

Assessing the Level of Internal Audit Readiness in Mitigating Cyberattack Risks and Ensuring Information Security: (A Field Study on North Africa Bank – Sabratha Branch)

khaled Al-Bashir Mohammed Ahmed ^{*1}, Zanjabeel Al Tahir Mohammed Alhaaj ²

¹Department of Accounting, Faculty of Economics and Political Science, University of Sabratha, Libya.

²Postgraduate researcher, Accounting Department, Faculty of Economics, Surman, Sabratha University, Libya

* Email (for reference researcher): khaled.ahmed@sabu.edu.ly

تقييم مستوى جاهزية المراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية وأمن المعلومات (دراسة ميدانية على مصرف شمال افريقيا صرمان)

خالد البشير احمد محمد ^{*1} ، زنجبيل الطاهر محمد الحاج ²

¹قسم المحاسبة، كلية الاقتصاد والعلوم السياسية، جامعة صبراتة، ليبيا.

²طالبة دراسات عليا، قسم المحاسبة، كلية الاقتصاد صرمان ، جامعته صبراتة، ليبيا

Received:02-08-2026; Accepted: 22-09-2026; Published: 25-09-2026

الملخص

هدفت هذه الدراسة إلى تقييم مستوى جاهزية المراجعة الداخلية بأبعادها الحديثة والمتمثلة في (إدارة المخاطر، والدور الحوكمي، وإضافة القيمة) في الحد من مخاطر الهجمات السيبرانية وأمن المعلومات، وذلك من خلال دراسة ميدانية على مصرف شمال أفريقيا – فرع صرمان. واعتمدت الدراسة على المنهج الوصفي التحليلي، واستخدمت الاستبانة أداة لجمع البيانات، حيث تم توزيع (40) استبانة على المراجعين الداخليين والعاملين بإدارة تقنية المعلومات ومديري الإدارات ورؤساء الأقسام والموظفين بالمصرف، واسترداد (36) استبانة صالحة للتحليل الإحصائي باستخدام برنامج (SPSS). وأظهرت نتائج الدراسة وجود مستوى جيد من جاهزية المراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية وأمن المعلومات، حيث بلغ متوسط جاهزية محور إدارة المخاطر (82.65%)، ومحور الدور الحوكمي (83.33%)، ومحور إضافة القيمة (82.10%)، كما بلغت نسبة الجاهزية الكلية للمراجعة الداخلية (82.69%)، وهي نسبة تقع ضمن مستوى الجاهزية الجيد. كما أثبتت نتائج اختبارات (T-Test) ومعامل ارتباط بيرسون وجود دلالة إحصائية تؤكد قبول الفرضية الرئيسية والفرضيات الفرعية للدراسة، بما يعكس فاعلية أبعاد المراجعة الداخلية الحديثة في الحد من مخاطر الهجمات السيبرانية وتعزيز أمن المعلومات بالمصرف، وأوصت الدراسة بالاستمرار في تطوير مهارات المراجعين الداخليين في مجال الأمن السيبراني، وتكثيف البرامج التدريبية المتخصصة، وتعزيز التنسيق بين إدارة المراجعة الداخلية وإدارة تقنية المعلومات، وتحديث خطط إدارة المخاطر بصورة دورية لمواكبة التهديدات السيبرانية المتجددة، مع دعم تطبيق مبادئ الحوكمة وتطوير الضوابط الأمنية بما يساهم في رفع مستوى جاهزية المراجعة الداخلية وتعزيز أمن المعلومات بالمصارف التجارية الليبية.

الكلمات المفتاحية: المراجعة الداخلية، جاهزية المراجعة الداخلية، إدارة المخاطر، الدور الحوكمي، إضافة القيمة، الهجمات السيبرانية، أمن المعلومات، المصارف التجارية الليبية.

Abstract

This study aimed to evaluate the level of internal audit readiness, based on its modern dimensions (risk management, governance role, and value addition), in mitigating cyberattack risks and enhancing information security through a field study conducted at Bank of North Africa – Surman Branch. The study adopted the descriptive-analytical approach and used a questionnaire as the primary data collection instrument. A total of 40 questionnaires were distributed to internal auditors, information technology staff, department managers, section heads, and bank employees. Of these, 36 valid questionnaires were retrieved and analyzed using the Statistical Package for the Social Sciences (SPSS).

The findings revealed a good level of internal audit readiness in mitigating cyberattack risks and enhancing information security. The readiness level reached 82.65% for the risk management dimension, 83.33% for the governance role dimension, and 82.10% for the value addition dimension, while the overall internal audit readiness level reached 82.69%, indicating

a good level of readiness. Furthermore, the results of the One-Sample T-Test and Pearson Correlation Coefficient demonstrated statistically significant evidence supporting the acceptance of both the main hypothesis and the sub-hypotheses. These findings confirm the effectiveness of the modern dimensions of internal audit in mitigating cyberattack risks and strengthening information security within the bank. The study recommends continuously enhancing the competencies of internal auditors in the field of cybersecurity, expanding specialized training programs, strengthening coordination between the Internal Audit Department and the Information Technology Department, and periodically updating risk management plans to address evolving cyber threats. It also recommends reinforcing governance practices and improving security controls to enhance internal audit readiness and strengthen information security in Libyan commercial banks.

Keywords: Internal Audit, Internal Audit Readiness, Risk Management, Governance Role, Value Addition, Cyberattacks, Information Security, Libyan Commercial Banks.

المقدمة:

يشهد القطاع المصرفي تحولاً رقمياً متسارعاً صاحبه تزايد في استخدام الأنظمة الإلكترونية والخدمات المصرفية الرقمية، مما أدى إلى ظهور مخاطر وهجمات سيبرانية تهدد أمن المعلومات واستمرارية العمل داخل المصارف. (Hasan, Alshatshati, & Alastay, 2026) وفي ظل هذه التحديات، برز دور المراجعة الداخلية في تقييم نظم الرقابة وإدارة المخاطر وتعزيز الحوكمة، بما يساهم في رفع جاهزية المصارف لمواجهة التهديدات السيبرانية، ومن هذا المنطلق، تأتي هذه الدراسة لتقييم مستوى جاهزية المراجعة الداخلية بأبعادها الحديثة، والمتمثلة في إدارة المخاطر، والدور الحوكمي، وإضافة القيمة، في الحد من مخاطر الهجمات السيبرانية، من خلال دراسة ميدانية على مصرف شمال أفريقيا – فرع صرمان.

مشكلة الدراسة:

تتمثل مشكلة الدراسة في التزايد المستمر للهجمات السيبرانية وتطور تقنيات الاختراق التي تواجه المصارف التجارية الليبية، مما قد يؤدي إلى خسائر مالية فادحة وتسريب بيانات حساسة، وبناءً على ذلك، تبرز الحاجة لتقييم جاهزية المراجعة الداخلية في مواجهة هذه التهديدات، ويمكن صياغة المشكلة في السؤال الرئيسي التالي:

ما تقييم مستوى جاهزية المراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا صرمان؟ ويتفرع منه التساؤلات التالية:

- ما مستوى جاهزية أنشطة إدارة المخاطر بالمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية؟
- ما مستوى جاهزية الدور الحوكمي للمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية؟
- ما مستوى جاهزية أنشطة إضافة القيمة بالمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية؟

أهداف الدراسة:

يسعى الدراسة لتحقيق الأهداف التالية:

الهدف الرئيسي:

هدفت الدراسة الى تقييم مستوى جاهزية المراجعة الداخلية بأبعادها الحديثة في الحد من مخاطر الهجمات السيبرانية.

الأهداف الفرعية:

- تقييم جاهزية أنشطة إدارة المخاطر بالمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية.
- تقييم جاهزية الدور الحوكمي للمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية.
- تحديد وتقييم جاهزية أنشطة إضافة القيمة بالمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية.

أهمية الدراسة :

الأهمية العلمية: إثراء المكتبة العربية والليبية بأبحاث تجمع بين المراجعة الداخلية والأمن السيبراني في القطاع المصرفي.

الأهمية العملية: تزويد إدارات المصارف الليبية بمؤشرات تساعد على تقييم مستوى جاهزية المراجعة الداخلية وتعزيز دورها في مواجهة التهديدات السيبرانية، بما يساهم في دعم أمن المعلومات وتعزيز ثقة العملاء.

فرضيات الدراسة:

الفرضية الرئيسية:

يوجد تقييم مستوى مرتفع من جاهزية المراجعة الداخلية بأبعادها الحديثة في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا صرمان.

الفرضيات الفرعية:

الفرضية الأولى: يوجد مستوى مرتفع من جاهزية أنشطة إدارة المخاطر بالمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية.

الفرضية الثانية: يوجد مستوى مرتفع من جاهزية الدور الحوكمي للمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية.

الفرضية الثالثة: يوجد مستوى مرتفع من جاهزية أنشطة إضافة القيمة بالمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية.

منهج الدراسة:

تعتمد الدراسة على المنهج الوصفي التحليلي لملاءمته لمثل هذه الدراسات الميدانية.

- **أداة جمع البيانات:** استبانة موجهة إلى المراجعين الداخليين والعاملين بإدارة تقنية المعلومات و الموظفين بمصرف شمال أفريقيا – فرع صرمان.

- **أساليب التحليل:** استخدام برنامج SPSS لتحليل البيانات واختبار الفرضيات .

- حدود الدراسة:

الحدود الموضوعية: تقييم مستوى جاهزية المراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية (السرية، سلامة المعلومات، وتوافر المعلومات واستمرارية العمل) .

الحدود المكانية: مصرف شمال افريقيا صرمان

الحدود الزمانية: الفترة ما بين (2026-2027م)

مصطلحات الدراسة:

- **المراجعة الداخلية:** وظيفة مستقلة وموضوعية لتقديم تأكيدات واستشارات تهدف لإضافة قيمة للمنظمة وتحسين عملياتها.

المخاطر السيبرانية: هي المخاطر الناتجة عن استخدام الأنظمة والشبكات وتقنيات المعلومات، والتي قد تؤثر في سرية المعلومات وسلامتها وتوافرها نتيجة التعرض للهجمات أو الاختراقات الإلكترونية.

- **الهجمات السيبرانية:** محاولات غير مشروعة للوصول إلى الأنظمة المصرفية أو تعطيلها أو التلاعب ببياناتها.

- **إضافة القيمة :** يقصد بإضافة القيمة في المراجعة الداخلية مساهمة نشاط المراجعة الداخلية في تحسين أداء المؤسسة من خلال تقديم التوصيات والاستشارات، وتعزيز إدارة المخاطر والرقابة والحوكمة، بما يساعد الإدارة على تحقيق أهدافها بكفاءة وفعالية.

- **أمن المعلومات :** هو مجموعة السياسات والإجراءات والتقنيات التي تهدف إلى حماية المعلومات وأنظمة المعلومات من الوصول غير المصرح به أو الاستخدام أو الإفصاح أو التعديل أو الإتلاف، بما يضمن الحفاظ على سرية المعلومات وسلامتها وتوافرها.

متغيرات الدراسة:

المتغير المستقل: جاهزية المراجعة الداخلية (إدارة المخاطر، الدور الحوكمي، إضافة القيمة).

المتغير التابع: الحد من مخاطر الهجمات السيبرانية وأمن المعلومات.

الدراسات السابقة :

الدراسة الأولى: أثر جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني

دراسة (أميرهم، 2022): هدفت الدراسة إلى اختبار أثر جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني في شركات الاتصالات المصرية. واعتمدت على المنهج الوصفي التحليلي، وبلغ مجتمع الدراسة (120) مفردة موزعة بالتساوي بين مسؤولي المراجعة الداخلية، ومسؤولي تكنولوجيا المعلومات، ومسؤولي إدارة المخاطر، والمستثمرين. وتوصلت الدراسة إلى أن المراجعة الداخلية تؤدي دوراً محورياً في الحد من مخاطر الأمن السيبراني، وأن أصحاب المصالح لا يستطيعون متابعة المخاطر السيبرانية بكفاءة دون وجود مراجعة داخلية فعالة. وأوصت الدراسة بضرورة تأهيل المراجعين الداخليين وتطوير مهاراتهم المهنية لمواكبة التطورات في مجال الأمن السيبراني.

الدراسة الثانية: دور الأنشطة الحديثة للمراجعة الداخلية في الحد من مخاطر الخدمات الإلكترونية

دراسة (موسى، 2024): هدفت الدراسة إلى التعرف على دور الأنشطة الحديثة للمراجعة الداخلية المتمثلة في إدارة المخاطر، والدور الحوكمي، وإضافة القيمة في الحد من مخاطر الخدمات الإلكترونية بالمصارف السودانية. واعتمدت الدراسة على المنهج الوصفي التحليلي، واستخدمت عينة قصدية بلغت (65) مفردة من المراجعين الداخليين والعاملين بإدارة تقنية المعلومات. وأظهرت النتائج وجود اهتمام كبير بالحد من مخاطر الخدمات الإلكترونية في ظل التحول الرقمي، وأوصت الدراسة بتعزيز تطبيق التقنيات الأمنية الحديثة وتطوير الخدمات الإلكترونية بما يضمن حماية بيانات العملاء.

الدراسة الثالثة: دور المراجعة الداخلية في إدارة المخاطر بالمصارف التجارية الليبية

دراسة (أبوزيد وأبو زقية، 2024): هدفت الدراسة إلى التعرف على دور المراجعة الداخلية في إدارة المخاطر بالمصارف التجارية الليبية. واعتمد الباحثان على المنهج الوصفي التحليلي، وأجريت الدراسة على عينة عشوائية مكونة من (109) من مسؤولي وموظفي إدارات المراجعة الداخلية وإدارة المخاطر بالمصارف التجارية بمدينة مصراتة. وتوصلت الدراسة إلى أن المراجعة الداخلية تسهم بفاعلية في تعزيز إدارة المخاطر، وأوصت بزيادة تفعيل دورها داخل المصارف التجارية الليبية.

الدراسة الرابعة: دور المراجعة الداخلية في إدارة مخاطر الأمن السيبراني

دراسة (جديع ومحمد، 2025): هدفت الدراسة إلى التعرف على دور المراجعة الداخلية في إدارة مخاطر الأمن السيبراني بالمصارف التجارية العاملة بمدينة طرابلس. واعتمدت على المنهج الوصفي التحليلي، وتم توزيع (53) استبانة على مديري ورؤساء وموظفي إدارات المراجعة الداخلية. وأظهرت النتائج أن المراجعة الداخلية تؤدي دوراً مهماً في تعزيز إدارة المخاطر السيبرانية، وأوصت الدراسة بتوفير برامج تدريبية متخصصة للمراجعين الداخليين لفهم وتقييم المخاطر السيبرانية المعقدة.

الدراسة الخامسة: دور حوكمة الأمن السيبراني في تعزيز دقة التقارير المالية دراسة (سحيم، 2026): هدفت الدراسة إلى التعرف على دور حوكمة الأمن السيبراني في تعزيز دقة التقارير المالية بالمصارف التجارية الليبية. واعتمدت على المنهج الوصفي التحليلي، وبلغت عينة الدراسة (35) مفردة من العاملين بالمصارف التجارية بمدينة صبراتة. وتوصلت الدراسة إلى وجود أثر ذي دلالة إحصائية لحوكمة الأمن السيبراني في تعزيز دقة التقارير المالية، وأوصت بإنشاء لجنة متخصصة لحوكمة الأمن السيبراني داخل المصارف.

التعقيب على الدراسات السابقة:

يتضح من الدراسات السابقة أنها تناولت موضوع المراجعة الداخلية وعلاقتها بإدارة المخاطر والأمن السيبراني من زوايا متعددة، حيث ركزت بعض الدراسات على أثر جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني، بينما تناولت دراسات أخرى دور الأنشطة الحديثة للمراجعة الداخلية، والمتمثلة في إدارة المخاطر، والدور الحوكمي، وإضافة القيمة، في تعزيز أمن الخدمات الإلكترونية وإدارة المخاطر بالمصارف. كما اهتمت بعض الدراسات ببيان دور حوكمة الأمن السيبراني في تحسين الأداء المالي وجودة التقارير المالية.

وقد استفادت الباحثة من هذه الدراسات في بناء الإطار النظري، وتحديد أبعاد المراجعة الداخلية، وصياغة مشكلة الدراسة وأهدافها، واختيار المنهج المناسب وأداة جمع البيانات، وعلى الرغم من أهمية هذه الدراسات، إلا أنها اختلفت في بيئاتها التطبيقية وأهدافها، حيث أجريت معظمها في بيئات عربية مختلفة، كما أن الدراسات الليبية تناولت موضوع إدارة المخاطر أو حوكمة الأمن السيبراني بصورة عامة، ولم تركز على تقييم مستوى جاهزية المراجعة الداخلية في ظل التطورات التقنية والمنشورات الرقابية الحديثة الصادرة عن مصرف ليبيا المركزي بشأن حوكمة تكنولوجيا المعلومات.

وفي حدود اطلاع الباحثة، لم تتناول أي دراسة **تقييم مستوى جاهزية المراجعة الداخلية بأبعادها الحديثة في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا – فرع صرمان**، الأمر الذي يمثل فجوة بحثية تسعى هذه الدراسة إلى معالجتها من خلال تقديم نتائج ميدانية تساهم في دعم المراجعة الداخلية وتعزيز جاهزيتها لمواجهة المخاطر السيبرانية في البيئة المصرفية الليبية.

الإطار النظري

المبحث الأول: الإطار المفاهيمي للمراجعة الداخلية وجاهزيتها

يُعد نشاط المراجعة الداخلية أحد أهم الأدوات الرقابية التي تعتمد عليها المؤسسات المصرفية في تعزيز كفاءة الأداء، ودعم نظم الرقابة الداخلية، وإدارة المخاطر، وتحقيق أهداف الحوكمة المؤسسية، وقد شهد هذا النشاط خلال السنوات الأخيرة تطوراً ملحوظاً، فلم يعد يقتصر على اكتشاف الأخطاء والتحقق من الالتزام بالإجراءات، بل أصبح يؤدي دوراً استراتيجياً في تقديم التأكيدات والاستشارات التي تساهم في حماية المؤسسة وإضافة القيمة إليها، لا سيما في ظل التطور المتسارع في بيئة الأعمال والتوسع في استخدام التقنيات الرقمية.

وفي ظل تصاعد التهديدات السيبرانية وتزايد المخاطر المرتبطة بأمن المعلومات، أصبحت جاهزية المراجعة الداخلية تمثل أحد المتطلبات الأساسية لضمان قدرة المصارف على مواجهة هذه التحديات، وذلك من خلال تطوير أدوارها الحديثة في إدارة المخاطر، وتعزيز الحوكمة، والمساهمة في تحسين الأداء المؤسسي. وانطلاقاً من ذلك، يتناول هذا المبحث الإطار المفاهيمي للمراجعة الداخلية وجاهزيتها، من خلال استعراض مفهوم المراجعة الداخلية وأهدافها، ثم توضيح مفهوم جاهزية المراجعة الداخلية ومتطلباتها، وأخيراً عرض الأبعاد الحديثة للمراجعة الداخلية المتمثلة في إدارة المخاطر، والدور الحوكمي، وإضافة القيمة، باعتبارها الأساس الذي تقوم عليه الدراسة الحالية.

المطلب الأول: المراجعة الداخلية في البيئة المصرفية

تُعد المراجعة الداخلية من أهم الوظائف الرقابية التي تعتمد عليها المؤسسات بصفة عامة والمصارف بصفة خاصة في المحافظة على أصولها، والتحقق من سلامة عملياتها، ورفع كفاءة نظم الرقابة الداخلية وإدارة المخاطر. وقد ازدادت أهميتها في البيئة المصرفية نتيجة اتساع حجم المعاملات المالية، والاعتماد المتزايد على الأنظمة الإلكترونية، وظهور مخاطر جديدة مرتبطة بالتحول الرقمي وأمن المعلومات والهجمات السيبرانية.

أولاً: مفهوم المراجعة الداخلية

شهد مفهوم المراجعة الداخلية تطوراً ملحوظاً؛ إذ لم يعد نشاطها مقتصرًا على فحص السجلات والتحقق من صحة العمليات المالية واكتشاف الأخطاء والمخالفات، بل أصبحت نشاطاً مستقلاً وموضوعياً يقدم خدمات تأكيدية واستشارية، ويهدف إلى إضافة قيمة للمؤسسة وتحسين عملياتها، من خلال اتباع أسلوب منظم في تقييم فاعلية إدارة المخاطر والرقابة والحوكمة.

وفي هذا الإطار، ينظر إلى المراجعة الداخلية في المصارف باعتبارها نشاطاً رقابياً مستقلاً يساعد الإدارة ومجلس الإدارة في التحقق من سلامة العمليات المصرفية، ومدى الالتزام بالقوانين والتعليمات والسياسات الداخلية، وكفاية الضوابط المستخدمة لحماية أموال المصرف وبيانات العملاء. كما تساهم في تقييم قدرة المصرف على تحديد المخاطر وقياسها والاستجابة لها، وتقديم التوصيات المناسبة لمعالجة نقاط الضعف والقصور.

وتؤكد المعايير العالمية للمراجعة الداخلية أن الغرض من المراجعة الداخلية يتمثل في تعزيز قدرة المؤسسة على إنشاء القيمة وحمايتها واستدامتها، من خلال تقديم تأكيدات ومشورة موضوعية ومستقلة إلى مجلس الإدارة والإدارة. ويبين هذا المفهوم أن المراجعة الداخلية لم تعد مجرد أداة لفحص الأحداث الماضية، وإنما أصبحت وظيفة مستقبلية تساعد المؤسسة على تحقيق

أهدافها والاستعداد للمخاطر المحتملة (معهد المراجعين الداخليين، 2024). وقد صدرت المعايير العالمية الجديدة في 9 يناير 2024، وأصبحت واجبة التطبيق اعتباراً من 9 يناير 2025.

ثانياً: أهداف المراجعة الداخلية

تهدف المراجعة الداخلية في المصارف إلى تحقيق مجموعة من الأهداف المترابطة، يأتي في مقدمتها تقييم مدى كفاءة وفعالية نظام الرقابة الداخلية، والتحقق من سلامة العمليات المالية والمصرفية، ومدى الالتزام بالقوانين واللوائح والتعليمات الصادرة عن الجهات الرقابية. كما تهدف إلى حماية أصول المصرف وموارده ومعلوماته من الضياع أو سوء الاستخدام أو الاختراق، والتأكد من دقة البيانات المحاسبية والتقارير المالية وإمكانية الاعتماد عليها في اتخاذ القرارات. وتسهم المراجعة الداخلية كذلك في تقييم المخاطر التي تواجه النشاط المصرفي، والتأكد من وجود إجراءات مناسبة لتحديد وقياسها ومتابعتها ومعالجتها. وقد أوضحت دراسة أبو زيد وأبورقية (2024) أن المراجعة الداخلية تؤدي دوراً مهماً في تعزيز إدارة المخاطر بالمصارف التجارية الليبية، من خلال تقييم المخاطر والاستجابة لها ورفع مستوى إدراك العاملين بأهميتها. وفي ظل اعتماد المصارف على نظم المعلومات والخدمات الرقمية، أصبحت المراجعة الداخلية تهدف أيضاً إلى تقييم ضوابط أمن المعلومات، والتحقق من حماية سرية البيانات وسلامتها وتوافرها، ومراجعة خطط استمرارية الأعمال والتعافي من الكوارث. كما تهدف إلى تقديم الاستشارات والتوصيات التي تساعد الإدارة على تحسين الأداء وتطوير الإجراءات، وبذلك تجمع المراجعة الداخلية بين الدور الرقابي والدور الاستشاري وإضافة القيمة.

ثالثاً: معايير المراجعة الداخلية

تخضع المراجعة الداخلية لمجموعة من المعايير المهنية التي أصدرها معهد المراجعين الداخليين، بهدف توحيد ممارساتها وضمان جودة أدائها. وقد أعيد تنظيم هذه المعايير ضمن المعايير العالمية للمراجعة الداخلية لعام 2024، التي أصبحت نافذة في سنة 2025، وتضمنت خمسة مجالات رئيسية هي: غرض المراجعة الداخلية، والأخلاق والمهنية، وحوكمة وظيفة المراجعة الداخلية، وإدارة وظيفة المراجعة الداخلية، وأداء خدمات المراجعة الداخلية. وتقوم هذه المعايير على خمسة مبادئ أساسية، من أهمها النزاهة، والمحافظة على الموضوعية، وإثبات الكفاءة، وبذل العناية المهنية اللازمة، والمحافظة على السرية، والاستقلال التنظيمي، والإشراف من مجلس الإدارة، والتخطيط الاستراتيجي، وإدارة الموارد، والتواصل الفعال، وتعزيز الجودة، والتخطيط لمهام المراجعة وتنفيذها وإبلاغ نتائجها ومتابعة الإجراءات التصحيحية. ويتطلب تطبيق هذه المعايير في البيئة المصرفية أن تتمتع إدارة المراجعة الداخلية بالاستقلالية، وأن ترتبط تنظيمياً بمجلس الإدارة أو لجنة المراجعة، وأن تتوافر للمراجعين الداخليين الكفاءة المهنية والمعرفة بالمخاطر المصرفية والتقنية. كما يتطلب وضع خطة مراجعة قائمة على المخاطر، وإتاحة جميع البيانات والسجلات للمراجعين، وتنفيذ برنامج مستمر لضمان جودة نشاط المراجعة الداخلية وتحسينه.

رابعاً: تطور دور المراجعة الداخلية في المصارف

مر دور المراجعة الداخلية في المصارف بعدة مراحل؛ فقد بدأ بالتركيز على مراجعة المعاملات المالية واكتشاف الأخطاء والغش، ثم اتسع ليشمل تقييم نظم الرقابة الداخلية والتحقق من الالتزام بالقوانين والسياسات. وبعد تزايد المخاطر وتطور بيئة الأعمال، أصبحت المراجعة الداخلية تشارك في تقييم إدارة المخاطر والحوكمة وتقديم الخدمات الاستشارية التي تساعد الإدارة على تحسين أدائها وتحقيق أهدافها.

وأدى التحول الرقمي في القطاع المصرفي إلى زيادة مسؤوليات المراجعة الداخلية، حيث أصبحت مطالبة بتقييم مخاطر الأنظمة الإلكترونية، وأمن البيانات، والخدمات المصرفية الرقمية، ووسائل الدفع الإلكتروني، وخطط استمرارية العمل. كما أصبح من الضروري أن يمتلك المراجع الداخلي معرفة مناسبة بتكنولوجيا المعلومات والمخاطر السيبرانية، وأن يستعين بالخبراء المتخصصين عندما تتجاوز طبيعة المخاطر حدود خبرته المهنية.

وفي هذا السياق، توصلت دراسة جديع ومحمد (2025) إلى أن المراجعة الداخلية تؤدي دوراً مهماً في إدارة المخاطر السيبرانية، وأن فاعلية هذا الدور تتطلب توافر الكفاءة المهنية والتدريب المتخصص والاستقلالية وإمكانية الوصول إلى المعلومات اللازمة. كما بينت الدراسات الحديثة أن الدور الاستشاري والتوكيدي للمراجعة الداخلية يساهم في دعم الحوكمة المصرفية وتحسين جودة القرارات والتقارير، الأمر الذي يعكس انتقال المراجعة الداخلية من الدور التقليدي القائم على اكتشاف الأخطاء إلى دور حديث يقوم على إدارة المخاطر والحوكمة وإضافة القيمة (إبراهيم، 2024).

وبناءً على ما سبق، يتضح أن المراجعة الداخلية في البيئة المصرفية أصبحت شريكاً أساسياً للإدارة ومجلس الإدارة في حماية أصول المصرف ومعلوماته، وتحسين إدارة المخاطر والرقابة والحوكمة. كما أن قدرتها على الحد من المخاطر السيبرانية ترتبط بمدى جاهزيتها من حيث الاستقلالية والكفاءة المهنية والتدريب والموارد التقنية والقدرة على تقييم الضوابط الأمنية، وهو ما يمثل الأساس الذي تنطلق منه الدراسة الحالية في تقييم جاهزية المراجعة الداخلية بمصرف شمال أفريقيا – فرع صرمان

المطلب الثاني: جاهزية المراجعة الداخلية

تُعد جاهزية المراجعة الداخلية من المفاهيم الحديثة التي برزت نتيجة التطورات المتسارعة في بيئة الأعمال، وما صاحبها من تغيرات تقنية وتشريعية ومخاطر متزايدة، خاصة في القطاع المصرفي. ولم يعد نجاح نشاط المراجعة الداخلية يقاس بمجرد تنفيذ خطط المراجعة، وإنما بمدى جاهزيته للاستجابة للمتغيرات، والتعامل مع المخاطر الناشئة، وتقديم خدمات تأكيدية واستشارية تساهم في حماية المؤسسة وتحقيق أهدافها. وفي ظل التحول الرقمي وازدياد مخاطر الأمن السيبراني، أصبحت جاهزية المراجعة الداخلية عنصراً أساسياً لضمان استمرارية المصارف وتعزيز أمن المعلومات.

أولاً: مفهوم الجاهزية

يقصد بالجاهزية مدى استعداد المؤسسة أو النشاط الوظيفي للقيام بمهامه بكفاءة وفاعلية عند مواجهة الظروف الاعتيادية أو الطارئة، من خلال توافر الموارد البشرية المؤهلة، والأنظمة والإجراءات المناسبة، والتقنيات الحديثة، والقدرة على التكيف مع المتغيرات الداخلية والخارجية. ويعكس مفهوم الجاهزية قدرة المؤسسة على الاستجابة للمخاطر والتهديدات بصورة استباقية، بما يضمن استمرارية الأداء وتحقيق الأهداف المؤسسية. ويؤكد هذا المفهوم أن الجاهزية ليست حالة ثابتة، وإنما عملية مستمرة تعتمد على التطوير والتحسين والتقييم الدوري (معهد المراجعين الداخليين، 2024). وقد أولت المعايير العالمية للمراجعة الداخلية الصادرة عام 2024 اهتماماً واضحاً بتخطيط نشاط المراجعة، وإدارة موارده، وتعزيز جودة الأداء، باعتبارها من أهم متطلبات جاهزية وظيفة المراجعة الداخلية، وأصبحت هذه المعايير نافذة اعتباراً من يناير 2025.

ثانياً: مفهوم جاهزية المراجعة الداخلية

تشير جاهزية المراجعة الداخلية إلى قدرة إدارة المراجعة الداخلية على أداء مسؤولياتها بكفاءة وفاعلية في ظل المتغيرات التنظيمية والتقنية، من خلال امتلاك الكفاءات المهنية، والاستقلالية، والموارد الكافية، والاعتماد على منهج قائم على المخاطر، بما يمكنها من تقديم قيمة مضافة للإدارة ومجلس الإدارة. كما تعكس مدى استعداد المراجعة الداخلية لتقييم المخاطر الناشئة، وعلى رأسها المخاطر السيبرانية، والتحقق من كفاية الضوابط الرقابية، وتقديم التوصيات التي تعزز الحوكمة وتحسن الأداء المؤسسي.

وفي البيئة المصرفية، ترتبط جاهزية المراجعة الداخلية بقدرتها على مواكبة التحول الرقمي، وفهم مخاطر أمن المعلومات، واستخدام التقنيات الحديثة في تنفيذ أعمال المراجعة. وقد أشارت دراسة جديع ومحمد (2025) إلى أن نجاح المراجعة الداخلية في إدارة المخاطر السيبرانية يتطلب توافر التأهيل المهني، والتدريب المستمر، والاستقلالية، والتنسيق مع إدارات تقنية المعلومات وإدارة المخاطر. كما أوضحت دراسة موسى (2024) أن الأنشطة الحديثة للمراجعة الداخلية أصبحت تمثل ركيزة أساسية للحد من مخاطر الخدمات الإلكترونية بالمصارف، من خلال إدارة المخاطر، والدور الحوكمي، وإضافة القيمة.

ثالثاً: متطلبات جاهزية المراجعة الداخلية

تتطلب جاهزية المراجعة الداخلية توافر مجموعة من المقومات الأساسية، أهمها الاستقلالية والموضوعية، ووجود كفاءات مهنية مؤهلة تمتلك المعرفة المحاسبية والتقنية، إضافة إلى التدريب المستمر لمواكبة التطورات في مجال الأمن السيبراني وتقنيات المعلومات. كما تتطلب توفير الموارد البشرية والتقنية الكافية، والاعتماد على خطط مراجعة مبنية على المخاطر، مع وجود دعم من الإدارة العليا ومجلس الإدارة، وتطبيق برامج ضمان وتحسين الجودة وفق المعايير المهنية الدولية. وتؤكد المعايير العالمية للمراجعة الداخلية (IIA، 2024) أن جاهزية وظيفة المراجعة تعتمد كذلك على التخطيط الاستراتيجي، والإدارة الفعالة للموارد، والتواصل مع أصحاب المصلحة، وقياس الأداء وتحسينه بصورة مستمرة، بما يضمن قدرة المراجعة الداخلية على تحقيق رسالتها في تعزيز الحوكمة وإدارة المخاطر والرقابة.

رابعاً: مؤشرات قياس جاهزية المراجعة الداخلية

يمكن قياس جاهزية المراجعة الداخلية من خلال مجموعة من المؤشرات، من أهمها مستوى تأهيل المراجعين الداخليين، ومدى الالتزام بالمعايير المهنية الدولية، ودرجة استقلالية إدارة المراجعة الداخلية، وتوافر الموارد المالية والتقنية اللازمة، ووجود خطط مراجعة قائمة على المخاطر، ومستوى التنسيق مع إدارات المخاطر وتقنية المعلومات، إضافة إلى سرعة الاستجابة للمخاطر الناشئة، وفاعلية تنفيذ التوصيات، ومستوى رضا الإدارة عن خدمات المراجعة الداخلية. كما تعد قدرة المراجعة الداخلية على تقييم المخاطر السيبرانية، والمشاركة في مراجعة ضوابط أمن المعلومات، وتقديم التقارير الدورية للإدارة، من أهم المؤشرات التي تعكس جاهزيتها في البيئة المصرفية الحديثة. وتتفق هذه المؤشرات مع الأبعاد الرئيسة للدراسة الحالية، والمتمثلة في إدارة المخاطر، والدور الحوكمي، وإضافة القيمة.

خامساً: العوامل المؤثرة في جاهزية المراجعة الداخلية

تتأثر جاهزية المراجعة الداخلية بعدة عوامل، من أبرزها دعم الإدارة العليا، واستقلالية إدارة المراجعة الداخلية، وكفاءة المراجعين الداخليين، وتوافر التدريب المستمر، ودرجة استخدام التكنولوجيا، وجودة نظم المعلومات، وثقافة إدارة المخاطر داخل المؤسسة. كما تؤثر التشريعات والتعليمات الرقابية، ومستوى التنسيق بين إدارات المراجعة الداخلية وإدارة المخاطر وتقنية المعلومات، في تعزيز جاهزية المراجعة الداخلية لمواجهة المخاطر الحديثة.

وفي القطاع المصرفي الليبي، تزداد أهمية هذه العوامل مع تزايد الاعتماد على الخدمات المصرفية الإلكترونية، وظهور مخاطر سيبرانية أكثر تعقيداً، الأمر الذي يتطلب تطوير قدرات المراجعة الداخلية بصورة مستمرة. وقد بينت دراسة أبو زيد وأبو زقية (2024) أن فاعلية المراجعة الداخلية في إدارة المخاطر ترتبط بدرجة الدعم الإداري وتوافر الكفاءات المهنية، بينما أكدت دراسة سحيم (2026) أن تعزيز حوكمة الأمن السيبراني يساهم في رفع كفاءة الأداء المؤسسي وتحسين جودة المعلومات المالية، الأمر الذي يعزز من جاهزية المراجعة الداخلية لأداء دورها الرقابي والاستشاري.

وبناءً على ما سبق، فإن جاهزية المراجعة الداخلية تمثل الأساس الذي تنطلق منه الدراسة الحالية، إذ إن قدرة المراجعة الداخلية على الحد من مخاطر الهجمات السيبرانية لا تتحقق إلا من خلال توافر متطلبات الجاهزية، وانعكاسها على أبعادها الحديثة المتمثلة في إدارة المخاطر، والدور الحوكمي، وإضافة القيمة، وهي الأبعاد التي اعتمدتها الدراسة في قياس مستوى جاهزية المراجعة الداخلية بمصرف شمال أفريقيا – فرع صرمان.

المطلب الثالث: الأبعاد الحديثة للمراجعة الداخلية

شهدت المراجعة الداخلية خلال السنوات الأخيرة تطوراً ملحوظاً نتيجة التغيرات المتسارعة في بيئة الأعمال، والتوسع في استخدام التقنيات الرقمية، وازدياد المخاطر التي تواجه المؤسسات، خاصة في القطاع المصرفي. وقد أدى هذا التطور إلى انتقال المراجعة الداخلية من دورها التقليدي القائم على فحص العمليات المالية والتحقق من الالتزام، إلى دور استراتيجي يركز على إدارة المخاطر، وتعزيز الحوكمة، وإضافة القيمة للمؤسسة. وأصبحت هذه الأبعاد تمثل الركائز الأساسية التي تستند إليها المراجعة الداخلية الحديثة في تحقيق أهدافها وتعزيز قدرة المؤسسات على مواجهة المخاطر وتحسين الأداء.

أولاً: إدارة المخاطر

تُعد إدارة المخاطر أحد أهم الأبعاد الحديثة للمراجعة الداخلية، حيث يتمثل دورها في مساعدة الإدارة على تحديد المخاطر وتحليلها وتقييمها، واقتراح الإجراءات المناسبة للحد من آثارها، والتأكد من كفاءة الضوابط الرقابية المطبقة لمواجهتها. وتعتمد المراجعة الداخلية الحديثة على منهج قائم على المخاطر عند إعداد خططها وتنفيذ برامجها، بما يضمن توجيه جهود المراجعة نحو المجالات الأكثر تعرضاً للمخاطر.

وفي البيئة المصرفية، توسع مفهوم إدارة المخاطر ليشمل المخاطر التشغيلية، والائتمانية، والمالية، إضافة إلى المخاطر السيبرانية الناتجة عن استخدام الأنظمة الإلكترونية والخدمات الرقمية. ومن ثم أصبحت المراجعة الداخلية مطالبة بتقييم فعالية السياسات والإجراءات الخاصة بحماية البيانات، واستمرارية الأعمال، والاستجابة للحوادث السيبرانية.

وقد أكدت دراسة موسى (2024) أن إدارة المخاطر تمثل أحد أهم الأدوار الحديثة للمراجعة الداخلية في الحد من مخاطر الخدمات الإلكترونية بالمصارف، كما توصلت دراسة أبو زيد وأبو زقية (2024) إلى وجود دور فاعل للمراجعة الداخلية في دعم إدارة المخاطر بالمصارف التجارية الليبية، من خلال تقييم المخاطر وتعزيز كفاءة الرقابة الداخلية. كما أشارت دراسة جديع ومحمد (2025) إلى أن نجاح المراجعة الداخلية في إدارة المخاطر السيبرانية يعتمد على تبني منهج قائم على المخاطر، وتوفير التدريب المتخصص للمراجعين الداخليين.

ثانياً: الدور الحوكمي

أصبحت الحوكمة من المفاهيم الرئيسة التي ترتبط بالمراجعة الداخلية الحديثة، حيث تؤدي المراجعة الداخلية دوراً محورياً في دعم مبادئ الحوكمة، وتعزيز الشفافية والمساءلة، وتحسين جودة اتخاذ القرارات داخل المؤسسة. ويتمثل الدور الحوكمي للمراجعة الداخلية في تقييم مدى التزام المؤسسة بالتشريعات والسياسات، ومراجعة كفاءة نظم الرقابة، والتحقق من سلامة إدارة المخاطر، وتقديم تقارير موضوعية إلى مجلس الإدارة ولجنة المراجعة.

وتؤكد المعايير العالمية للمراجعة الداخلية (IIA، 2024) أن المراجعة الداخلية تعد عنصراً أساسياً في منظومة الحوكمة، من خلال توفير التأكيد المستقل بشأن كفاءة الحوكمة وإدارة المخاطر والرقابة الداخلية، بما يساهم في حماية المؤسسة وتحقيق أهدافها الاستراتيجية. وقد أصبحت هذه المعايير نافذة اعتباراً من يناير 2025، مع تركيز واضح على تعزيز دور مجلس الإدارة في الإشراف على نشاط المراجعة الداخلية (معهد المراجعين الداخليين، 2024).

وفي القطاع المصرفي، تزداد أهمية الدور الحوكمي للمراجعة الداخلية مع التوسع في الخدمات المصرفية الرقمية، حيث تساهم في تقييم مدى الالتزام بضوابط أمن المعلومات، ومتابعة تنفيذ السياسات الرقابية، وتعزيز ثقافة الامتثال داخل المصرف. كما أوضحت دراسة سحيم (2026) أن تطبيق حوكمة الأمن السيبراني يساهم في تحسين جودة المعلومات المالية وتعزيز ثقة أصحاب المصلحة، وهو ما يعكس أهمية التكامل بين الحوكمة والمراجعة الداخلية في البيئة المصرفية.

ثالثاً: إضافة القيمة

لم تعد المراجعة الداخلية تقتصر على اكتشاف الأخطاء أو تقييم الرقابة، وإنما أصبحت تهدف إلى إضافة قيمة للمؤسسة من خلال تقديم خدمات استشارية وتوصيات عملية تساعد الإدارة على تحسين الأداء ورفع كفاءة استخدام الموارد وتحقيق الأهداف المؤسسية. ويقصد بإضافة القيمة مساهمة المراجعة الداخلية في تحسين العمليات، وتطوير نظم الرقابة، وتعزيز إدارة المخاطر، ودعم اتخاذ القرارات، بما يؤدي إلى تحسين الأداء المؤسسي بصورة مستمرة.

وتتحقق إضافة القيمة من خلال تقديم حلول عملية للمشكلات، والمشاركة في تطوير الإجراءات، واقتراح فرص التحسين، وتقييم كفاءة العمليات التشغيلية، ودعم مشروعات التحول الرقمي، ومراجعة فعالية الضوابط الخاصة بأمن المعلومات والهجمات السيبرانية. كما تساهم المراجعة الداخلية في تحسين جودة التقارير وتعزيز ثقة الإدارة وأصحاب المصالح في المعلومات الصادرة عن المؤسسة.

وقد بينت دراسة أميرهم (2022) أن جودة المراجعة الداخلية تساهم بصورة مباشرة في الحد من مخاطر الأمن السيبراني، من خلال تحسين جودة الرقابة الداخلية ورفع كفاءة تقييم المخاطر، بينما أكدت دراسة موسى (2024) أن إضافة القيمة أصبحت من أهم الأبعاد الحديثة للمراجعة الداخلية في المصارف، لما لها من دور في دعم التحول الرقمي والحد من مخاطر الخدمات الإلكترونية.

وبناءً على ما سبق، يتضح أن الأبعاد الحديثة للمراجعة الداخلية والمتمثلة في إدارة المخاطر، والدور الحوكمي، وإضافة القيمة أصبحت تشكل الإطار الذي تستند إليه المراجعة الداخلية الحديثة في أداء مهامها، ولا سيما في المؤسسات المصرفية التي تواجه تحديات تقنية ومخاطر سيبرانية متزايدة. كما تمثل هذه الأبعاد المتغيرات الرئيسة للدراسة الحالية، إذ إن مستوى جاهزية المراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية يعتمد بدرجة كبيرة على فاعلية هذه الأبعاد وتكاملها في دعم أمن المعلومات واستمرارية العمل داخل مصرف شمال أفريقيا – فرع صرمان.

المبحث الثاني: الهجمات السيبرانية وأمن المعلومات

أدى التوسع في استخدام تكنولوجيا المعلومات والتحول نحو تقديم الخدمات المصرفية الرقمية إلى إحداث تغييرات جوهرية في طبيعة العمل المصرفي، حيث أصبحت المصارف تعتمد بصورة كبيرة على الأنظمة الإلكترونية وشبكات الاتصال وقواعد البيانات في تنفيذ العمليات المالية وتقديم الخدمات للعملاء. وعلى الرغم من المزايا التي حققها هذا التحول من حيث السرعة والدقة وتخفيض التكاليف، فإنه أدى في المقابل إلى ظهور مجموعة من المخاطر والتهديدات السيبرانية التي قد تستهدف الأنظمة المصرفية وبيانات العملاء وتؤثر في استمرارية الأعمال.

وتُعد المصارف من أكثر المؤسسات عرضة للهجمات السيبرانية، نظرًا لما تحتفظ به من بيانات مالية وشخصية حساسة، وما تديره من تحويلات وأصول مالية، فضلاً عن ارتباطها بشبكات وأنظمة دفع إلكترونية متعددة. وقد أوضحت لجنة بازل للرقابة المصرفية أن رقمنة الخدمات المالية، رغم ما توفره من فرص لتحسين الكفاءة والابتكار، ترتبط بمخاطر تقنية وتشغيلية متزايدة تستلزم تطوير قدرات المصارف والجهات الرقابية على إدارتها ومتابعتها (لجنة بازل للرقابة المصرفية، 2024). ولا تقتصر آثار الهجمات السيبرانية على الخسائر المالية المباشرة، بل قد تمتد إلى تعطيل الخدمات المصرفية، والإضرار بسمعة المصرف، وفقدان ثقة العملاء، وتسريب المعلومات، والتأثير في سلامة النظام المالي. كما أن الترابط بين المصارف ومقدمي الخدمات التقنية وأنظمة الدفع يجعل أثر الحادث السيبراني قابلاً للانتقال من مؤسسة واحدة إلى مؤسسات أخرى، الأمر الذي يجعل الأمن السيبراني جزءاً أساسياً من إدارة المخاطر والحكمة واستمرارية الأعمال في القطاع المصرفي. وانطلاقاً من ذلك، يتناول هذا المبحث الهجمات السيبرانية وأمن المعلومات من خلال توضيح مفهوم الهجمات السيبرانية وأنواعها وآثارها على المصارف، ثم بيان مفهوم أمن المعلومات وأهدافه وعناصره الأساسية، وأخيراً توضيح دور المراجعة الداخلية في تقييم المخاطر السيبرانية وتعزيز أمن المعلومات، بما يخدم أهداف الدراسة الحالية المتعلقة بتقييم جاهزية المراجعة الداخلية في مصرف شمال أفريقيا – فرع صرمان.

المطلب الأول: الهجمات السيبرانية في القطاع المصرفي

أصبحت الهجمات السيبرانية من أبرز المخاطر التي تواجه المصارف في البيئة الرقمية الحديثة، نتيجة الاعتماد المتزايد على التطبيقات المصرفية والأنظمة الإلكترونية والخدمات المتصلة بالإنترنت. وتتميز هذه الهجمات بسرعة تطورها وتعدد أساليبها، كما قد تستهدف المصرف بصورة مباشرة، أو تستغل أحد العملاء أو الموظفين أو مقدمي الخدمات الخارجيين للوصول إلى الأنظمة والبيانات المصرفية.

أولاً: مفهوم الهجمات السيبرانية

يمكن تعريف الهجمات السيبرانية بأنها محاولات متعمدة وغير مشروعة تهدف إلى الوصول إلى الأنظمة أو الشبكات أو الأجهزة الرقمية دون تصريح، بقصد سرقة البيانات أو كشفها أو تغييرها أو تعطيلها أو إتلافها. وقد تستهدف هذه الهجمات سرية المعلومات، أو سلامتها، أو توافرها، وهي العناصر الأساسية التي تقوم عليها حماية المعلومات والأنظمة الإلكترونية. وفي البيئة المصرفية، تشير الهجمات السيبرانية إلى جميع المحاولات التي تستهدف الأنظمة المصرفية وقواعد البيانات والحسابات والخدمات الإلكترونية بهدف الحصول على الأموال أو البيانات، أو تعطيل العمليات المصرفية، أو التلاعب بالسجلات والمعاملات المالية. وقد تنفذ هذه الهجمات من قبل أفراد أو جماعات إجرامية منظمة أو جهات ذات قدرات تقنية متقدمة، باستخدام وسائل يصعب أحياناً اكتشافها في مراحلها الأولى.

ويرتبط مفهوم الهجوم السيبراني بمفهوم المخاطر السيبرانية، إلا أنهما لا يمتثلان المعنى نفسه؛ فالهجوم السيبراني يمثل الفعل أو المحاولة الفعلية لاختراق الأنظمة أو تعطيلها، بينما تعبر المخاطر السيبرانية عن احتمال وقوع هذا الهجوم وما قد يترتب عليه من خسائر أو آثار سلبية. ولذلك فإن إدارة المخاطر السيبرانية تشمل تحديد التهديدات والثغرات وتقدير احتمالية استغلالها وآثارها، ثم وضع إجراءات الحماية والاستجابة والتعافي المناسبة.

ثانياً: أنواع الهجمات السيبرانية

تتعدد الهجمات السيبرانية التي قد تتعرض لها المصارف، ومن أبرزها هجمات التصيد الإلكتروني، التي تعتمد على إرسال رسائل أو إنشاء مواقع مزيفة تبدو وكأنها صادرة عن المصرف، بهدف خداع العملاء أو الموظفين ودفعهم إلى الإفصاح عن كلمات المرور أو بيانات الحسابات. ويزداد خطر التصيد مع تطور تقنيات الذكاء الاصطناعي، التي يمكن أن تساعد المهاجمين على إعداد رسائل ومقاطع صوتية أو مرئية مزيفة أكثر إقناعاً وتعقيداً (Ahmed & Ashneen, 2026).

ومن الأنواع الشائعة كذلك البرمجيات الخبيثة، التي تشمل الفيروسات وبرامج التجسس وأحصنة طروادة، ويتم استخدامها للوصول إلى الأجهزة والأنظمة وسرقة المعلومات أو مراقبة المستخدمين أو تعطيل العمليات. كما تعد برامج الفدية من أخطر هذه البرمجيات، إذ تقوم بتشفير البيانات أو إيقاف الأنظمة، ثم يطلب المهاجم مبالغاً مالياً لإعادة الوصول إليها. (Abokraa & Abdullah, 2026)

وتشمل الهجمات أيضاً هجمات حجب الخدمة الموزعة، التي تعتمد على إرسال عدد هائل من الطلبات إلى موقع المصرف أو خوادمه بهدف إبطائه أو تعطيله ومنع العملاء من الوصول إلى الخدمات المصرفية. كما توجد هجمات اختراق الحسابات وسرقة بيانات الدخول، التي تستهدف الحسابات المصرفية أو حسابات الموظفين من خلال تخمين كلمات المرور أو سرقتها أو استغلال ضعف المصادقة الإلكترونية (Dileab, 2026; Al-Jaghalli, 2025).

ومن صور الهجمات السيبرانية أيضاً الهندسة الاجتماعية، التي تستهدف العنصر البشري بدلاً من مهاجمة النظام التقني مباشرة، وذلك عن طريق انتحال صفة موظف أو مسؤول أو عميل وإقناع الضحية بإفشاء معلومات سرية أو تنفيذ تحويل مالي. وقد

اتسعت هذه الهجمات لتشمل استخدام الأصوات والصور ومقاطع الفيديو المزيفة لإيهام الموظفين بأن الطلب صادر عن مسؤول حقيقي. (Alazoozey & Shebli, 2026)

وتتعرض المصارف كذلك إلى الهجمات الداخلية التي قد تنتج عن موظف يسيء استخدام الصلاحيات الممنوحة له، سواء بقصد تحقيق منفعة شخصية أو الإضرار بالمصرف، أو نتيجة الإهمال وعدم الالتزام بإجراءات الأمن. كما قد تنشأ الهجمات من خلال مقدمي الخدمات والأطراف الخارجية، كالشركات التي تقدم خدمات الحوسبة السحابية أو البرمجيات أو الاتصالات، مما يجعل مخاطر سلسلة التوريد التقنية من المخاطر المهمة في البيئة المصرفية الحديثة. ويؤكد إطار الأمن السيبراني الصادر عن المعهد الوطني الأمريكي للمعايير والتكنولوجيا أهمية إدماج مخاطر سلسلة التوريد ضمن منظومة حوكمة وإدارة المخاطر السيبرانية (NIST، 2024).

ثالثاً: آثار الهجمات السيبرانية على المصارف

يترتب على الهجمات السيبرانية عدد من الآثار المالية والتشغيلية والقانونية، حيث قد تؤدي إلى سرقة الأموال أو تنفيذ تحويلات غير مصرح بها، أو تحمل المصرف تكاليف استعادة الأنظمة والبيانات وإصلاح الثغرات وتعويض العملاء المتضررين. كما قد يترتب عليها تحمل نفقات إضافية لتطوير أنظمة الحماية والاستعانة بالخبراء، إلى جانب الخسائر الناتجة عن توقف العمليات المصرفية.

وتتمثل الآثار التشغيلية في تعطيل الأنظمة والخدمات الإلكترونية وأجهزة الصراف الآلي وتطبيقات الهاتف والخدمات المرتبطة بالدفع والتحويل، مما يؤثر في قدرة المصرف على تنفيذ أعماله اليومية وخدمة عملائه. وقد يؤدي فقدان البيانات أو تشفيرها إلى صعوبة استعادة العمليات بصورة طبيعية، خاصة عند عدم وجود نسخ احتياطية آمنة وخطط فعالة للاستجابة للحوادث والتعافي منها. ويؤكد NIST ضرورة دمج الاستجابة للحوادث السيبرانية في جميع أنشطة إدارة المخاطر، بما يشمل الاستعداد للحوادث واكتشافه والاستجابة له والتعافي من آثاره (NIST، 2025).

أما الآثار المعلوماتية فتتمثل في المساس بسرية بيانات العملاء أو تعديل السجلات والمعاملات أو إتلافها، بما يهدد دقة المعلومات وسلامة التقارير المالية والمصرفية. وقد تؤدي الهجمات كذلك إلى كشف بيانات الحسابات والبطاقات والمعلومات الشخصية، واستغلالها في عمليات احتيال أو سرقة هوية.

كما يترتب على الهجمات السيبرانية آثار قانونية ورقابية، نتيجة عدم التزام المصرف بالتشريعات والتعليمات المتعلقة بحماية البيانات وأمن المعلومات. وقد يتعرض المصرف لعقوبات أو مطالبات بالتعويض، فضلاً عن خضوعه لمزيد من الرقابة والتحقيقات. وإلى جانب ذلك، قد تتأثر سمعة المصرف وتنخفض ثقة العملاء والمستثمرين فيه، خاصة عندما يعجز عن حماية معلوماتهم أو المحافظة على استمرارية خدماته.

ولا تقف آثار الهجمات عند حدود المصرف المتضرر، بل قد تنتقل إلى بقية المؤسسات المالية نتيجة الترابط بين المصارف وأنظمة الدفع ومقدمي الخدمات التقنية. ولذلك يمثل الخطر السيبراني تهديداً محتملاً للاستقرار المالي، خاصة عندما تستهدف الهجمات مؤسسة كبيرة أو خدمة تقنية مشتركة تعتمد عليها عدة مصارف. وقد بينت الدراسات الرقابية الحديثة أن تحسين البيانات المتعلقة بالتهديدات والثغرات والترابط بين المؤسسات المالية يساعد على قياس الآثار المحتملة للحوادث السيبرانية على المصارف والنظام المالي بصورة أفضل.

وقد أوضحت دراسة موسى (2024) أن تزايد الاعتماد على الخدمات الإلكترونية أدى إلى ارتفاع المخاطر المرتبطة بها، وأن الحد من هذه المخاطر يتطلب دعم إدارة المخاطر، وتعزيز الدور الحوكمي، وتطوير الأنشطة الرقابية والاستشارية للمراجعة الداخلية. كما ترتبط هذه النتيجة بموضوع الدراسة الحالية؛ إذ إن الحد من آثار الهجمات السيبرانية داخل مصرف شمال أفريقيا – فرع صرمان يتوقف على مدى جاهزية المراجعة الداخلية لتقييم هذه المخاطر، وفحص ضوابط الحماية، ومتابعة الاستجابة للحوادث، وتقديم التوصيات التي تعزز سرية المعلومات وسلامتها وتوافرها واستمرارية العمل.

المطلب الثاني: أمن المعلومات في المصارف

يقصد بأمن المعلومات مجموعة السياسات والإجراءات والوسائل التقنية والتنظيمية التي تعتمد عليها المصارف لحماية بياناتها وأنظمتها الإلكترونية من الوصول غير المصرح به، أو الاستخدام أو الإفصاح أو التعديل أو الإتلاف، بما يضمن سلامة العمليات المصرفية واستمرار تقديم الخدمات للعملاء. وتزداد أهمية أمن المعلومات في المصارف نتيجة اعتمادها المتزايد على قواعد البيانات، والتطبيقات المصرفية، وأنظمة الدفع والتحويل الإلكتروني، وما قد يترتب على اختراقها من خسائر مالية وتشغيلية وقانونية، فضلاً عن الإضرار بسمعة المصرف وثقة العملاء.

ويقوم أمن المعلومات على ثلاثة عناصر أساسية، تتمثل في سرية المعلومات، والتي تعني عدم السماح بالوصول إلى البيانات إلا للأشخاص المخولين بذلك؛ وسلامة المعلومات، التي تشير إلى المحافظة على دقة البيانات واكتمالها ومنع تعديلها أو إتلافها بطريقة غير مشروعة؛ وتوافر المعلومات، ويقصد به ضمان إمكانية الوصول إلى الأنظمة والبيانات والاستفادة منها عند الحاجة. وتمثل هذه العناصر الأساس الذي تستند إليه حماية المعلومات المصرفية واستمرارية الأعمال، كما تعد من الجوانب التي ينبغي للمراجعة الداخلية تقييم مدى كفاية الضوابط المرتبطة بها بصورة دورية (NIST، 2024).

وتعتمد المصارف على مجموعة من الضوابط الأمنية، من أهمها تنظيم صلاحيات الدخول إلى الأنظمة، واستخدام المصادقة متعددة العوامل، وتشفير البيانات، وتحديث البرامج بصورة منتظمة، وإعداد النسخ الاحتياطية، ومراقبة الشبكات والأنشطة غير المعتادة، وتوعية الموظفين بالمخاطر السيبرانية، إضافة إلى إعداد خطط للاستجابة للحوادث والتعافي منها. ومن أبرز المعايير الدولية المستخدمة في هذا المجال معيار ISO/IEC 27001:2022 الخاص بنظم إدارة أمن المعلومات، وإطار الأمن السيبراني

NIST CSF 2.0 الصادر عام 2024، الذي يقوم على وظائف الحوكمة والتحديد والحماية والكشف والاستجابة والتعافي (ISO، 2022؛ NIST، 2024).

المطلب الثالث: العلاقة بين جاهزية المراجعة الداخلية والحد من المخاطر السيبرانية

ترتبط جاهزية المراجعة الداخلية ارتباطاً مباشراً بقدرتها على التعامل مع المخاطر السيبرانية والحد من آثارها، حيث تعتمد هذه الجاهزية على توافر الاستقلالية التنظيمية، والكفاءة المهنية والتقنية، والتدريب المستمر، والموارد البشرية والتكنولوجية المناسبة، إلى جانب اعتماد خطط مراجعة قائمة على المخاطر. وكلما ارتفع مستوى جاهزية المراجعة الداخلية، زادت قدرتها على اكتشاف نقاط الضعف وتقييم الضوابط الأمنية ومتابعة الإجراءات التصحيحية قبل تحول المخاطر إلى حوادث فعلية. وتظهر هذه العلاقة من خلال الأبعاد الحديثة للمراجعة الداخلية؛ إذ تساعد أنشطة إدارة المخاطر على تحديد التهديدات السيبرانية وتقييم احتمالية وقوعها وقياس آثارها، بينما يسهم الدور الحوكمي في التأكد من وضوح المسؤوليات، وفاعلية إشراف الإدارة ومجلس الإدارة، ومدى الالتزام بالسياسات والمعايير الأمنية. كما تتحقق إضافة القيمة من خلال تقديم المراجعة الداخلية للتوصيات والاستشارات التي تساعد على تطوير الضوابط، وتحسين الاستجابة للحوادث، وتعزيز أمن المعلومات واستمرارية العمل.

وقد أوضحت دراسة موسى (2024) أن الأنشطة الحديثة للمراجعة الداخلية تسهم في الحد من مخاطر الخدمات الإلكترونية، من خلال دعم إدارة المخاطر والحوكمة وتقديم التوصيات التي تحسن الضوابط الرقابية. كما أشارت دراسة جديع ومحمد (2025) إلى أن تعزيز دور المراجعة الداخلية في إدارة المخاطر السيبرانية يتطلب توافر التأهيل المهني والتقني، والتدريب المستمر، والاستقلالية، وإمكانية الوصول إلى المعلومات الضرورية.

وبناءً على ذلك، تقوم الدراسة الحالية على أن ارتفاع مستوى جاهزية المراجعة الداخلية بأبعدها المتمثلة في إدارة المخاطر، والدور الحوكمي، وإضافة القيمة، يسهم في تعزيز أمن المعلومات والحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا – فرع صرمان.

الدراسة الميدانية:

وتحقيقاً لأهداف الدراسة استخدم الباحثان المنهج الوصفي التحليلي للتعرف على مستوى جاهزية المراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية وأمن المعلومات بمصرف شمال أفريقيا صرمان، وذلك من خلال الرجوع والاطلاع على الكتب والدوريات والمجلات.

ويتكون مجتمع الدراسة من مصرف شمال أفريقيا فرع صرمان، فيما كانت العينة من المراجعين الداخليين، والعاملين بإدارة تقنية المعلومات، والمدير ورؤساء الأقسام، وموظفي مصرف شمال أفريقيا فرع صرمان، كما تم تصميم استبانة مكونة أربعة أجزاء، الجزء الأول معلومات عامة عن عينة الدراسة، أما الجزء الثاني مكون من (9) فقرات، لتغطية الجوانب المتعلقة بمحور إدارة المخاطر، والجزء الثالث يتكون من (9) فقرات تتعلق بمحور الدور الحوكمي للمراجعة الداخلية، كما أهتم الجزء الرابع بمحور إضافة القيمة في (9) فقرات، حيث تم توزيع (40) استبانة أسلم منها (36) استبانة صالحة لتحليل فقراتها. وقد تم استخدام مقياس ليكرت الخماسي (Likert scale) في الإجابة على استبانة الدراسة المتعلقة بالمتغيرات المستقلة للبحث، وقد أعطيت الإجابات الدرجات التالية: موافق بشدة: 5 درجات، موافق: 4 درجات، موافق إلى حد ما: 3 درجات، غير موافق: 2 درجتان، غير موافق بشدة: 1 درجة.

هذا وقد تم تحديد درجة القوة والضعف في مستوى جاهزية المراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية وأمن المعلومات بمصرف شمال أفريقيا صرمان محل الدراسة من خلال متوسط إجابات الفقرات ونسبة الجاهزية وهي من 1 إلى أقل من 1.80 درجة وما نسبته 20%-36% تعتبر ضعيفة جداً، ومن 1.80 إلى أقل من 2.60 درجة وما نسبته 36%-52% تعتبر ضعيفة، ومن 2.60 إلى أقل من 3.40 درجة وما نسبته 52%-68% تعتبر متوسطة، ومن 3.40 إلى أقل من 4.20 وما نسبته 68%-84% تعتبر جيدة، ومن 4.20 إلى 5 وما نسبته 84%-100% تعتبر مرتفعة، وهذا واعتمد الباحثان على وسط حسابي فرضي مقداره (68%) والذي يمثل درجة الجاهزية والتي تقع ضمن نسبة الجاهزية (من 68% إلى أقل من 84%) واعتبر الوسط الحسابي (3.4) هو المتغير التابع والتي يمكن أن يقبل بها الباحثان لقياس درجة مستوى جاهزية المراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية وأمن المعلومات بمصرف شمال أفريقيا صرمان، وتم توزيع الاستبانة على عينة الدراسة، تم تحليل بياناتها باستخدام البرنامج الإحصائي (SPSS)، والذي من خلاله تم تطبيق الاختبارات الإحصائية، كما تم استخدام القاعدة الأساسية المتبعة لاتخاذ القرار هو أن تكون قيمة p-value أكبر من (0.05) نقبل فرضية العدم أي وجود استقلالية وعدم وجود فروقات ذات دلالة إحصائية وإذا كانت قيمة p-value أصغر من (0.05) نرفض فرضية العدم، وتحقق الباحثان من الصدق المنطقي للاستبانة بعد أن تم عرضها على مجموعة من أساتذة المحاسبة، بالإضافة إلى بعض المتخصصين في الإحصائي، وقد تم إدخال بعض التعديلات على بنود الاستبانة على ضوء ملاحظاتهم واقتراحاتهم.

واستخدم الباحثان معادلة كورنباخ ألفا (Cornbach,s Alpha) للتحقق من ثبات الاستبانة لكل جزء من أجزائها وكانت معاملات الثبات تتمتع بدلالات ثبات واتساق مقبولة لغايات الدراسة العلمي، ويتضح أن قيمة ألفا لفقرات الاستبانة مجتمعة بلغت (88.2%) وهذه النسبة ممتازة وهذا يعني توفر درجة عالية جداً من المصداقية والثبات في إجابات الفقرات.

تحليل البيانات واختبار الفرضيات

1- تحليل بيانات مجتمع وعينة الدراسة:

يتكون مجتمع الدراسة من موظفي مصرف شمال أفريقيا فرع صرمان، ويبين الجدول رقم(1) خصائص عينة الدراسة:

جدول رقم (1) خصائص عينة الدراسة

معلومات عامة	البيان	التكرار	النسبة المئوية %
العمر	أقل من 30 سنة	4	11.1
	من 30 سنة إلى أقل من 40 سنة	10	27.8
	من 40 سنة إلى أقل من 50 سنة	17	47.2
	من 50 سنة فأكثر	5	13.9
المؤهل العلمي	بكالوريوس	17	47.2
	ماجستير	11	30.6
	دكتوراه	2	5.6
	أخرى	6	16.7
التخصص	محاسبة	21	58.3
	إدارة أعمال	10	27.8
	تقنية معلومات	4	11.1
	أخرى	1	2.8
سنوات الخبرة	أقل من 5 سنوات	5	13.9
	من 5 إلى أقل من 10 سنوات	8	22.2
	من 10 سنة فأكثر	23	63.9

ويتضح من الجدول (1) :

- إن أغلب أفراد عينة الدراسة أعمارهم تزيد عن 40 سنة، حيث شكلت نسبتهم مجتمعه (61.1%)، وتدل هذه النسبة على مدى أدراك موظفي مصرف شمال أفريقيا فرع صرمان لأهمية المراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية وأمن المعلومات .

- إن أغلب أفراد عينة الدراسة يحملون درجة علمية عالية حيث بلغت نسبة الحاصلين على درجة البكالوريوس (47.2%) من عينة الدراسة، فيما شكلت نسبة الحاملين للمؤهل العلمي الماجستير (30.6%)، وهذا يدل على مستوى التأهيل العلمي المناسب ومن ثم حملة الدكتوراه وبنسبة بلغت (5.6%) وهذا يدل

- إن أكثر من نصف عينة الدراسة تخصصهم محاسبة حيث بلغت نسبتهم (58.3%)، فيما كانت نسبة تخصص تقنية المعلومات (11.1%)، وهذه النسبة مناسبة جداً لتعاون المتخصصين في تقنية المعلومات مع التخصصات المحاسبية والإدارية الأخرى .

- إن أكثر أفراد عينة الدراسة لديهم خبرة تزيد عن 10 سنوات حيث بلغت نسبتهم (63.9%) من عينة الدراسة، فيما كانت نسبة الذين لديهم خبرة ما بين 5 سنوات إلى أقل من 10 سنوات كانت نسبتهم (22.2%) من عينة الدراسة، وهذا يدل أن سنوات الخبرة تأتي مناسبة لطبيعة المهام والأعمال الموكلة إليهم ومدي جاهزيتهم .

2. اختبار الفرضيات:

يهدف الإحصاء الوصفي إلى تقديم مقاييس تلخيصية للبيانات المتوفرة عن عناصر العينة حيث استخدمت مقاييس النزعة المركزية ومقاييس التشتت ومقاييس تجمع بين مقاييس النزعة المركزية ومعايير التشتت، واختبار (t-test)، واختبار الارتباط بيرسون .

فرضيات الدراسة:

يهدف هذا الدراسة إلى تقييم مستوى جاهزية المراجعة الداخلية بأبعادها الحديثة في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا – فرع صرمان، وتم اختبار الفرضية الرئيسية القائلة ((يوجد مستوى مرتفع من جاهزية المراجعة الداخلية بأبعادها الحديثة في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا فرع صرمان)) ومن خلال الفرضيات الفرعية التالية:

الفرضية الأولى:

" يوجد مستوى مرتفع من جاهزية أنشطة إدارة المخاطر بالمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا فرع صرمان "، تم اختبار هذه الفرضية من خلال الفقرات (1-9) من الاستبانة، كما في الجدول رقم (2).
جدول رقم (2) نتائج التحليل المتعلقة بمحور جاهزية أنشطة إدارة المخاطر بالمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا فرع صرمان

الفقرة	المجموعات	الوسط الحسابي	النسبة %	الانحراف المعياري	معامل الاختلاف %	الأهمية الترتيبية
1.	المراجعة الداخلية تساهم في تحديد وتقييم المخاطر السيبرانية.	4.47	89.44	0.941	21.03	الأولى
2.	يتم تحديث خطط إدارة المخاطر بشكل دوري لمواكبة التهديدات السيبرانية.	4.33	86.67	0.956	22.07	الثالثة
3.	المراجعة الداخلية توفر تقارير دقيقة حول مستوى المخاطر السيبرانية.	4.22	84.44	1.098	26.01	الرابعة

4.	هناك آليات واضحة لرصد محاولات الاختراق مبكراً.	3.92	78.33	1.052	26.86	السابعة
5.	يتم إشراك المراجعة الداخلية في وضع خطط الطوارئ لمواجهة الهجمات السيبرانية.	3.92	78.33	1.180	30.13	السابعة مكرر
6.	المراجعة الداخلية تساهم في تقليل احتمالية حدوث خسائر مالية بسبب الهجمات السيبرانية.	4.03	80.56	1.000	24.82	السادسة
7.	يتم تدريب المراجعين الداخليين على مواجهة خطر الهجمات السيبرانية.	3.89	77.78	1.141	29.34	الثامنة
8.	المراجعة الداخلية تساهم في تعزيز قدرة المصرف على الاستجابة السريعة للهجمات.	4.06	81.11	1.241	30.60	الخامسة
9.	يتم تقييم فعالية أنشطة إدارة المخاطر بشكل دوري من قبل المراجعة الداخلية.	4.36	87.22	0.833	19.11	الثانية
متوسط محور جاهزية أنشطة إدارة المخاطر بالمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا فرع صرمان		4.13	82.65	0.546	13.22	
اختبار T-test المزدوج						
قيمة (t)		8.050				
درجة الحرية		35				
مستوى المعنوية (t)		0.000				
مستوى الثقة		0.050				

ويوضح الجدول رقم (2) نتائج اختبار الفرضية والذي جاء في تسعة فقرات حيث جاء المتوسط الحسابي لمجموع فقرات الفرضية المتعلقة بمستوى جاهزية أنشطة إدارة المخاطر بالمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا فرع صرمان (4.13) وما نسبته (82.65%) وهي نسبة تقع في درجة الجاهزية الجيدة والتي وسطها الحسابي ما بين (3.40 إلى أقل من 4.20) وما نسبته (68% إلى أقل من 84%) وليس هناك اختلاف كبير في إجابات عينة الدراسة حول فقرات الاستبانة حيث بلغ معامل الاختلاف لمجموع الفقرات (13.22%) وهو يدل على تجانس وتوافق وانسجام فيما بينهم، فيما بلغ الانحراف المعياري للفرضية ما نسبته (0.546) وهذا يدل على تمحور إجابات عينة الدراسة حول الوسط الحسابي العام للفقرات محل الدراسة.

جاءت الفقرات رقم (1) في الترتيب الأول بوسط حسابي بلغ (4.47) وما نسبته (89.4%) وهي تقع في درجة الجاهزية المرتفعة، بأن المراجعة الداخلية تساهم في تحديد وتقييم المخاطر السيبرانية، فيما كانت الفقرة رقم (9) في الترتيب الثاني والمتعلقة بتقييم فعالية أنشطة إدارة المخاطر بشكل دوري من قبل المراجعة الداخلية، وهي كذلك تقع في درجة الجاهزية المرتفعة وبوسط حسابي بلغ (4.36) وما نسبته (87.22%)، كما أن معامل الاختلاف لهذه الفقرات يعتبر ممتاز من حيث الانسجام والتوافق بين أفراد عينة الدراسة في الإجابة على هذا الفقرات حيث بلغ (21.0%، 19.11%) على التوالي، وكذلك الانحراف المعياري يدل على عدم وجود تشتت كبير في الإجابات.

فيما جاءت الفقرات رقم (2، 3) ضمن فترة الجاهزية المرتفعة، حيث كان المتوسط الحسابي (من 4.20 إلى 5) وما نسبته (من 84% إلى 100%) من حيث تحديث خطط إدارة المخاطر بشكل دوري لمواكبة التهديدات السيبرانية، وأن المراجعة الداخلية توفر تقارير دقيقة حول مستوى المخاطر السيبرانية.

كما جاءت الفقرات رقم (4، 5، 6، 7، 8) من ضمن الفقرات المتعلقة بالجاهزية الجيدة حيث كان الوسط الحسابي ونسبته لهذه الفقرات ما بين (من 3.4 إلى أقل من 4.2) وما نسبته (من 68% إلى أقل من 84%)، مما يدل على أن المراجعة الداخلية تساهم في تعزيز قدرة المصرف على الاستجابة السريعة للهجمات، وتساهم في تقليل احتمالية حدوث خسائر مالية بسبب الهجمات السيبرانية، كما أن هناك آليات واضحة لرصد محاولات الاختراق مبكراً، ويتم إشراك المراجعة الداخلية في وضع خطط الطوارئ لمواجهة الهجمات السيبرانية، كما يتم تدريب المراجعين الداخليين على مواجهة خطر الهجمات السيبرانية.

عند إجراء اختبار T-test المزدوج لقياس الدلالة الإحصائية بين كل من الوسط الحسابي لمستوى جاهزية أنشطة إدارة المخاطر بالمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا فرع صرمان وبين الوسط الحسابي الفرضي لمستوى الجاهزية (3.40) الذي يمثل الحد الأدنى للدرجة الجيدة للجاهزية، يتبين أن هناك مستوى عالي من الدلالة الإحصائية حيث كانت قيمة (t = 8.050) وكان مستوى معنوية t تساوى (0.000) وهذا المستوى ذا دلالة إحصائية قوية.

كما تم اختبار هذه الفرضية بتحليل الارتباط (باستخدام معامل الارتباط بيرسون)، كما في الجدول رقم (3).

جدول رقم (3) نتائج التحليل المتعلقة بمستوى جاهزية أنشطة إدارة المخاطر بالمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا فرع صرمان

المتغير	قيمة معامل بيرسون	مستوى المعنوية
محور أنشطة إدارة المخاطر بالمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا فرع صرمان	0.838	0.000
مستوى الجاهزية		(82.65%) .

ويلاحظ أن قيمة اختبار معامل بيرسون بلغت (0.838) وبمستوى المعنوية لمعامل بيرسون بلغ (0.000) وهو أقل من مستوى الدلالة المعتمد بالدراسة والبالغ (0.05) مما يدل على وجود علاقة احصائية موجبة لمعامل الارتباط بيرسون وقوة (83.3%) وهو ارتباط موجب و ممتاز جداً.

وبناء على ما تقدم فإنه نقبل الفرضية القائلة على (يوجد مستوى مرتفع من جاهزية أنشطة إدارة المخاطر بالمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا فرع صرمان) بدرجة جاهزية جيدة بلغت نسبتها (82.65%) .
الفرضية الثانية :

" يوجد مستوى مرتفع من جاهزية الدور الحوكمي للمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا فرع صرمان "، تم اختبار هذه الفرضية من خلال الفقرات (1-9) من الاستبانة، كما في الجدول رقم (4).
جدول رقم (4) نتائج التحليل المتعلقة بمحور جاهزية الدور الحوكمي للمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا فرع صرمان

الفقرة	المجموعات	الوسط الحسابي	النسبة %	الانحراف المعياري	معامل الاختلاف %	الاهمية الترتيبية
1.	المراجعة الداخلية تضمن التزام المصرف بسياسات الأمن السيبراني.	4.33	86.67	0.986	22.74	الأولى
2.	هناك تنسيق فعال بين المراجعة الداخلية وإدارة تقنية المعلومات.	4.19	83.89	1.009	24.06	الرابعة
3.	يتم رفع تقارير دورية للإدارة العليا حول جاهزية الضوابط الأمنية.	4.31	86.11	0.889	20.64	الثانية
4.	المراجعة الداخلية تساهم في تعزيز الشفافية في تطبيق سياسات الأمن السيبراني.	4.08	81.67	0.996	24.40	السادسة
5.	يتم التحقق من مدى التزام الموظفين بإجراءات الأمن السيبراني بشكل دوري.	3.94	78.89	1.241	31.46	السابعة
6.	المراجعة الداخلية تساهم في تعزيز ثقافة الالتزام بالحوكمة داخل المصرف.	3.94	78.89	1.241	31.46	السابعة مكرر
7.	هناك متابعة مستمرة لتطبيق تعليمات مصرف ليبيا المركزي المتعلقة بالأمن السيبراني.	4.31	86.11	0.822	19.09	الثانية مكرر
8.	المراجعة الداخلية تساهم في تقليل المخاطر الناتجة عن ضعف الالتزام بالحوكمة.	4.11	82.22	1.090	26.50	الخامسة
9.	يتم تقييم كفاءة الضوابط الأمنية وفق معايير الحوكمة المعتمدة.	4.28	85.56	0.974	22.78	الثالثة
	متوسط محور جاهزية الدور الحوكمي للمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا فرع صرمان	4.17	83.33	0.582	13.96	
اختبار T-test المزدوج						
قيمة (t)		7.909				
درجة الحرية		35				
مستوى المعنوية (t)		0.000				
مستوى الثقة		0.050				

ويوضح الجدول رقم (4) نتائج اختبار الفرضية والذي جاء في تسعة فقرات حيث جاء المتوسط الحسابي لمجموع فقرات الفرضية المتعلقة بمستوى جاهزية الدور الحوكمي للمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا فرع صرمان (4.17) وما نسبته (83.33%) وهي نسبة تقع في درجة الجاهزية الجيدة والتي وسطها الحسابي ما بين (3.40 إلى أقل من 4.20) وما نسبته (68% إلى أقل من 84%) وليس هناك اختلاف كبير في إجابات عينة الدراسة حول فقرات الاستبانة حيث بلغ معامل الاختلاف لمجموع الفقرات (13.96%) وهو يدل على تجانس وتوافق وانسجام ممتاز فيما بينهم، فيما بلغ الانحراف المعياري للفرضية ما نسبته (0.582) وهذا يدل على تمحور إجابات عينة الدراسة حول الوسط الحسابي العام للفقرات محل الدراسة.

جاءت الفقر رقم (1) في الترتيب الأول بوسط حسابي بلغ (4.33) وما نسبته (86.67%) وهي تقع في درجة الجاهزية المرتفعة، بأن المراجعة الداخلية تضمن التزام المصرف بسياسات الأمن السيبراني، فيما كانت الفقرة رقم (3) في الترتيب الثاني والمتعلقة برفع تقارير دورية للإدارة العليا حول جاهزية الضوابط الأمنية ، وهي كذلك تقع في درجة الجاهزية المرتفعة وبوسط حسابي بلغ (4.31) وما نسبته (86.11%)، وجاءت أيضاً الفقرة رقم (9) في الترتيب الثالث وفي درجة الجاهزية المرتفعة من حيث يتم تقييم كفاءة الضوابط الأمنية وفق معايير الحوكمة المعتمدة، و بوسط حسابي بلغ (4.28) وما نسبته (85.56%)، كما أن معامل الاختلاف لهذه الفقرات يعتبر ممتاز من حيث الانسجام والتوافق بين أفراد عينة الدراسة في

الاجابة على هذا الفقرات حيث بلغ (22.7%، 20.64%) على التوالي، وكذلك الانحراف المعياري يدل على عدم وجود تشتت كبير في الاجابات .

فيما جاءت الفقرات رقم (2، 4، 5، 6) ضمن فترة الجاهزية الجيدة حيث كان الوسط الحسابي ونسبته لهذه الفقرات ما بين (3.4 إلى أقل من 4.2) وما نسبته (68% إلى أقل من 84%)، مما يدل على أن هناك تنسيق فعال بين المراجعة الداخلية وإدارة تقنية المعلومات، وأن المراجعة الداخلية تساهم في تقليل المخاطر الناتجة عن ضعف الالتزام بالحوكمة، كما أن هناك مساهمة للمراجعة الداخلية في تعزيز الشفافية في تطبيق سياسات الأمن السيبراني، ويتم التحقق من مدى التزام الموظفين بإجراءات الأمن السيبراني بشكل دوري، كما أن المراجعة الداخلية تساهم في تعزيز ثقافة الالتزام بالحوكمة داخل المصرف.

عند إجراء اختبار T-test المزدوج لقياس الدلالة الإحصائية بين كل من الوسط الحسابي لمستوى جاهزية الدور الحوكمي للمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا فرع صرمان وبين الوسط الحسابي الفرضي لمستوى الجاهزية (3.40) الذي يمثل الحد الأدنى للدرجة الجيدة للجاهزية، يتبين أن هناك علاقة إحصائية قوية فيما بينهم حيث بلغت قيمة $t = 7.99$ وكان مستوى معنوية t تساوى (0.000) وهذا المستوى ذا دلالة إحصائية قوية . كما تم اختبار هذه الفرضية بتحليل الارتباط (باستخدام معامل الارتباط بيرسون)، كما في الجدول رقم (5).
جدول رقم (5) نتائج التحليل المتعلقة بمستوى جاهزية الدور الحوكمي للمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا فرع صرمان

المتغير	قيمة معامل بيرسون	مستوى المعنوية
محور الدور الحوكمي للمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا فرع صرمان	0.926	0.000
مستوى الجاهزية		(83.33%)

وبلاحظ أن قيمة اختبار معامل بيرسون بلغت (0.926) وبمستوى المعنوية لمعامل بيرسون بلغ (0.000) وهو أقل من مستوى الدلالة المعتمد بالدراسة والبالغ (0.05) مما يدل على وجود علاقة إحصائية موجبة لمعامل الارتباط بيرسون وقوة (92.6%) وهو ارتباط موجب وممتاز جداً.

وبناء على ما تقدم فإنه نقبل الفرضية القائلة على (يوجد مستوى مرتفع من جاهزية الدور الحوكمي للمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا فرع صرمان) بدرجة جاهزية جيدة بلغت نسبتها (83.33%) الفرضية الثالثة:

" يوجد مستوى مرتفع من جاهزية أنشطة إضافة القيمة بالمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا فرع صرمان "، تم اختبار هذه الفرضية من خلال الفقرات (1-9) من الاستبانة، كما في الجدول رقم (6).
جدول رقم (6) نتائج التحليل المتعلقة بمحور جاهزية أنشطة إضافة القيمة بالمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا فرع صرمان.

الفقرة	المجموعات	الوسط الحسابي	النسبة %	الانحراف المعياري	معامل الاختلاف %	الاهمية الترتيبية
1.	المراجعة الداخلية تقدم توصيات عملية تقلل من احتمالية الهجمات السيبرانية.	4.17	83.33	0.941	22.59	الثالثة
2.	المراجعة الداخلية تساهم في تعزيز ثقة العملاء في الخدمات الإلكترونية.	4.36	87.22	0.867	19.88	الأولى
3.	المراجعة الداخلية تدعم استمرارية الأداء المالي والتشغيلي للمصرف.	4.14	82.78	1.073	25.93	الرابعة
4.	المراجعة الداخلية تساهم في تحسين جودة الخدمات الإلكترونية المقدمة للعملاء.	4.22	84.44	0.959	22.72	الثانية
5.	يتم الأخذ بتوصيات المراجعة الداخلية في تطوير أنظمة الأمن السيبراني.	3.92	78.33	1.228	31.34	السابعة
6.	المراجعة الداخلية تساهم في تعزيز القدرة التنافسية للمصرف.	4.22	84.44	0.898	21.27	الثانية مكرر
7.	المراجعة الداخلية توفر قيمة مضافة من خلال تحسين كفاءة استخدام الموارد التقنية.	3.89	77.78	1.214	31.21	الثامنة
8.	المراجعة الداخلية تساهم في تقليل التكاليف الناتجة عن معالجة آثار الهجمات السيبرانية.	4.06	81.11	1.120	27.61	الخامسة
9.	المراجعة الداخلية تدعم الابتكار في تطوير حلول أمنية جديدة.	3.97	79.44	1.055	26.57	السادسة
	متوسط محور جاهزية أنشطة إضافة القيمة بالمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا فرع صرمان	4.10	82.10	0.621	15.13	
اختبار T-test المزدوج						
	قيمة (t)	6.809				
	درجة الحرية	35				
	مستوى المعنوية (t)	0.000				
	مستوى الثقة	0.05				

ويوضح الجدول رقم (6) نتائج اختبار الفرضية والذي جاء في تسعة فقرات حيث جاء المتوسط الحسابي لمجموع فقرات الفرضية المتعلقة بمستوى جاهزية أنشطة إضافة القيمة بالمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا فرع صرمان (4.10) وما نسبته (82.10%) وهي نسبة تقع في درجة الجاهزية الجيدة والتي وسطها الحسابي ما بين (3.40 إلى أقل من 4.20) وما نسبته (68% إلى أقل من 84%) وليس هناك اختلاف كبير في إجابات عينة الدراسة حول فقرات الاستبانة حيث بلغ معامل الاختلاف لمجموع الفقرات (15.13%) وهو يدل على تجانس وتوافق وانسجام ممتاز فيما بينهم، فيما بلغ الانحراف المعياري للفرضية ما نسبته (0.621) وهذا يدل على تمحور إجابات عينة الدراسة حول الوسط الحسابي العام للفقرات محل الدراسة.

جاءت الفقر رقم (2) في الترتيب الأول بوسط حسابي بلغ (4.36) وما نسبته (87.22%) وهي تقع في درجة الجاهزية المرتفعة، بأن المراجعة الداخلية تساهم في تعزيز ثقة العملاء في الخدمات الإلكترونية، فيما كانت الفقرتان رقم (4، 6) في الترتيب الثاني والمتعلقة بأن المراجعة الداخلية تساهم في تحسين جودة الخدمات الإلكترونية المقدمة للعملاء، وفي تعزيز القدرة التنافسية للمصرف، وبوسط حسابي بلغ (4.22) وما نسبته (84.44%)، كما أن معامل الاختلاف لهذه الفقرات يعتبر ممتاز من حيث الانسجام والتوافق بين أفراد عينة الدراسة في الإجابة على هذا الفقرات حيث بلغ (22.72%، 19.88%) على التوالي، وكذلك الانحراف المعياري يدل على عدم وجود تشتت كبير في الإجابات.

فيما جاءت الفقرات رقم (1، 3، 8، 9، 5، 7) في الترتيب الثالث والرابع والخامس والسادس والسابع والثامن على التوالي، وضمن فترة الجاهزية الجيدة، حيث كان المتوسط الحسابي (4.17، 4.14، 4.06، 3.97، 3.92، 3.89) على التوالي وما نسبته (83.33%، 82.78%، 81.11%، 79.44%، 78.33%، 77.78%) على التوالي، من حيث أن المراجعة الداخلية تقدم توصيات عملية تقلل من احتمالية الهجمات السيبرانية، وتدعم استمرارية الأداء المالي والتشغيلي للمصرف، كما أن المراجعة الداخلية تساهم في تقليل التكاليف الناتجة عن معالجة آثار الهجمات السيبرانية، وكذلك تدعم الابتكار في تطوير حلول أمنية جديدة، ويتم الأخذ بتوصيات المراجعة الداخلية في تطوير أنظمة الأمن السيبراني، كما أن المراجعة الداخلية توفر قيمة مضافة من خلال تحسين كفاءة استخدام الموارد التقنية.

عند إجراء اختبار T-test المزدوج لقياس الدلالة الإحصائية بين كل من الوسط الحسابي لمستوى جاهزية أنشطة إضافة القيمة بالمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا فرع صرمان وبين الوسط الحسابي الفرضي لمستوى الجاهزية (3.40) الذي يمثل الحد الأدنى للدرجة الجيدة للجاهزية، يتبين أن هناك مستوى عالي من الدلالة الإحصائية حيث كانت قيمة $t = 6.809$ وكان مستوى معنوية t تساوى (0.000) وهذا المستوى ذا دلالة إحصائية قوية. كما تم اختبار هذه الفرضية بتحليل الارتباط (باستخدام معامل الارتباط بيرسون)، كما في الجدول رقم (7).

جدول رقم (7) نتائج التحليل المتعلقة بمستوى جاهزية أنشطة إضافة القيمة بالمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا فرع صرمان

المتغير	قيمة معامل بيرسون	مستوى المعنوية
محور أنشطة إضافة القيمة بالمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا فرع صرمان	0.899	0.000
مستوى الجاهزية		(82.10%)

ويلاحظ أن قيمة اختبار معامل بيرسون بلغت (0.899) وبمستوى المعنوية لمعامل بيرسون بلغ (0.000) وهو أقل من مستوى الدلالة المعتمد بالدراسة والبالغ (0.05) مما يدل على وجود علاقة إحصائية موجبة لمعامل الارتباط بيرسون وقوة (89.9%) وهو ارتباط موجب قوي وممتاز جداً.

وبناء على ما تقدم فإنه نقبل الفرضية القائلة على (يوجد مستوى مرتفع من جاهزية أنشطة إضافة القيمة بالمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا فرع صرمان) بدرجة جاهزية جيدة بلغت نسبته (82.10%).

ومما سبق يُمكن اختبار الفرضية الرئيسية القائلة ((يوجد مستوى مرتفع من جاهزية المراجعة الداخلية بأبعادها الحديثة في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا فرع صرمان)) للتعرف على مستوى الجاهزية يتبين الاتي :

جدول رقم (8) نتائج التحليل المتعلقة بمستوى جاهزية المراجعة الداخلية بأبعادها الحديثة في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا فرع صرمان

ت	الفرضيات	الوسط الحسابي	النسبة %	الانحراف المعياري	معامل الاختلاف %	الأهمية الترتيبية
1.	متوسط محور جاهزية أنشطة إدارة المخاطر بالمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا فرع صرمان.	4.13	82.65	0.546	13.22	الثانية
2.	متوسط محور جاهزية الدور الحوكمي للمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا فرع صرمان	4.17	83.33	0.582	13.96	الأولى
3.	متوسط محور جاهزية أنشطة إضافة القيمة بالمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا فرع صرمان	4.10	82.10	0.621	15.13	الثالثة
	المتوسط العام لمستوى الجاهزية المراجعة الداخلية بأبعادها الحديثة في الحد من مخاطر الهجمات السيبرانية	4.13	82.70	0.518	12.53	

اختبار T-test المزدوج	
قيمة (t)	8.510
درجة الحرية	35
مستوى المعنوية (t)	0.000
مستوى الثقة	0.050

ومن خلال الفرضيات السابقة يتبين بأن الوسط الحسابي العام لمجموع الفقرات بلغ (4.13) وبنسبه بلغت (82.70%) كما يتضح بأن هناك توافق وانسجام فيما بين عينة الدراسة من خلال معامل الاختلاف البالغ (12.53%) وليس هناك تشتت من خلال الانحراف المعياري البالغ (0.518).

عند إجراء اختبار T-test المزدوج لقياس الدلالة الإحصائية بين كل من الوسط الحسابي لمستوى جاهزية المراجعة الداخلية بأبعادها الحديثة في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا فرع صرمان وبين الوسط الحسابي الفرضي لمستوى الجاهزية (3.40) الذي يمثل الحد الأدنى للدرجة الجيدة للجاهزية، يتبين أنه ذا دلالة إحصائية قوية حيث كانت قيمة $t = 8.510$ وكانت معنوية t تساوي (0.000) وهذا المستوى ذا دلالة إحصائية لأنه أكبر من مستوى الدلالة المعتمد بالبحث والبالغ (0.050) (5%).

وبناء على ما تقدم فإنه نقبل الفرضية الرئيسية التي تنص على (يوجد مستوى مرتفع من جاهزية المراجعة الداخلية بأبعادها الحديثة في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا فرع صرمان) بدرجة جاهزية جيدة بلغت نسبتها (82.70%).

الاستنتاجات و التوصيات

في ضوء نتائج الدراسة فيما يتعلق بمستوى الجاهزية للمراجعة الداخلية في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا فرع صرمان، يورد الباحثان أهم الاستنتاجات والتوصيات ذات العلاقة .

الاستنتاجات :

انطلاقاً من أهمية جاهزية المراجعة الداخلية بأبعادها الحديثة في الحد من مخاطر الهجمات السيبرانية بمصرف شمال أفريقيا فرع صرمان، ولما تمثله المهنة من دور هام وأساسي في المصرف من خلال الأعمال والنشاطات الاقتصادية، توصل الباحثان إلى الاستنتاجات التالية:

- 1- أظهرت نتائج الدراسة وجود مستوى جيد من جاهزية المراجعة الداخلية بأبعادها الحديثة في الحد من مخاطر الهجمات السيبرانية وأمن المعلومات بمصرف شمال أفريقيا – فرع صرمان.
- 2- تبين أن بعد إدارة المخاطر يتمتع بمستوى جاهزية جيد، مما يعكس اهتمام المصرف بتحديد المخاطر السيبرانية وتقييمها وتحديث خطط إدارتها بصورة دورية.
- 3- أظهرت النتائج أن الدور الحوكمي للمراجعة الداخلية يسهم بفاعلية في تعزيز الالتزام بسياسات الأمن السيبراني، ورفع التقارير الدورية، ومتابعة تطبيق تعليمات مصرف ليبيا المركزي ذات العلاقة.
- 4- أوضحت الدراسة أن إضافة القيمة تمثل أحد الأبعاد المهمة للمراجعة الداخلية، من خلال تقديم التوصيات والاستشارات التي تسهم في تحسين الضوابط الأمنية، وتعزيز ثقة العملاء، ودعم استمرارية العمل.
- 5- أثبتت نتائج التحليل الإحصائي وجود دلالة إحصائية تؤيد الفرضية الرئيسية والفرضيات الفرعية، بما يؤكد أن جاهزية المراجعة الداخلية بأبعادها الحديثة تسهم في الحد من مخاطر الهجمات السيبرانية وأمن المعلومات.
- 6- كشفت النتائج عن وجود مستوى مرتفع من الاتفاق بين أفراد عينة الدراسة حول أهمية دور المراجعة الداخلية في تعزيز أمن المعلومات وتقليل الآثار المحتملة للهجمات السيبرانية.
- 7- أكدت الدراسة أن التطور المستمر في التهديدات السيبرانية يتطلب تطويراً مستمراً لقدرات المراجعة الداخلية بما يضمن مواكبة المخاطر التقنية الحديثة.

التوصيات:

بعد عرض النتائج والاستنتاجات، يوصي الباحثان بما يلي:

- 1- الاستمرار في تطوير جاهزية المراجعة الداخلية من خلال تحديث خطط المراجعة لتكون مبنية على المخاطر السيبرانية المستجدة.
- 2- تنظيم برامج تدريبية متخصصة للمراجعين الداخليين في مجالات الأمن السيبراني وأمن المعلومات وتقنيات المراجعة الرقمية.
- 3- تعزيز التعاون والتنسيق بين إدارة المراجعة الداخلية وإدارة تقنية المعلومات وإدارة المخاطر لضمان سرعة اكتشاف التهديدات والاستجابة لها.
- 4- دعم تطبيق مبادئ الحوكمة وتعزيز استقلالية إدارة المراجعة الداخلية بما يرفع من كفاءة دورها الرقابي والاستشاري.
- 5- الاستمرار في تحديث الضوابط والإجراءات الأمنية بما يتوافق مع تعليمات مصرف ليبيا المركزي والمعايير الدولية الخاصة بالأمن السيبراني وأمن المعلومات.
- 6- الاهتمام بإجراء تقييمات دورية لفاعلية الضوابط الأمنية وخطط استمرارية الأعمال والتعافي من الكوارث لضمان جاهزية المصرف لمواجهة الحوادث السيبرانية.

7- الاستفادة من نتائج المراجعة الداخلية في تطوير السياسات والإجراءات المتعلقة بحماية المعلومات، بما يساهم في تعزيز الثقة بالخدمات المصرفية الإلكترونية.

8- تشجيع إجراء المزيد من الدراسات المستقبلية حول جاهزية المراجعة الداخلية في مصارف ليبية أخرى، أو دراسة علاقتها بمتغيرات حديثة مثل الذكاء الاصطناعي، والمراجعة الرقمية، وحوكمة تكنولوجيا المعلومات، بما يثري الأدبيات العلمية في هذا المجال.

المراجع :

1. أميرهم، جيهان عادل. (2022). أثر جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني. مجلة البحوث المالية والتجارية، جامعة بورسعيد.
2. موسى، عبد المجيد محمد. (2024). دور الأنشطة الحديثة للمراجعة الداخلية في الحد من مخاطر الخدمات الإلكترونية. وقائع مؤتمرات جامعة سبها.
3. عمر، حنان، ورزق الله، رزق الله. (2025). دور آليات التحول الرقمي في تحسين جودة المراجعة الداخلية بالمصارف التجارية الليبية. مجلة جامعة فزان العلمية.
4. أبوزيد وأبورقية، خالد، عبد الناصر. (2024). دور المراجعة الداخلية في إدارة المخاطر بالمصارف التجارية العاملة في ليبيا. مجلة دراسات الاقتصاد والأعمال.
5. جديع ومحمد، إكرام، خالد. (2025). المراجعة الداخلية ودورها في إدارة المخاطر السيبرانية. مجلة دراسات الإنسان والمجتمع.
6. سحيم، مريم مصباح. (2026). دور حوكمة الأمن السيبراني في تعزيز دقة التقارير المالية بالمصارف التجارية الليبية. مجلة الدراسات الاقتصادية.
7. إبراهيم، الهادي آدم محمد. (2024). «الأنشطة الحديثة للمراجعة الداخلية ودورها في تفعيل الحوكمة المصرفية». المجلة العربية للعلوم الإنسانية والاجتماعية.
8. معهد المراجعين الداخليين (IIA). (2024). المعايير العالمية للمراجعة الداخلية. فلوريدا، الولايات المتحدة الأمريكية: معهد المراجعين الداخليين. صدرت في 9 يناير 2024، وأصبحت نافذة للتطبيق في 9 يناير 2025.
9. المعهد الوطني الأمريكي للمعايير والتكنولوجيا (NIST). (2024). إطار الأمن السيبراني، الإصدار 2.0. وزارة التجارة الأمريكية.
10. المعهد الوطني الأمريكي للمعايير والتكنولوجيا (NIST). (2025). توصيات الاستجابة للحوادث واعتبارات إدارة المخاطر السيبرانية، الإصدار الثالث SP 800-61.
11. لجنة بازل للرقابة المصرفية. (2024). رقمنة التمويل: الآثار المترتبة على المصارف والرقابة المصرفية. بنك التسويات الدولية.
12. بنك التسويات الدولية. (2024). مشروع رافن: استخدام الذكاء الاصطناعي لتقييم الأمن السيبراني ومرونة النظام المالي.
13. بنك التسويات الدولية. (2026). اختبارات تحمل المخاطر السيبرانية في المصارف.
14. المعهد الوطني الأمريكي للمعايير والتكنولوجيا (NIST). (2024). إطار الأمن السيبراني، الإصدار 2.0. المنظمة الدولية للتقييس ISO/IEC 27001:2022. (2022). (ISO). نظم إدارة أمن المعلومات – المتطلبات.
15. 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 مسلاتة. مجلة العلوم الإنسانية والطبيعية، 6(7)، 583-554.
15. Sulayman Mohammed Ali Hasan, Rehab Mansor Alshatshati, & Azeezah Abdullah Alastay. (2026). Digital transformation and its role in bureaucratic leadership style: A field study within Al-Yaqeen Bank, Zliten branch and agency. *Sada Al-Jamia Journal for Financial and Administrative Sciences (SAJFAS)*, 2(2), 186-199. <https://doi.org/10.65422/sajfas.v2i2.453>
16. Ahmed Alsanosey Ahmed, & Nasser Ramadan Masoud Ashneen. (2026). The Role of Credit Quality Management in Reducing Credit Risk and Supporting Economic Stability in Islamic Banks, A Descriptive Applied Study on the Libyan Islamic Bank – Tripoli. *Sada Al-Jamia Journal for Financial and Administrative Sciences (SAJFAS)*, 2(2), 176-185. <https://doi.org/10.65422/sajfas.v2i2.450>
17. Sana Almahdi Khalifa Abokraa, & Sideenah allafi abdullah. (2026). Public Finance and the Challenges of Continuing to Finance the Fuel Subsidy Program. *Sada Al-Jamia Journal for Financial and Administrative Sciences (SAJFAS)*, 2(1), 326-337. <https://doi.org/10.65422/sajfas.v2i1.242>

18. Dileab, A. K. (2026). Artificial Intelligence and Economic Growth in Malaysia: A Composite Index Approach Using PCA. *Sada Al-Jamia Journal for Financial and Administrative Sciences (SAJFAS)*, 2(1), 288-278 .
19. Mohamed S Altraiki, & Fathi Mohammed Abu Ghalya. (2026). Evaluating the Role of Artificial Intelligence Technologies in Achieving a Balance between Economic Growth and Environmental Preservation in Libya: An Analytical Theoretical Study. *Sada Al-Jamia Journal for Financial and Administrative Sciences (SAJFAS)*, 2(1), 253-263. <https://doi.org/10.65422/sajfas.v2i1.219>
20. Arafat Mohammed Al-Basheer Al-Jaghalli. (2025). The Importance of the Beneish Model in Detecting Creative Accounting Practices in Banks. *Sada Al-Jamia Journal for Financial and Administrative Sciences (SAJFAS)*, 1(2), 200-213. <https://doi.org/10.65422/sajfas.v1i2.106>
21. Asmaa Kamal Youssef, & Al-Jaili Mohammad Al- Hassan Babeker. (2025). The role of operational and investment activities in the cash flow statement in the effectiveness of working capital efficiency in Sudanese banks: A case study on banks operating in the Nile River State. *Sada Al-Jamia Journal for Financial and Administrative Sciences (SAJFAS)*, 1(2), 214-225. <https://doi.org/10.65422/sajfas.v1i2.107>
22. Dr. Saleh Ali AlWasai, & Dr. Omar Faraj Mutiq. (2025). The role of Islamic banking windows in improving financial performance and creating a competitive advantage for commercial banks in Sirte: A field study from the employees' perspective. *Sada Al-Jamia Journal for Financial and Administrative Sciences (SAJFAS)*, 1(2), 145-157. <https://doi.org/10.65422/sajfas.v1i2.103>
23. Mohamed Omar Al-Sharif, & Omran Attia Albkori. (2025). The impact of funding sources on bank profitability and the role of risk as an intermediary in the relationship: A critical study of commercial banks. *Sada Al-Jamia Journal for Financial and Administrative Sciences (SAJFAS)*, 1(2), 118-130. <https://doi.org/10.65422/sajfas.v1i2.81>
24. Khaled Al-Bashir Mohammed Ahmed, & Abdulrahim Mohammed Ramadan Misbah. (2026). The Contribution of Infrastructure and Investment to Supporting the Adoption of Modern Accounting Systems in Libyan Companies: An Exploratory Study from the Perspective of Accounting Faculty Members at Libyan Universities. *Sada Al-Jamia Journal for Financial and Administrative Sciences (SAJFAS)*, 2(2), 47-66. <https://doi.org/10.65422/sajfas.v2i2.400>
25. Khaled Al-Bashir Mohammed Ahmed, & Abdulrahim Mohammed Ramadan Misbah. (2026). The Contribution of Infrastructure and Investment to Supporting the Adoption of Modern Accounting Systems in Libyan Companies: An Exploratory Study from the Perspective of Accounting Faculty Members at Libyan Universities. *Sada Al-Jamia Journal for Financial and Administrative Sciences (SAJFAS)*, 2(2), 47-66. <https://doi.org/10.65422/sajfas.v2i2.400>
26. Khaled Al-Bashir Mohammed Ahmed, & Ahmed Saad Idrees. (2026). High Performance Work Systems and Innovation Performance Through Knowledge Sharing and Organizational Learning Culture. *Sada Al-Jamia Journal for Financial and Administrative Sciences (SAJFAS)*, 2(2), 1-26. <https://doi.org/10.65422/sajfas.v2i2.355>
27. Khadeejah Ali Abraheem Abdulsamad. (2026). The impact of digital transformation on improving the quality of institutional performance: An applied study on service institutions in Libya. *Sada Al-Jamia Journal for Financial and Administrative Sciences (SAJFAS)*, 2(1), 316-325. <https://doi.org/10.65422/sajfas.v2i1.241>
28. Abdullah Maetouq Ahmed Almarash. (2026). Analysis of the dual exchange rate reality and its implications for monetary stability (The parallel market for the Libyan dinar as a case study). *Sada Al-Jamia Journal for Financial and Administrative Sciences (SAJFAS)*, 2(1), 264-277. <https://doi.org/10.65422/sajfas.v2i1.220>
29. Naser Muftah Alferjani. (2026). The Importance of Risk Management in Improving the Performance of Engineering Projects: A Comparative Analytical Study and Simulation

Algorithm. Sada Al-Jamia Journal for Financial and Administrative Sciences (SAJFAS), 2(1), 306-315. <https://doi.org/10.65422/sajfas.v2i1.240>

30. Huda A. A. Megeirhi. (2026). Artificial Intelligence, Economic Inequality, and Labour Market Polarization: A Theoretical Perspective on the Future of Work. *Sada Al-Jamia Journal for Humanities*, 4(2), 167-180. <https://doi.org/10.65422/sajh.v4i2.273>

31. Fatimah Faraj Mohammed Ghameedh, & Fouzeyaa Almutah Abdulhamd. (2026). Digital transformation as an approach to reforming public finances and achieving economic sustainability in Libya. *Sada Al-Jamia Journal for Humanities*, 4(2), 32-49. <https://doi.org/10.65422/sajh.v4i2.217>

32. Yones Ali Mohamed Alazoozey, & Najma Massoud Shebli. (2026). Digital Human Resource Practices and Employee Performance in Libyan Financial Companies: The Role of Digital HR Practitioners. *Sada Al-Jamia Journal for Humanities*, 4(4), 16-29. <https://doi.org/10.65422/sajh.v4i4.470>

33. Mohhsen Ali Albasher Alhbasihi. (2026). The Role of the Administrative Organizational Structure in Supporting the Efficiency of Strategic Planning Implementation: A Field Study on the Oil and Gas Sector in Libya. *Sada Al-Jamia Journal for Humanities*, 4(4), 42-56. <https://doi.org/10.65422/sajh.v4i4.473>

Disclaimer/Publisher's Note: The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of **SAJFAS** and/or the editor(s). **SAJFAS** and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.