أسلوب العينة العشوائية، حيث تم توزيع (150) استبانة إلكترونية شملت جميع الفئات الوظيفية المستهدفة في مجتمع الدراسة. وقد أسفرت عملية جمع البيانات عن استرجاع (140) استبانة صالحة للتحليل

2-2 الأساليب الإحصائية المستخدمة في الدراسة

بعد جمع البيانات من خلال الاستبيان، تم معالجتها وتحليلها إحصائياً باستخدام الحزمة الإحصائية للعلوم الاجتماعية (SPSS)لتحقيق أهداف الدراسة واختبار فرضياتها. لضمان جودة القياس، تم التحقق من **صدق** الأداة بعرضها على محكمين أكاديميين، ومن **ثباتها** بحساب معامل كرونباخ ألفا الذي تجاوز القيمة المعيارية (0.60). لوصف عينة الدراسة، استُخدمت **أساليب الإحصاء الوصفي** كالتكرارات والنسب المئوية والمتوسطات الحسابية والانحراف المعياري. ولاختبار الفرضيات، طُبق **التحليل الاستدلالي** عبر أسلوب الانحدار الخطي البسيط لفحص تأثير المتغير المستقل على التابع.

جدول(1)معامل الثبات (طريقة الفا كرونباخ)

المحاور	عدد	الثبات	المصداقية
البعد المحور الأول: تعزيز الرقابة على الأمن السيبراني	6	.878	0.937
المحور الثاني: إدارة المخاطر المالية	10	.880	0.938
جميع المحاور	**44**	**.905**	**0.951**

المصدر: إعداد الباحثان، الدراسة الميدانية، 2025م

بناءً على نتائج تحليل الثبات الموضحة في الجدول (1)، أظهرت الأداة البحثية مستويات ثبات ومصداقية عالية جداً. حيث بلغ معامل ألفا كرونباخ للمحور الأول (تعزيز الرقابة على الأمن السيبراني) 0.878، وللمحور الثاني (إدارة المخاطر المالية) 0.880، مما يشير إلى اتساق داخلي ممتاز لفقرات كل محور على حدة. أما معامل الثبات الكلي لجميع محاور الاستبانة البالغ عددها 44 فقرة، فقد بلغ 0.905، وهي قيمة عالية جداً تؤكد موثوقية الأداة ككل وملاءمتها للبحث العلمي. كما أن قيم معاملات المصداقية (0.937، 0.938، 0.951 على التوالي) تعزز من درجة الثقة في صدق النتائج وقدرة الأداة على قياس ما صُممت لقياسه بدقة، مما يضفي مصداقية وقوة على التحليلات والاستنتاجات المستخلصة من البيانات التي جُمِعَت بواسطتها.

3-2 تحليل البيانات الشخصية:

اشتملت على الخصائص التالية : التخصص العلمي، المؤهل العلمي، المسمى الوظيفي، سنوات الخبرة، وفيما يلي التوزيع التكراري لإجابات الوحدات المبحوثة والذي يعكس الخصائص الأولية لعينة الدراسة:

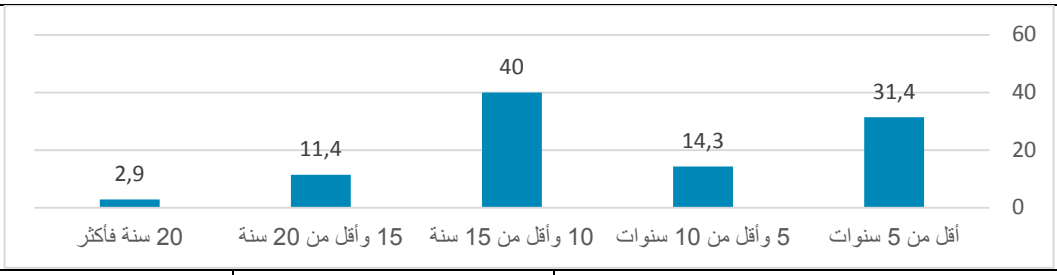
جدول(2) التوزيع التكراري لإفراد عينة الدراسة وفق التخصص العلمي

التخصص العلمي	التكرار	النسبة%
المحاسبة	68,6	
الدراسات المالية والمصرفية	7,1	
نظم المعلومات المحاسبية	2,9	
ادارة الاعمال	17,1	
الاقتصاد	4,3	
المجموع	140	100.0

المؤهل العلمي	التكرار	النسبة%
بكلاريوس	52,9	
دبلوم عالي	8,6	
ماجستير	25,7	
دكتوراة	10	
أخرى	2,9	
المجموع	140	100.0

المسمى الوظيفي	التكرار	النسبة%
محاسب	50	
مدير إدارة مراجعة داخلية	2,9	
رئيس فريق مراجعة داخلية	8,6	
عضو فريق مراجعة داخلية	2,9	
رئيس قسم	4,3	
رئيس قسم حسابات	7,1	
أخرى	24,3	
المجموع	140	100.0

سنوات الخبرة	التكرار	النسبة%

سنوات الخبرة			
المجموع	140	100	

المصدر: إعداد الباحثين، من بيانات الدراسة الميدانية، 2025م

يظهر الجدول (2) التوزيع التكراري لأفراد عينة الدراسة وفقًا للبيانات الشخصية، حيث يُلاحظ أن عينة البحث تتكون بشكل أساسي من مختصين في المجال المالي والمحاسبي (82.9%)، حيث مثل المحاسبون النسبة الأكبر (68.6%)، مع وجود تمثيل لتخصصات إدارة الأعمال والدراسات المالية والاقتصاد. كما أظهرت النتائج تمتع العينة بمستوى تعليمي عالٍ، حيث حمل 88.6% من أفرادها مؤهلات جامعية (بكالوريوس فما فوق). من الناحية الوظيفية، مثل العاملون في المجالات المحاسبية والرقابية والإشرافية 75.7% من العينة، مع تركيز على شاغلي وظيفة "محاسب" (50%). فيما يتعلق بالخبرة العملية، امتلك 54.3% من أفراد العينة خبرة تزيد عن 10 سنوات، مما يعكس عمق الخبرة والمعرفة العملية الكافية. يستنتج الباحثون أن هذه الخصائص تضفي مصداقية وقوة على استجابات العينة وتعزز موثوقية النتائج المتعلقة بتقييم محاور الدراسة المعقدة.

4-2 تحليل البيانات الأساسية:

1-4-2 التوزيع التكراري والنسبة المئوية لعبارات المحاور:

يهدف هذا التحليل إلى استعراض آراء أفراد عينة الدراسة حول محاور البحث الرئيسية، من خلال عرض التكرارات والنسب المئوية لدرجات الموافقة على كل عبارة من عبارات الاستبيان. يُعد هذا التحليل الأساس الأولي لفهم اتجاهات العينة وتصورها العام تجاه ممارسات الرقابة الداخلية المعاصرة وإدارة المخاطر المالية وتقويم الأداء.

المحور الأول: تعزيز الرقابة على الامن السيبراني

جدول(3)التوزيع التكراري والنسبة المئوية لعبارات المحور الأول

العبارات	ت	مستوي الموافقة				
	%	أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة
1 نعمل على تطوير سياسات رقابية تضمن حماية البيانات الحساسة.	ت	70	70	0	0	0
	%	50.0	50.0	0	0	0
2 نسعى لمراقبة الأنظمة التكنولوجية بشكل مستمر ضد التهديدات السيبرانية.	ت	80	42	18	0	0
	%	57.1	30.0	12.9	0	0
3 نقوم بتدريب الموظفين على التعامل مع التهديدات الإلكترونية المحتملة.	ت	66	62	4	8	0
	%	47.1	44.3	2.9	5.7	0
4 نحرص على استخدام أدوات متقدمة لضمان	ت	70	58	8	4	0

أمان الشبكات الداخلية.	%	50.0	41.4	5.7	2.9	0
5 نعمل على تحديث أنظمة الأمن السيبراني بانتظام	ت	76	38	22	4	0
	%	54.3	27.1	15.7	2.9	0
6 نسعى لتعزيز الوعي المؤسسي بأهمية الأمن السيبراني	ت	74	36	22	8	0
	%	52.9	25.7	15.7	5.7	0

المصدر: إعداد الباحثين، من بيانات الدراسة الميدانية، 2025م

يظهر الجدول (3) نتائج التوزيع التكراري والنسبة المئوية لاستجابات عينة الدراسة حول محور تعزيز الرقابة على الأمن السيبراني، حيث تُظهر النتائج وجود اتجاه إيجابي وقوي لدى أفراد العينة نحو جميع عبارات هذا المحور. فقد حظيت جميع العبارات على موافقة عالية، حيث تجاوزت نسبة الموافقة (أوافق + أوافق بشدة) على جميع العبارات حاجز 90%، مع ملاحظة أن العبارة الأولى "نعمل على تطوير سياسات رقابية تضمن حماية البيانات الحساسة" سجلت أعلى مستوى موافقة بنسبة 100%، بينما سجلت العبارة الثالثة "نقوم بتدريب الموظفين على التعامل مع التهديدات الإلكترونية المحتملة" أدنى نسبة موافقة نسبياً لكنها ظلت عالية جداً بلغت 91.4%. كما يُلاحظ انخفاض ملحوظ في نسب الحياد وعدم الموافقة على جميع العبارات، مما يعكس إدراكاً واضحاً واقتناعاً كبيراً بأهمية تطبيق ممارسات الرقابة على الأمن السيبراني في بيئة العمل.

المحور الثاني : إدارة المخاطر المالية

جدول(4)التوزيع التكراري والنسبة المئوية لعبارات المحور الثاني

العبارات	ت	مستوي الموافقة				
	%	أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة
1. تقييم حالات العسر المالي خاصة فيما يتعلق بالتدفقات النقدية.	ت	52	68	16	4	0
	%	37.1	48.6	11.4	2.9	0
2. تفادي مخاطر راس المال وامتصاص الخسائر التي يمكن ان تحدث.	ت	54	78	8	0	0
	%	38.6	55.7	5.7	0	0
3. ضمان حقوق المودعين والدائنين.	ت	50	90	0	0	0
	%	35.7	64.3	0	0	0
4. التأكد من تطبيق الإجراءات والسياسات التي تحد من المخاطر المالية	ت	76	60	4	0	0
	%	54.3	42.9	2.9	0	0
5. قياس حجم المخاطر باستخدام المقاييس المالية والإحصائية اللازمة.	ت	50	90	0	0	0
	%	35.7	64.3	0	0	0
6. يتم وضع خطة واضحة لإدارة المخاطر تتضمن رقابة فعالة للمخاطر	ت	66	66	4	4	0
	%	47.1	47.1	2.9	2.9	0
7. تخفيض درجة عدم التأكد للحد من المخاطر المالية لتكون في ادنى الحدود الممكنة.	ت	56	60	14	10	0
	%	40.0	42.9	10.0	7.1	0
8. تحديد وقياس المخاطر المالية التي تتعرض لها	ت	66	64	10	0	0
	%	47.1	45.7	7.1	0	0

المنشاة للحد من الأثار المترتبة عليها.						
9. تقييم حجم المخاطر الناجمة من قرار منح التمويل	ت	72	44	20	4	0
	%	51.4	31.4	14.3	2.9	0
10. التأكد من فاعلية نظم إدخال البيانات للتقليل من المخاطر.	ت	72	68	0	0	0
	%	51.4	48.6	0	0	0

المصدر: إعداد الباحثين ، من بيانات الدراسة الميدانية، 2025م

يظهر الجدول (4) نتائج التوزيع التكراري والنسب المئوية لاستجابات عينة الدراسة حول محور "إدارة المخاطر المالية"، حيث أظهرت النتائج وجود موافقة عالية جداً من قبل المبحوثين على جميع العبارات التي تقيس ممارسات إدارة المخاطر، حيث تجاوزت نسبة الموافقة (أوافق + أوافق بشدة) 90% في خمس عبارات رئيسية، وهي: "ضمان حقوق المودعين والدائنين" (100%)، و"قياس حجم المخاطر باستخدام المقاييس المالية والإحصائية اللازمة" (100%)، و"التأكد من فاعلية نظم إدخال البيانات للتقليل من المخاطر" (100%)، و"التأكد من تطبيق الإجراءات والسياسات التي تحد من المخاطر المالية" (97.2%)، و"تفادي مخاطر رأس المال وامتصاص الخسائر" (94.3%). كما أظهرت النتائج موافقة قوية على العبارات المتعلقة بوضع خطط واضحة لإدارة المخاطر (94.2%) وتحديد وقياس المخاطر المالية (92.8%)، بينما سجلت عبارة "تخفيض درجة عدم التأكد" أدنى نسبة موافقة بين العبارات، وإن كانت لا تزال مرتفعة (82.9%).

يستنتج الباحثان أن هذه النتائج تؤكد على وجود وعي وإدراك كبيرين في مؤسسات الضمان الاجتماعي لأهمية ودور ممارسات إدارة المخاطر المالية المتكاملة والشاملة، بدءاً من مرحلة التحديد والقياس ووصولاً إلى المراقبة والتحكم، مع تركيز واضح على حماية حقوق الأطراف ذات المصلحة واعتماد أساليب كمية في قياس المخاطر، مما ينعكس إيجاباً على تقويم الأداء المالي وتحقيق الاستقرار المالي.

2-4-2 الإحصاءات الوصفية لعبارات المحاور:

يهدف هذا التحليل إلى قياس اتجاه أفراد عينة الدراسة ودرجة تجانس آرائهم حول محاور البحث، من خلال حساب المتوسطات الحسابية والانحرافات المعيارية والأوزان النسبية لكل عبارة. يُعد هذا التحليل أساساً مهماً لتقييم مستوى قبول العينة لمفاهيم الدراسة ومدى اتساق آرائها حولها.

أ–المحور الأول: تعزيز الرقابة على الامن السيبراني:

جدول(5)الإحصاءات الوصفية لعبارات المحور الأول

العبارات	الوسط الحسابي	الانحراف المعياري	الوزن النسبي	اتجاه العينة
1. نعمل على تطوير سياسات رقابية تضمن حماية البيانات الحساسة.	4.5	.50180	90	أوافق بشدة
2. نسعى لمراقبة الأنظمة التكنولوجية بشكل مستمر ضد التهديدات السيبرانية.	4.44	.71239	88.8	أوافق بشدة
3. نقوم بتدريب الموظفين على التعامل مع التهديدات الإلكترونية المحتملة.	4.33	.79062	86.6	أوافق بشدة

4. نحرص على استخدام أدوات متقدمة لضمان أمان الشبكات الداخلية.	4.39	.72554	87.8	أوافق بشدة
5. نعمل على تحديث أنظمة الأمن السيبراني بانتظام.	4.33	.84345	86.6	أوافق بشدة
6. نسعى لتعزيز الوعي المؤسسي بأهمية الأمن السيبراني.	4.26	.92426	85.2	أوافق بشدة
الاتجاه العام للمحور ككل	4.37	.60005	87.4	أوافق بشدة

المصدر: إعداد الباحثين ، من بيانات الدراسة الميدانية، 2025م

يظهر الجدول (5) الإحصاءات الوصفية لعبارات محور تعزيز الرقابة على الأمن السيبراني، حيث كشفت النتائج عن ارتفاع القيم المتوسطة لجميع العبارات والتي تراوحت بين (4.26 – 4.50)، مع انحراف معياري منخفض يتراوح بين (0.50 – 0.92)، مما يشير إلى تجانس واتفاق كبير بين أفراد العينة في استجاباتهم. وسجل المحور ككل وسطاً حسابياً عاماً بلغ (4.37) ووزناً نسبياً (87.4%)، مما يعكس اتجاهًا إيجابيًا قويًا نحو الموافقة بشدة على جميع ممارسات تعزيز الرقابة على الأمن السيبراني، حيث جاءت أعلى العبارات قيمةً تلك المتعلقة بتطوير سياسات رقابية لحماية البيانات الحساسة (الوسط = 4.50، الوزن النسبي = 90%)، بينما حصلت عبارة تعزيز الوعي المؤسسي على أدنى قيمة (الوسط = 4.26، الوزن النسبي = 85.2%)، مما يؤكد على أهمية هذا المحور وإجماع العينة على ضرورة تطبيقه.

المحور الثاني: إدارة المخاطر المالية

جدول(6)الإحصاءات الوصفية لعبارات المحور الثاني

العبارات	الوسط الحسابي	الانحراف المعياري	الوزن النسبي	اتجاه العينة
1. تقييم حالات العسر المالي خاصة فيما يتعلق بالتدفقات النقدية.	4.2	.75102	84	أوافق
2. تفادي مخاطر راس المال وامتصاص الخسائر التي يمكن ان تحدث.	4.33	.58078	86.6	أوافق بشدة
3. ضمان حقوق المودعين والدائنين.	4.36	.48088	87.2	أوافق بشدة
4. التأكد من تطبيق الإجراءات والسياسات التي تحد من المخاطر المالية	4.49	.65135	89.8	أوافق بشدة
5. قياس حجم المخاطر باستخدام المقاييس المالية والإحصائية اللازمة.	4.36	.48088	87.2	أوافق بشدة
6. يتم وضع خطة واضحة لإدارة المخاطر تتضمن رقابة فعالة للمخاطر	4.39	.68473	87.8	أوافق بشدة
7. تخفيض درجة عدم التأكد للحد من المخاطر المالية لتكون في ادنى الحدود الممكنة.	4.16	.87550	83.2	أوافق بشدة
8. تحديد وقياس المخاطر المالية التي تتعرض لها المنشاة للحد من الأثار المترتبة عليها.	4.33	.80861	86.6	أوافق
9. تقييم حجم المخاطر الناجمة من قرار منح التمويل	4.31	.82310	86.2	أوافق بشدة
10. التأكد من فاعلية نظم إدخال البيانات للتقليل من المخاطر.	4.51	.50159	90.2	أوافق بشدة
الاتجاه العام للمحور ككل	4.34	.47059	86.8	أوافق بشدة

المصدر: إعداد الباحثين ، من بيانات الدراسة الميدانية، 2025م

يظهر الجدول (6) الإحصاءات الوصفية لمحور "إدارة المخاطر المالية"، حيث سجل المحور ككل متوسطاً حسابياً مرتفعاً بلغ (4.34) ووزناً نسبياً (86.8%) مما يعكس اتجاه العينة نحو الموافقة القوية على ممارسات إدارة المخاطر المالية. تميزت عبارة "التأكد من فاعلية نظم إدخال البيانات للتقليل من المخاطر" بأعلى متوسط حسابي (4.51) ووزن نسبي (90.2%)، تليها عبارة "التأكد من تطبيق الإجراءات والسياسات التي تحد من المخاطر المالية" بمتوسط (4.49) ووزن نسبي (89.8%). كما أظهرت النتائج تركيزاً قوياً على الجوانب الوقائية والرقابية حيث سجلت عبارات "ضمان حقوق المودعين والدائنين" و"قياس حجم المخاطر باستخدام المقاييس المالية" و"وضع خطة واضحة لإدارة المخاطر" متوسطات مرتفعة تجاوزت .(4.33)

يستنتج الباحثين أن هذه النتائج تؤكد وجود منهجية متكاملة لإدارة المخاطر المالية في مؤسسات الضمان الاجتماعي، مع تركيز ملحوظ على آليات الرقابة الوقائية وضمان دقة النظم المعلوماتية، بينما ظهرت الحاجة لتعزيز الممارسات المتعلقة بتقييم العسر المالي وتخفيض درجة عدم التأكد والتي سجلت نسب موافقة أقل نسبياً، مما يشير إلى أهمية تطوير أدوات تنبؤية أكثر تطوراً لإدارة المخاطر المالية بشكل استباقي.

5-2 اختبار فرضية الدراسة:

توجد علاقة ذات دلالة إحصائية بين تعزيز الرقابة على الأمن السيبراني وإدارة المخاطر المالية

لاختبار صحة هذه الفرضية، تم استخدام أسلوب الانحدار الخطي البسيط لتحليل العلاقة بين متغيري الدراسة: الرقابة على الأمن السيبراني (المتغير المستقل) وإدارة المخاطر المالية (المتغير التابع).

جدول(7)نتائج تحليل الانحدار الخطي البسيط على عبارات الفرضية

نموذج الانحدار			
النموذج	معامل الارتباط	معامل التحديد	معامل التحديد المعدل
1	.536[a]	.287	.282
التباين			
	قيمة (F)		مستوي المعنوية
	55.520		.000[a]
معاملات الانحدار			
المعاملات الانحدار	قيمة المعاملات	قيمة (T)	مستوي المعنوية
الثابت	2.506	10.068	.000
تعزيز الرقابة على الأمن السيبراني	.420	7.451	.000

المصدر: إعداد الباحثين من بيانات الدراسة الميدانية 2025م.

كشف تحليل الانحدار الخطي البسيط في الجدول (7) عن وجود علاقة إيجابية قوية ودالة إحصائياً بين تعزيز الرقابة على الأمن السيبراني وإدارة المخاطر المالية، حيث بلغ معامل الارتباط (0.536) مما يشير إلى علاقة قوية وموجبة، بينما بلغ معامل التحديد (0.287) مما يعني أن تعزيز الرقابة على الأمن السيبراني يفسر ما نسبته 28.7% من التباين في إدارة المخاطر المالية. وأظهرت نتائج تحليل التباين (ANOVA) دلالة إحصائية عالية عند مستوى (0.000) بقيمة (F = 55.520)، كما أكدت معاملات الانحدار على دلالة الثابت (2.506) عند مستوى (0.000) ومعامل الانحدار لتعزيز الرقابة على الأمن السيبراني (0.420) عند مستوى دلالة (0.000) بقيمة.(T = 7.451)

بناءً على هذه النتائج الإحصائية الدالة، يمكن قبول فرضية الدراسة التي تؤكد وجود علاقة إيجابية ودالة إحصائياً بين تعزيز الرقابة على الأمن السيبراني وإدارة المخاطر المالية في مؤسسات الضمان الاجتماعي قيد الدراسة.

خاتمة: نتائج الدّراسة والتوصيات

بعد عرض الاطار النظري للدراسة وإجراء الدراسة الميدانية ، كشفت الدراسة عن نتائج إيجابية ومتماسكة تؤكد فعالية الرقابة على الأمن السيبراني في إدارة المخاطر المالية بمؤسسات الضمان الاجتماعي. حيث أظهرت النتائج وجود علاقات طردية قوية ودالة إحصائياً ، مما يعكس نجاح هذه المؤسسات في تبني منهجيات متطورة تدعم تحقيق أهدافها الاستراتيجية. حيث يمكن عرض هذه النتائج على النحو التالي:

1. تبين وجود علاقة إيجابية ودالة إحصائياً بين تعزيز الرقابة على الأمن السيبراني وإدارة المخاطر المالية في مؤسسات الضمان الاجتماعي
2. في محور تعزيز الرقابة على الأمن السيبراني، تم تطوير أنظمة حماية متكاملة للبيانات تضمنت سياسات رقابية صارمة لحماية المعلومات الحساسة، كما حققت المؤسسة تقدماً ملحوظاً في رفع الوعي التنظيمي بأهمية الأمن السيبراني ومخاطر القرصنة الإلكترونية.
3. فيما يختص بإدارة المخاطر المالية تم تطبيق إجراءات رقابية فعالة للحد من المخاطر المالية، حيث أظهرت النتائج وجود التزام عالٍ بتطبيق السياسات والإجراءات الوقائية التي تحول دون تحقق المخاطر المحتملة.
4. تم وضع خطط واضحة وشاملة لإدارة المخاطر، اشتملت على آليات منهجية لتحديد وقياس المخاطر المالية المختلفة وتقييم أثرها على أداء المؤسسة.

بناءً على النتائج التي تم التوصل اليها توصي الباحثة بالاتي:

1. تطوير استراتيجية شاملة للأمن السيبراني تشمل أنظمة حماية متقدمة وبرامج تدريبية مستمرة.
2. تعزيز كفاءة إدارة السيولة من خلال تطوير نظم تخطيط مالي متقدمة.
3. تحسين دقة المعلومات المحاسبية وخاصة تلك المتعلقة بنسب السيولة والملاءة المالية.
4. تعزيز ثقافة الابتكار في أساليب إدارة المخاطر والرقابة الداخلية.

قائمة المراجع باللغة العربية

أبو الفضل, عبدالعال مصطفى. (2024). أثر الإنفاق في الأمن السيبراني على الأداء في البنوك التجارية المصرية : مع دراسة ميدانية. *مجلة الدراسات التجارية المعاصرة*, *10*(17), 1851-1906. doi: 10.21608/csj.2024.394855

الفضل, د. (2024). أثر الإنفاق في الأمن السيبراني على الأداء في البنوك التجارية السعودية مع دراسة ميدانية. International Journal of Scientific Studies Publishing. 21. 22-67. 10.62690/ijssp2.

علي عبد الستار ابو كطيفة & ,د. ريما فرج. (2024). المسؤولية المدنية لمقدمي خدمات الأمن السيبراني. *المجلة العربية للعلوم الإنسانية والاجتماعية*. (23), https://doi.org/10.59735/arabjhs.vi23.1264

سالم, أ.م.د/ نهلة المتولي إبراهيم & ,هداية, أ.م.د/ رشا حمدي حسن. (2024). نمط حشد المصادر (المفتوح/ الانتقائي) بيئة تدريب نقالة وأثرها على تنمية مهارات الأمن السيبراني والذكاء الرقمي لدى أعضاء هيئة التدريس ومعاونيهم وفقا لشغفهم الأكاديمي. *المجلة الدولية للتعليم الإلكتروني* :doi. 293-425. (2), *14*, 10.21608/ijel.2024.398961

السيد محمد عبدالله, ايمان. (2024). دراسة العلاقة بين تفعيل ادوات الأمن السيبراني وأنظمة محاسبة التكاليف الرقمية دراسة تطبيقية علي شركات القطاع العقاري بمصر. *المجلة العلمية للبحوث والدراسات التجارية* *38*(1), 63-100. doi: 10.21608/sjrbs.2024.248404.1557 ,

حميد، نادر الفاتح صالح .(2020). *مخاطر التمويل المصرفي دراسات اقتصادية*. مكتبة المعرفة.

سيسي، صلاح .(2000). *الموسوعة المصرفية العلمية والعملية (2 جزء)*. مجموعة النيل العربية.

عبد ربه، محمد محمود. (2006). مخاطر الاعتماد على المعلومات المحاسبية عند تقييم الاستثمارات في سوق الأوراق المالية المصرية. *مجلة الفكر المحاسبي*، (1)، 228-229.

علي، محمد .(2005) .*إدارة المخاطر المالية* [رسالة دكتوراه غير منشورة]. جامعة القاهرة، كلية التجارة.

قندوز، عبد الكريم .(2018) .*التحوط وإدارة المخاطر مدخل مالي* .دار أي-كتب للنشر والتوزيع.

محسن، علي محسن إسماعيل .(2019) .*مسودة دليل العمل الرقابي ضوابط إدارة المخاطر في المصارف التقليدية* .البنك المركزي العراقي، دائرة مراقبة الصيرفة.

ممتاز جدا بنفس الطريقة : اريد ان اكتب فقرات موسعة عن (دور تعزيز الرقابة على الامن السيبراني في إدارة المخاطر المالية)، في فقرات ولا اريد عناوين جانبية، وهذه هي المراجع:

عبد الحكيم, مجدي مليجي, عبدالسلام, فاطمة جبر صالح & ,أحمد زاهد, إسلام. (2025). أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على جودة التقارير المالية وانعكاس ذلك على قيمة المنشأة – دراسة تطبيقية .*مجلة الشروق للعلوم التجارية* , *17*(17.2), 355-415. doi: 10.21608/sjcs.2025.371873.1156

رشا على ابراهيم الفقي; رحاب كمال محمود محمد الزكى. "الدور التأثيري لبرنامج إدارة مخاطر الأمن السيبراني في تفسير العلاقة بين جودة المعلومات المحاسبية وجذب الإستثمارات غير المباشرة – دليل تطبيقي من قطاع الإتصالات بالبورصة المصرية ,"*مجلة البحوث الإدارية والمالية والكمية* , 4, 4, 2024, 613-652. doi: 10.21608/safq.2024.335504.1144

التونى, شريهان مصطفى. (2023). أثر وعى العملاء بالقرصنة الإلكترونية كأداه لتحقيق الأمن السيبراني" دراسة ميدانية علي البنوك الحكومية بمحافظة بورسعيد .*التجارة والتمويل* , *43*(4), 609-653. doi: 10.21608/caf.2023.332810

طلبة, مي. رمضان. (2024). العلاقة بين معدل حوادث الأمن السيبراني وخبرة مراقب الحسابات بصناعة عميله دراسة تطبيقية على الشركات المقيدة بالبورصة المصرية .*مجلة إسكندرية للبحوث الإدارية ونظم المعلومات* , *3*(3), 74-104. doi: 10.21608/ajmris.2024.376692

References in english

Quinn, S., Ivy, N., Barrett, M., Witte, G., & Gardner, R. K. (2022). *Staging cybersecurity risks for enterprise risk management and governance oversight* , National Institute of Standards and Technology. https://doi.org/10.6028

Lowry, M. R., Vance, A., & Vance, M. D. (in press). Inexpert supervision: Field evidence on boards' oversight of cybersecurity. *Management Science*. https://doi.org/10.1287/mnsc.2023.04147

Kanyongo, G., & Wadesango, N. (2025). Impact of cybersecurity on risk mitigation strategy by commercial banks in emerging markets: A legal perspective case study. *Corporate Law & Governance Review*, *7*(1), 28–37. https://doi.org/10.22495/clgrv7i1p3

Opdenbusch, J.C., Hielscher, J., & Sasse, M.A. (2025). "Where Are We On Cyber?" - A Qualitative Study On Boards' Cybersecurity Risk Decision Making. *Proceedings 2025 Network and Distributed System Security Symposium*. https://dx.doi.org/10.14722/ndss.2025.240595

Olufunke Cynthia Metibemu. (2025). "Financial Risk Management in Digital-Only Banks: Addressing Fraud and Cybersecurity Threats in a Cashless Economy". *Asian Journal of Research in Computer Science* 18 (3):434–455. https://doi.org/10.9734/ajrcos/2025/v18i3603.

AbdelSalam, Y. (2022). The Role of Electronic Administrative Control in Cyber Monitoring and Creating a Secure Cyber Environment. *Journal of Law and Emerging Technologies*, *2*(1), 139–176. https://doi.org/10.54873/jolets.v2i1.22

M.M. Saja Fadel Abbas, M. S. F. A. (2024). Digital governance in light of cybersecurity threats: the UAE as a model. *Hammurabi Journal for Studies*, *13*(49), 323–338. https://doi.org/10.61884/hjs.v13i49.445

Sundas Ali Khalifa. (2025). Strategies for Enhancing Cybersecurity and Impact on Customer Trust and the Performance of Iraqi Banks. *Tikrit Journal of Administrative and Economic Sciences*, *21*(69, part 1), 1–17. https://doi.org/10.25130/tjaes.21.69.1.1

Edwards, B. (2019). Cybersecurity oversight liability. *Georgia State University Law Review*, (35)(3), 663. https://ssrn.com/abstract=3390805

Widen, W. H. (2023). *Corporate governance, cybersecurity and oversight: A comment on NIST's proposed framework 2.0 for cybersecurity* (University of Miami Legal Studies Research Paper No. 4624868). SSRN. https://doi.org/10.2139/ssrn.4624868