٥

أثر أنشطة المراجعة الداخلية على مخاطر الأمن السيبراني في البنوك اليمنية (دراسة ميدانية)

١.د. غزي علي محمد الغزي استاذ المحاسبة والمراجعة المساعد – جامعة عمران
٢. د. منير محمد سرحان المخلافي استاذ المحاسبة والمراجعة المساعد – جـــامعة سبأ
٣.د. صبحي سعيد القباطي استاذ المحاسبة والمراجعة المساعد جامعة الحديدة

ملخص البحث

تهدف هذه الدراسة إلى تحليل أثر أنشطة المراجعة الداخلية على مخاطر الأمن السيبراني في البنوك اليمنية. تنطلق الدراسة من واقع التحول الرقمي المتسارع وما يصاحبه من تفاقم في المخاطر السيبرانية، خاصةً في قطاع حيوي كالبنوك. وقد تم استخدام المنهج الوصفي التحليلي في هذه الدراسة، وكانت أداة جمع البيانات هي الاستبانة وزعت على مجتمع وعينة الدراسة والبالغ عددها (١٩) بنكاً تجارياً وإسلامياً حيث تم استهداف المراجعين الداخليين العاملين في تلك البنوك. وقد استخدمت الدراسة طريقة المسح الشامل نظراً لصغر حجم الفئة المستهدفة من مجتمع وعينة الدراسة، حيث وزعت (١٠٠) استبانة وتم استرداد (٨٢) استبانة صالحة للتحليل. وتؤكد نتائج الدراسة أن المراجعة الداخلية في البنوك اليمنية تمارس أنشطة تقييم وتخطيط فعالة لمخاطر الأمن السيبراني، لكنها تحتاج إلى تطوير دورها الاستراتيجي وفحصها لأدوات الهندسة الاجتماعية. الأهم من ذلك، أثبتت الدراسة وجود أثر سلبي ذي دلالة إحصائية لأنشطة المراجعة الداخلية في خفض مخاطر الأمن السيبراني. تسلط هذه النتائج الضوء على الدور المحوري للمراجعة الداخلية في حماية القطاع المصرفي من التهديدات المتزايدة. وأخيراً توصي الدراسة بتعزيز الدور الاستراتيجي للمراجعة الداخلية، وتوفير التدريب المتخصص لمراجعي الأمن السيبراني، وتشجيع البنوك على تبني الأطر الأمنية العالمية.

الكلمات المفتاحية: المراجعة الداخلية، الأمن السيبراني، المخاطر السيبرانية، البنوك

The Impact of Internal Audit Activities on Cybersecurity Risks in Yemeni Banks: A Field Study

Abstract:

This study aimed to analyse the impact of internal audit activities on cybersecurity risks within Yemeni banks, proceeding from the reality of accelerating digital transformation and the attendant escalation of cyber threats — particularly in a sector as critical as banking. A descriptive-analytical methodology was employed, with a questionnaire used as the data collection instrument. The questionnaire was distributed to the study population and sample, comprising 19 commercial and Islamic banks, with internal auditors working within those institutions serving as the target group. Given the relatively small size of this group, a comprehensive survey approach was adopted: 100 questionnaires were distributed and 82 valid responses were retrieved for analysis. The findings confirm that internal audit functions in Yemeni banks carry out effective risk assessment and planning activities with respect to cybersecurity risks; however, they need to further develop their strategic role, particularly in scrutinising social engineering threats. Crucially, the study established a statistically significant negative relationship between internal audit activities and cybersecurity risk levels — indicating that such activities effectively contribute to risk reduction. These findings highlight the pivotal role of internal auditing in safeguarding the banking sector against growing threats. The study concluded by recommending the reinforcement of the strategic role of internal auditing, the provision of specialised training for cybersecurity auditors, and the encouragement of banks to adopt internationally recognised security frameworks.

Keywords: Internal Audit, Cybersecurity, Cyber Risks, Banks

مقدمة:

يشهد العصر الرقمي المتسارع تزايداً غير مسبوق في اعتماد المؤسسات على تكنولوجيا المعلومات، وشبكات الإنترنت، والحوسبة السحابية. حيث أن هذا التحول، وإن كان يعزز الكفاءة والابتكار، إلا أنه أدى إلى تفاقم مخاطر الأمن السيبراني (Cyber security Risks). ويُعرف الأمن السيبراني بأنه: عبارة عن مجموعة من التقنيات والعمليات المصممة لحماية الشبكات، الأجهزة، البرامج، وقواعد البيانات من الهجمات أو الأضرار أو الوصول غير المصرح به (Tosun, 2020: p.3). وقد أصبحت هذه المخاطر مصدر قلق بالغ للمؤسسات على مستوى العالم، وتحديداً للمؤسسات المالية التي تحتفظ بكميات هائلة من بيانات العملاء الحساسة، مما يجعلها أهدافاً رئيسية لمجرمي الإنترنت. (Masuch, Greve, M., Trang, S., & Kolbe, 2022)

تُلحق حوادث الأمن السيبراني أضراراً بالغة بالمنشآت، تتجاوز الخسائر المادية المباشرة لتشمل تعطيل العمليات، سرقة الأسرار والمعلومات، تدهور السمعة، فقدان ثقة أصحاب المصلحة، انخفاض أسعار الأسهم والقيمة السوقية، وتكاليف التقاضي والغرامات (Tosun, 2020: p.3).

في ظل هذه البيئة المليئة بالتهديدات، تبرز الحاجة الملحة لوظيفة المراجعة الداخلية (Internal Audit Function - IAF) كعنصر استراتيجي لمواكبة التغيرات والمخاطر المتسارعة (PWC, 2018, p.4). وتقوم المراجعة الداخلية بدورها الاستشاري بتقديم النصح والتوجيه لتحسين جودة ومحتوى المعلومات المتاحة لمتخذي القرار ومجالس الإدارة، خاصة في مجالات الرقابة، إدارة المخاطر، وحوكمة أنشطة المنشأة وعملياتها (شحاته، ٢٠٢١، ص ٢٩).

تُظهر التقارير والدراسات الحديثة التزايد المطرد في إدراك خطورة الأمن السيبراني. فقد أشار مسح معهد المراجعين الداخليين في أمريكا الشمالية لعام ٢٠٢٣ إلى أن ٧٨٪ من المشاركين يعتبرون الأمن السيبراني خطراً كبيراً/عالياً جداً على مؤسساتهم، متصدراً بذلك المخاطر التكنولوجية الأخرى (Institute of Internal Auditors IIA,2023). كما أظهر استطلاع لمعهد المراجعين الداخليين بالاتحاد

الأوروبي (European Confederation of Institute of Internal Auditors, ECIIA,2023) أن كبار المسؤولين التنفيذيين للمراجعة الداخلية في (١٥) دولة أوروبية صنفوا الأمن السيبراني وأمن البيانات ضمن أكبر عشرة مخاطر أعمال.

تُصنف مخاطر الأمن السيبراني ضمن المخاطر التشغيلية، وتُعرف بأنها مخاطر الخسارة الناتجة عن الحوادث الرقمية الناجمة عن حوادث داخلية أو خارجية أو أطراف ثالثة، بما في ذلك سرقة المعلومات، المساس بالنزاهة، تلف الأصول التكنولوجية، الاحتيال الداخلي والخارجي، وتعطيل الأعمال (رشوان وقاسم، ٢٠٢٢، ص٩٠).

من هنا، يمكن لوظيفة المراجعة الداخلية، من خلال دورها الاستشاري والرقابي، أن تساهم بفاعلية في مساعدة المؤسسات على التطور لمواجهة هذه التحديات وضمان الامتثال وفعالية الرقابة على الأنشطة. يتطلب هذا الدور من المراجعة الداخلية تبني نهج مرن وقادر على التعامل مع التكنولوجيا القائمة على المخاطر. بناءً على هذه الأهمية المتزايدة، تأتي هذه الدراسة لاستكشاف فعالية أنشطة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني.

مشكلة الدراسة:

لقد أحدث التحول الرقمي في القطاع المصرفي ثورة في الخدمات المالية، حيث عزز رضا العملاء وكفاءة المعاملات، ومع ذلك، فقد نتج عن هذا التحول ظهور عدد لا يحصى من مخاطر الأمن السيبراني التي تُهدد سلامة وسرية وتوافر الأنظمة المصرفية وبيانات العملاء (Oyewole, Okoye, Ofodile, & Ugochukwu,2024,627). تُشير التقارير الدولية إلى تصاعد هذه التهديدات، حيث واجهت المؤسسات المالية في عام ٢٠١٧ ما متوسطه ٨٥ هجوماً إلكترونياً سنوياً، كان ثلثها ناجحاً (Accenture Security,2017). كما ركزت الهجمات السيبرانية عالمياً على قطاع الخدمات المالية، حيث شهد عام ٢٠١٦ هجمات فاقت القطاعات الأخرى بنسبة ٦٥٪ (World Bank,2018). إقليمياً، شهدت دول ومنشآت أعمال في المنطقة تزايداً في أنشطة الجرائم السيبرانية، مع خسائر مالية كبيرة تكبدتها البنوك (Kshetri,2014,12). ففي عام ٢٠٢١، ضرب خرق

أمني سيبراني كبير إحدى أكبر شركات الخدمات المالية في الإمارات العربية المتحدة، مما أدى إلى كشف بيانات مالية حساسة وشل العمليات العادية. كان ذلك دليلاً على الضعف المتزايد لأنظمة المحاسبة على المنصات الرقمية حيث تخضع المنطقة تدريجيًا لتحول رقمي متسارع (Morshed, &Khrais,2025). تُعاني اليمن، على وجه الخصوص، من مستويات مرتفعة من الهجمات السيبرانية، حيث احتلت المرتبة الثانية عالمياً في نسبة المستخدمين الذين هاجمتهم البرامج الضارة للأجهزة المحمولة وبرامج الفدية، والمرتبة الخامسة في معدل التعرض لهجمات البرمجيات المالية الخبيثة، وذلك وفقاً لتقرير كاسبر سكاي للربع الثالث من عام ٢٠٢٢ (منظمة سام، ٢٠٢٣). وفي ظل توجه بعض البنوك اليمنية نحو الخدمات المصرفية الإلكترونية (Al-Fahim,2016)، فإن القطاع المصرفي اليمني ليس بمعزل عن هذه التهديدات المتزايدة. تُثير هذه التهديدات تساؤلاً حول مدى جاهزية أنظمة إدارة أمن المعلومات في البنوك اليمنية ومدى التزامها بضوابط الأمن للتخفيف من المخاطر (Al-Khulaidi, Al-Ashwal, Nasser, & Al-Anesi,2023.227) وقد أكدت دراسات سابقة وجود نقاط ضعف ملحوظة في ممارسات أمن المعلومات داخل البنوك اليمنية:

- أشارت دراسة (Nasser, Al Ansi, & Al Sharabi, 2020: p17) إلى ضعف في تقييم نقاط الضعف في أنظمة المعلومات، وتحديات في تنفيذ اختبارات الاختراق، وعدم كفاية مراجعة الالتزام وتحديث صلاحيات المستخدمين.
- كشفت دراسة (Al-Khulaidi, Nasser, Alanesi, Hazaa, & Aljober,2022: p145) عن نقاط ضعف في أنظمة إدارة أمن المعلومات، تشمل عدم وجود وحدة مستقلة لأمن المعلومات، والفشل في إجراء الاختبارات الأمنية للمؤهلين لشغل المناصب الرئيسية، ومحدودية وعي الإدارات بمتطلبات أمن المعلومات، وغياب التنسيق الأمني الأمثل، ونقص برامج التدريب والتوعية، والتصنيف غير المناسب للمعلومات.

كما تُشير تقارير دولية، مثل تقرير لجنة بازل للإشراف على البنوك (Basel Committee on Banking، ٢٠١٨) إلى أن التحديات العالمية في مجال المرونة السيبرانية

تشمل الجمود في الاستراتيجيات، والخلط في الأدوار والمسؤوليات، ونقص العمال المهرة، وضعف الاستجابة للحوادث، مما "يعوق فعالية" نموذج "خطوط الدفاع الثلاثة" (خط الدفاع الأول: العمليات التشغيلية، خط الدفاع الثاني: إدارة المخاطر والامتثال، خط الدفاع الثالث: المراجعة الداخلية).

في ظل هذا المشهد المعقد، حيث تتصاعد مخاطر الأمن السيبراني وتظهر نقاط ضعف في ممارسات الأمن السيبراني بالبنوك اليمنية، يبرز التساؤل حول مدى فعالية انشطة المراجعة الداخلية في الحد من هذه المخاطر. وبناءً على ما سبق، تتحدد مشكلة الدراسة في التساؤل الرئيسي التالي:

ما أثر أنشطة المراجعة الداخلية المرتبطة بالأمن السيبراني (أنشطة تقييم المخاطر، أنشطة تخطيط المخاطر، أنشطة فحص الأدوات الرقابية) على مخاطر الأمن السيبراني في البنوك اليمنية؟

ويتفرع عن هذا السؤال التساؤلات البحثية الآتية:

١. ما أثر أنشطة تقييم المخاطر على مخاطر الأمن السيبراني في البنوك اليمنية؟
٢. ما أثر أنشطة تخطيط المخاطر على مخاطر الأمن السيبراني في البنوك اليمينة؟
٣. ما أثر أنشطة فحص الأدوات الرقابية على مخاطر الأمن السيبراني في البنوك اليمينة؟

أهداف الدراسة:

هدفت الدراسة بشكل رئيسي الى تحليل ودراسة أثر أنشطة المراجعة الداخلية المرتبطة بالأمن السيبراني (أنشطة تقييم المخاطر، أنشطة تخطيط المخاطر، أنشطة فحص الأدوات الرقابية) على مخاطر الأمن السيبراني في البنوك اليمنية. ويمكن تقسيم هذا الهدف الى الأهداف الفرعية الآتية:

١. التعرف على أثر أنشطة تقييم المخاطر على مخاطر الأمن السيبراني في البنوك اليمنية.

٢. التعرف على أثر أنشطة تخطيط المخاطر على مخاطر الأمن السيبراني في البنوك اليمينة.

٣. التعرف على أثر أنشطة فحص الأدوات الرقابية على مخاطر الأمن السيبراني في البنوك اليمينة.

أهمية الدراسة:

تنبع أهمية هذه الدراسة من التحديات المتزايدة التي يفرضها مشهد الأمن السيبراني العالمي على المؤسسات، لا سيما القطاع المصرفي. مع تزايد وتيرة الهجمات السيبرانية وما تُسببه من خسائر مادية ومعنوية وتأثير على الأداء والسمعة، يُصبح البحث في آليات تعزيز الحصانة السيبرانية أمراً بالغ الأهمية. تكتسب هذه الدراسة أهميتها من بعدين رئيسيين:

الأهمية العلمية:

تُسهم هذه الدراسة في تعميق الأدبيات الأكاديمية في الجوانب الآتية:

- تُعالج الدراسة موضوعاً حيوياً ونقاشي يتمثل في دور المراجعة الداخلية في الحد من مخاطر الأمن السيبراني. هذا يُمثل إضافة علمية خاصة في سياق القطاع المصرفي اليمني الذي يفتقر إلى دراسات مماثلة.
- تُقدم الدراسة أدلة كمية ومحددة حول أدوار ومسؤوليات المراجعة الداخلية في الحد من مخاطر الأمن السيبراني، مما يُعزز الفهم النظري والتطبيقي للعلاقة بين الأمن السيبراني، إدارة مخاطره، وإدارة المخاطر المؤسسية، وفوائد الدمج بين هذه الجوانب.
- تُساهم الدراسة في إثراء البحث في المجال المحاسبي من خلال تحليل انعكاسات أدوار ومسؤوليات المراجعة الداخلية في الحد من مخاطر الأمن السيبراني، مما قد يُمهد لتطوير مؤشرات أو أطر لقياس مدى فعالية انشطة المراجعة الداخلية للأمن السيبراني مستقبلاً.

الأهمية العملية

تسعى الدراسة إلى تقديم قيمة عملية ملموسة للجهات المعنية متمثلة في الآتي:

- تُقدم الدراسة إطاراً عملياً يوضح متطلبات كفاءة وفاعلية المراجعين الداخليين لتعزيز انشطتهم في الحد من مخاطر الأمن السيبراني في البنوك اليمنية. هذا الإطار يمكن أن يُسهم في تحسين ممارسات المراجعين الداخليين الذين قد يواجهون صعوبة في فهم طبيعة ومدى فعالية دورهم في مراجعة مخاطر الأمن السيبراني.
- تُوفر النتائج التي سيتم التوصل إليها أدلة موثوقة لأهمية انشطة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني. يمكن لهذه الأدلة أن تُستخدم من قبل إدارات البنوك ومجالس الإدارة والجهات الرقابية (مثل البنك المركزي اليمني) لتوجيه الاستثمارات في تعزيز قدرات المراجعة الداخلية، وتطوير السياسات والإجراءات الرقابية، بما يُساهم في حماية الأصول المالية وبيانات العملاء.
- تُسلط الدراسة الضوء على نقاط القوة والضعف في الممارسات الحالية للمراجعة الداخلية المتعلقة بالأمن السيبراني في البنوك اليمنية، مما يمكن أن يُساعد المؤسسات على تحديد أولويات برامج التدريب والتطوير اللازمة للمراجعين، وتحسين آليات التقييم والتخطيط والتدقيق.

فرضيات الدراسة:

بناء على مشكلة واهداف الدراسة يمكن صياغة الفرضية الرئيسة للدراسة كما يلي:

لا يوجد أثر ذو دلالة احصائية عند مستوى معنوية ($\alpha \leq$ ٠.٠٥) لأنشطة المراجعة الداخلية المرتبطة بالأمن السيبراني (أنشطة تقييم المخاطر، أنشطة تخطيط المخاطر، أنشطة فحص الادوات الرقابية) على مخاطر الأمن السيبراني في البنوك اليمنية.

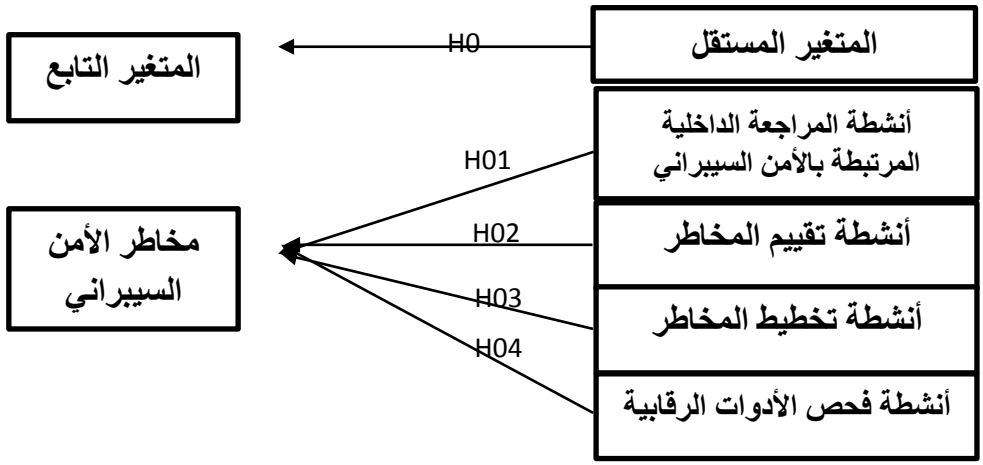
وينبثق عن هذه الفرضية الفرضيات الفرعية الآتية:

١. لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq$ ٠.٠٥) لأنشطة تقييم المخاطر على مخاطر الأمن السيبراني في البنوك اليمنية.

٢. لا يوجد أثر ذو دلالة احصائية عند مستوى معنوية ($\alpha \leq$ ٠.٠٥) لأنشطة تخطيط المخاطر على مخاطر الأمن السيبراني في البنوك اليمنية.

٣. لا يوجد أثر ذو دلالة احصائية عند مستوى معنوية ($\alpha \leq$ ٠.٠٥) لأنشطة فحص الادوات الرقابية على مخاطر الأمن السيبراني في البنوك اليمنية .

النموذج المعرفي للدراسة



النموذج المعرفي من إعداد الباحثين وفقاً للدراسات السابقة

مجتمع الدراسة:

يتمثل مجتمع الدراسة في البنوك اليمنية البالغ عددها (١٩) بنكا تجاريا واسلاميا، وتحديدا يتكون مجتمع الدراسة من المراجعين الداخليين العاملين في تلك البنوك.

حدود الدراسة:

الحدود الموضوعية: ستعتمد الدراسة الحالية على انشطة المراجعة الداخلية المرتبطة بالأمن السيبراني (تقييم المخاطر، تخطيط المخاطر وفحص الادوات الرقابية) كمقياس للمتغير المستقل ومخاطر الأمن السيبراني كمتغير تابع.

الحدود المكانية: البنوك اليمنية (المركز الرئيس وفروعه بأمانة العاصمة)

الحدود الزمانية: فترة إجراء الدراسة ٢٠٢٤- ٢٠٢٥.

الدراسات السابقة

تناولت عدد من الدراسات دور المراجعة الداخلية في سياق الأمن السيبراني، مُقدمةً رؤى حول جوانب مختلفة من هذا الموضوع. يتناول هذا القسم أبرز هذه الدراسات، مع التركيز على تحديد أوجه التشابه والاختلاف، لإبراز الفجوة البحثية التي تسعى الدراسة الحالية لسدها.

تناولت بعض الدراسات العوامل المؤثرة في مدى مراجعة الأمن السيبراني، حيث استكشفت دراسة (Islam, Farah, & Stafford,٢٠١٨) العلاقة بين خصائص المراجعة الداخلية ودعم مجلس الإدارة، وخلصت إلى وجود تأثير واضح لقدرات كفاءة المراجعة الداخلية على دورها في مراجعة الأمن السيبراني. وفي ذات السياق، ركزت دراسة Tušek, Sačer, & Halar (٢٠١٨) على الأدوار الجديدة للمراجعة الداخلية كأداة لتعزيز نجاح الأعمال في البيئة الرقمية، مؤكدة على طبيعتها الاستشارية والخبرة في تقييم المخاطر السيبرانية.

كما بحثت دراسات أخرى في العلاقة بين جودة المراجعة وحوادث الأمن السيبراني وتأثير العوامل التنظيمية. فقد وجدت دراسة Rosati. Gogolin, & Lyn (٢٠٢٠) أن المراجعين في الشركات الأمريكية يزيدون من جهود المراجعة والاختبارات الجوهرية بعد وقوع الاختراقات لتعويض المخاطر المتزايدة. ومن ماليزيا، استكشفت دراسة Shamsuddin, Adam, Adnan, & Yasin (٢٠٢٠) فعالية المراجعة الداخلية في إدارة الأمن السيبراني بالقطاع المصرفي، مؤكدة أن وعي المراجعين، السياسة التنظيمية، وإدارة المخاطر التنظيمية تعد عوامل محورية في هذه الفعالية.

هدفت دراسة الزيود (٢٠٢١) في البنوك التجارية الأردنية إلى تحديد أثر كفاءة، حيادية، ومركز وتخطيط المراجعة الداخلية في الحد من المخاطر السيبرانية، وخلصت إلى وجود أثر للكفاءة، المركز التنظيمي، والتخطيط. وفي سياق مختلف، كشفت دراسة Simić (٢٠٢٢)، باستخدام نهج نوعي في السويد، عن ممارسات المراجعين الداخليين في الأمن السيبراني، مشددة على أهمية وعي العاملين كعامل مؤثر.

من جانبها، ركزت بعض الدراسات على جوانب محددة من فعالية المراجعة الداخلية ومؤشراتها. فقد حللت دراسة Darmawati (٢٠٢٢) تأثير شهادة المراجع الداخلي، تقييم المخاطر، دور الإدارة العليا، والاستراتيجيات والإجراءات الفنية على فعالية الأمن السيبراني، لتجد أن لهذه العوامل تأثيراً إيجابياً. أما دراسة Slapničar, Vuko, Čular, & Drašček (٢٠٢٢) فقد سعت إلى تطوير مؤشر قياس لفعالية المراجعة الداخلية في ضمان الأمن السيبراني من خلال أبعاد (التخطيط، الأداء، وإعداد التقارير)، وأشارت نتائجها إلى أن هذه الفعالية كانت متوسطة.

أخيراً، تناولت دراسات أخرى أثر المراجعة الداخلية على قرارات المستثمرين وإطار تعزيز دور المراجعة. ففي شركات الاتصالات المصرية، بحثت دراسة أميرهم (٢٠٢٢) في أثر جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني وانعكاساتها على قرارات المستثمرين، مؤكدة وجود علاقة بين جودة المراجعة الداخلية ومخاطر الأمن السيبراني. وفي محاولة لتعزيز الدور، هدفت دراسة Usman, Che-Ahmad, & Abdulmalik (٢٠٢٣) إلى تقديم إطار لتعزيز دور المراجعة الداخلية في تقييم مخاطر الأمن السيبراني بالقطاع المالي، من خلال مراجعة الأدبيات وتسليط الضوء على خصائص المراجع الداخلي.

توضح هذه الدراسات الأهمية المتزايدة لدور المراجعة الداخلية في بيئة المخاطر السيبرانية المتنامية، وتبرز الحاجة المستمرة لفهم العوامل التي تعزز فعاليتها في هذا المجال.

الفجوة البحثية

على الرغم من الثراء المعرفي الذي توفره الدراسات السابقة حول دور انشطة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني، يمكن تحديد الفجوة البحثية الآتية التي تسعى هذه الدراسة لسدها:

١. غالبية الدراسات السابقة إما أنها دراسات مفاهيمية أو أجريت في سياقات جغرافية مختلفة (مثل ماليزيا، الأردن، السويد، الولايات المتحدة) وقطاعات متنوعة (شركات اتصالات، قطاعات عامة، شركات بشكل عام). تفتقر الأدبيات إلى دراسات تطبيقية كمية مُركزة على دور المراجعة الداخلية في الحد من مخاطر الأمن السيبراني في القطاع المصرفي تحديداً ضمن بيئة جيوسياسية واقتصادية فريدة ومليئة بالتحديات مثل الجمهورية اليمنية. هذه الفجوة تبرز الحاجة إلى فهم أعمق للواقع العملي في مثل هذه البيئات.

٢. على الرغم من أن بعض الدراسات أشارت إلى كفاءة المراجعة أو تخطيطها، إلا أن هناك مجالاً لتقديم تحليل أكثر تفصيلاً لآليات عمل المراجعة الداخلية وكيف تساهم انشطتها المتعلقة بتقييم المخاطر، والأنشطة التخطيطية، وتدقيق الأدوات الرقابية تحديداً في تقليل مخاطر الأمن السيبراني.

بناءً على هذه الفجوة، تسعى الدراسة الحالية لتقديم مساهمة أصيلة من خلال تطبيق منهج كمي في سياق البنوك اليمنية، لتقديم فهم شامل وموثوق لأثر أنشطة المراجعة الداخلية على مخاطر الأمن السيبراني في البنوك اليمنية.

الإطار النظري:

الأمن السيبراني (Cyber security)

يُمثل الأمن السيبراني مجالاً حيوياً في العصر الرقمي، ومع ذلك، لا يزال مفهومه يشهد تبايناً في التعريفات ضمن الأدبيات الأكاديمية والمهنية. يرى البعض أن الأمن السيبراني مفهوم شامل يتضمن أمن المعلومات وضمانها (Gyun & Vasarhelyi, 2017, p4)، بينما يُميزه البعض الآخر عن أمن المعلومات بالإشارة إلى أن

الأمن السيبراني يركز على المخاطر الناتجة عن الهجمات السيبرانية تحديداً (Li, H,2017).

ومن أبرز التعريفات للمنظمات المهتمة:

تعريف الاتحاد الدولي للاتصالات (TU, 2006) للأمن السيبراني بأنه "مجموعة من الأدوات والسياسات والمفاهيم الأمنية والضمانات الأمنية والمبادئ التوجيهية ونُهُج إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات وسبل الضمان والتكنولوجيات التي يمكن استخدامها في حماية البيئة السيبرانية والمنظمة وأصول المستخدمين".

اما المعهد الوطني للمعايير والتكنولوجيا (IST, 2013a) فيُعرفه كوسيلة لحماية المعلومات بمنع الهجمات واكتشافها والاستجابة لها. ويُعرفه المعهد الأمريكي للمحاسبين القانونيين المعتمدين (American Institute Certified Public Accountants AICPA, 2017b): بأنه "عملية تطبيق الإجراءات الأمنية لضمان سرية البيانات وتكاملها وتوافرها".

أكدت الدراسات العلمية بأن الأمن السيبراني يشتمل على التقنيات والعمليات والضوابط المصممة لحماية الأنظمة والشبكات والبيانات من الهجمات السيبرانية (Gyun and Vasarhelyi,2017,5)، ويهدف إلى منع الهجمات، الضرر، والوصول غير المصرح به (Perwej, Abbas, Dixit, Akhtar & Jaiswal, 2021: p 670؛ Möller & Haas, 2019: p 377). كما يشمل ممارسات حماية الأنظمة من الوصول غير المصرح به من الأطراف الداخلية والخارجية (Shamsuddin, et. al., 2020: p240).

بناءً على هذه التعريفات، يمكن القول إن الأمن السيبراني هو مجموعة متكاملة من الوسائل التقنية والإجراءات الإدارية الهادفة إلى حماية الأصول السيبرانية للمنشأة (كالشبكات، الأنظمة، البيانات) من الوصول غير المصرح به، سوء الاستغلال، والتخريب، مع ضمان استمرارية العمليات، سرية البيانات، وسلامتها وتوافرها للأطراف المصرح لها.

أهداف الأمن السيبراني:

تتركز أهداف الأمن السيبراني وفقا لـ Hoffmann, Napiórkowski, Protasowicki,& Stanik, 2020,p:657) حول مبادئ أساسية لضمان أمن المعلومات، وتتمثل في:

١. حماية سرية البيانات (Data Confidentiality): تهدف إلى منع الوصول غير المصرح به إلى المعلومات الحساسة، وضمان أن يقتصر الوصول على المستخدمين أو المجموعات المصرح لها فقط.
٢. الحفاظ على سلامة البيانات (Data Integrity): يعني الحفاظ على البيانات من التغيير أو التعديل غير المصرح به، ويشمل آليات لتقييد التغييرات واستعادة البيانات المخترقة (Hoffmann, et al., 2020: p ٦٥٧).
٣. تعزيز توافر البيانات (Data Availability): يُشير إلى ضمان توافر جميع أنظمة المعلومات (الأجهزة، الشبكات، البرامج، البيانات) للمستخدمين المصرح لهم في الأوقات اللازمة لأداء الأنشطة، مع ضمان الوصول الموثوق وفي الوقت المناسب.

الهدف العام للأمن السيبراني هو حماية أصول المنشآت لتمكينها من أداء أعمالها، وتقليل احتمالات وقوع المخاطر، والحد من الأضرار، وتأمين استعادة العمليات الطبيعية في فترة زمنية وتكلفة معقولة (Ursillo & Arnold ,2019)

وسائل الأمن السيبراني:

لتحقيق الأهداف المذكورة، يتطلب الأمن السيبراني نهجاً متعدد الطبقات يشمل الوقاية، الحماية، التخفيف، الاستجابة، والتعافي:

١. الوقاية (Prevention): تركز على الإجراءات التي تمنع أو توقف وقوع الحوادث السيبرانية التي تهدد سرية، سلامة، وتوافر البيانات (Gaidosch,2019,91 & Morozova Adelmann,).
٢. الحماية (Protecting): تتعلق باتخاذ تدابير لحماية وتأمين البيانات والمعلومات، مثل استخدام التشفير وتقنيات التحكم في الوصول (Perwej, et al., 2021: p684.)

٣. التخفيف (Mitigate): نظراً لاستحالة المنع التام، تركز تدابير التخفيف على الحد من تأثير وتقليل الضرر في حالة وقوع حادثة سيبرانية (Gaidosch, et al,2019,91).

٤. الاستجابة (Response): تتضمن وجود إجراءات لمعالجة تأثيرات حوادث الأمن السيبراني بعد وقوعها مباشرة، وتتطلب أحياناً تنسيقاً على المستويات الوطنية والدولية (Gaidosch, et al., 2019, p.92).

٥. التعافي (Recovery): تُعنى هذه العملية باستعادة العمليات والقدرات المتضررة بعد الحادث السيبراني، مع الإقرار بأنه قد لا يكون التعافي شاملاً في جميع الحالات (NIST,2018:9).

مخاطر الأمن السيبراني:

تُعد مخاطر الأمن السيبراني من أبرز وأخطر التحديات التي تواجه المجتمعات والمنظمات على مستوى العالم (World Economic Forum (WEF), 2020؛ Institute of Internal Auditors - IIA، ٢٠١٩)(يُعرف الخطر بشكل عام بأنه "الخطر الناتج عن الأحداث والظروف، والإجراءات التي يمكن أن تؤثر سلباً على قدرة المنشأة على تحقيق أهدافها وتنفيذ استراتيجياتها" (IFA. ISA، ٣١٥، ٢٠١٩). في السياق السيبراني، تُصبح الأنظمة والبنى التحتية المتصلة بالفضاء السيبراني عرضة لأنشطة إجرامية تُعطل خدماتها وتُدمر معلوماتها، مما يجعل الجريمة السيبرانية خطراً ملازماً للشركات (National Institute of Standards and Technology (NIST,2018) . يُعرف الهجوم السيبراني بأنه هجوم يُطلق من جهاز كمبيوتر ضد موقع ويب أو نظام كمبيوتر أو كمبيوتر فردي، ويُخل بسرية أو سلامة أو توافر النظام أو المعلومات (Perwej, et.al,٢٠٢١:٦٨٩ -٦٧٩). تُعرف مخاطر الأمن السيبراني بأنها المخاطر التي تمس عمليات أعمال المنظمة، بما في ذلك رؤيتها، سمعتها، أو أصولها، بسبب إمكانية الوصول غير المصرح به أو الاستخدام أو الإفصاح أو التعطيل أو التعديل أو تدمير المعلومات و/أو نظم المعلومات (الهيئة الوطنية للأمن السيبراني، ٢٠١٨). كما يُعرفها مجلس الاستقرار المالي (Financial Stability

Board FSB,2018) ولجنة بازل بأنها "مزيج من احتمالية وقوع الحوادث السيبرانية وتأثيرها" (Doerr,2022:6).

تُشير التقديرات إلى أن التكلفة العالمية للهجمات السيبرانية كانت ٨.٤ تريليون دولار في عام ٢٠٢٢، ومن المتوقع أن تتجاوز ١١ تريليون دولار في عام ٢٠٢٣. وقد سجل القطاع المالي ثاني أعلى متوسط تكلفة لخرق البيانات بعد الرعاية الصحية (IBM, (Statista ,(2022، ٢٠٢٣).

أنواع مخاطر الأمن السيبراني:

تُصنف التهديدات السيبرانية تقليدياً إلى ثلاث فئات بناءً على الطبيعة الفنية للتهديدات: (Hasanefendioglu,2019:48)

١. السرية (Confidentiality): اختراق سرية البيانات، يؤدي إلى تسريب معلومات حساسة ويُسبب خسائر مباشرة وتكاليف سمعة.
٢. التوافر (Availability): اختراق توافر البيانات أو الأنظمة، يؤدي إلى تعطيل العمليات وشل حركة رأس المال والسيولة، وقد يؤثر على قدرة البنك على أداء أنشطته الأساسية.
٣. النزاهة (Integrity): اختراق سلامة البيانات، يؤدي إلى تغيير أو تدمير البيانات، ويُسبب تكاليف مباشرة (للاستعادة) وتكاليف غير مباشرة (كضعف أداء البنك) (Eisenbach, Kovner&, Lee, 2022: 6-7).

أنواع الهجمات السيبرانية الشائعة:

من بين التهديدات السيبرانية البارزة التي تواجهها المؤسسات المالية بشكل متكرر:

١. هجمات البرامج الضارة (Malware Attacks): استخدام فيروسات، ديدان، وأحصنة طروادة لاختراق الأنظمة وسرقة المعلومات الهامة والحساسة (Hasanefendioglu,2019:47)
٢. التصيد الاحتيالي والهندسة الاجتماعية (Phishing and Social Engineering): خداع الأفراد للكشف عن معلومات حساسة أو الانخراط في

معاملات غير مصرح بها عبر رسائل احتيالية أو تلاعب نفسي (Efijemue, Obunadike, Taiwo, Kizor, Olisah, Odooh &, Ejimofor,2023).

٣. هجمات رفض الخدمة الموزعة (DDoS Attacks): إغراق الشبكات بحركة مرور هائلة لمنع العملاء من الوصول إلى الخدمات المالية، مما يعطل العمليات (Perwej, et al,2021:684).

٤. التهديدات الداخلية (Insider Threats): قيام موظفين أو متعاقدين لديهم وصول إلى بيانات حساسة بتعريض أمن المعلومات للخطر عن قصد أو غير قصد (Efijemue, et. Al,2023).

مخاطر الأمن السيبراني في القطاع المصرفي:

تُعتبر البنوك من أكثر القطاعات تعرضاً للمخاطر السيبرانية نظراً لاعتمادها الكبير على تكنولوجيا المعلومات والاتصالات في عملياتها وخدماتها (Crisanto, et. al,2024:3). هذه المخاطر تتجاوز المخاطر المصرفية التقليدية لتشمل المخاطر التشغيلية والاستراتيجية والقانونية ومخاطر السمعة الناتجة عن نقاط الضعف في الأنظمة الإلكترونية (السجيني وسمير، ٢٠٢٣، ص١١)

تساهم عدة عوامل في تفاقم المخاطر السيبرانية في المؤسسات المالية، منها: العولمة، الاعتماد المتزايد على التكنولوجيا المتطورة، الترابط الكبير داخل النظام المالي، والتطور المستمر لمجرمي الإنترنت (Crisanto, Ehrentraud, Fabian &, Monteil,2024:3)

نظراً للترابط والاعتماد المتبادل بين عناصر النظام المالي العالمي، يمكن لخرق واحد في شبكة مصرفية أن يُعطل النظام المالي بأكمله ويُحدث عواقب وخيمة (Shamsuddin et al., 2020: p240). تتخذ المخاطر السيبرانية في القطاع المالي أشكالاً متعددة، تتراوح بين اضطرابات وظائف الأعمال، وسرقة المعلومات الحساسة (سوقية أو شخصية)، وإلحاق الضرر بسلامة البيانات، أو الأنظمة (Peihani, 2022: p140). الهجمات السيبرانية الناجحة يمكن أن تُعرض المؤسسات المالية لمخاطر ثانوية كبرى تشمل الملاءة، السيولة، السوق، المخاطر التشغيلية، القانونية، والسمعة.

قنوات نقل المخاطر للأحداث السيبرانية:

تُؤثر انتهاكات الأمن السيبراني على القيمة السوقية للشركات وسمعتها وميزتها التنافسية ((Gavėnaitė-Sirvydienė,2024,42. يمكن لهذه الانتهاكات أن تنتشر عبر النظام المالي بأكمله وتُحدث مخاطر نظامية، تُهدد وظائف الأنظمة الحيوية. يُمكن للأحداث السيبرانية أن تنتقل عبر ثلاث قنوات (Goh, Kang, Koh, Lim, Sher &, Yao,2020,8):

تركز المخاطر: يحدث عندما تستهدف الهجمات السيبرانية بنى تحتية مالية رئيسية أو مزودي خدمات تابعين لجهات خارجية، مما يؤدي إلى فقدان خدمات لا يمكن استبدالها او استعادتها بسهولة (على سبيل المثال، أنظمة الدفع والتسوية).

مخاطر العدوى: يُمكن لهجوم سيبراني على مؤسسة مالية أن يؤدي إلى صعوبات تمتد إلى مؤسسات أخرى بسبب الطبيعة المترابطة للنظام المالي.

تآكل الثقة: قد يُسبب هجوم سيبراني في تآكل الثقة في العديد من المؤسسات المالية أو في النظام المالي ككل.

يُنظر إلى مخاطر الأمن السيبراني بشكل متزايد كأحد أهم التحديات التي تواجه الشركات (PwC,2018)، حيث يُمكن أن تُسفر الجرائم السيبرانية عن فقدان السمعة، والملكية الفكرية، وتوقف العمليات، وتحمل غرامات، وتعويضات، وتكاليف قضائية (AICPA, 2017; CAQ، ٢٠١٨).

المراجعة الداخلية

تطورت مهنة المراجعة الداخلية لتصبح نشاطاً مستقلاً وموضوعياً، يوفر تأكيداً واستشارات بهدف إضافة قيمة للمنشأة وتحسين عملياتها (Institute of Internal Auditors IIA,2017). لم يعد دور المراجع يقتصر على التقارير المالية فحسب، بل امتد ليشمل تقديم تأكيدات على العمليات التي تُنتج البيانات الكمية والنوعية، والسعي لتوفير ضمانات حول استمرارية وقدرة المنشأة على الاستجابة للمخاطر والفرص المختلفة .(Friedman, Akaaboune &, Margolis, 2013: p 27)

أصبحت وظيفة المراجعة الداخلية جزءاً مهماً من الهيكل التنظيمي للمنشآت وأداة هامة للإدارة العليا في تحقيق الرقابة الإدارية، لا سيما مع التركيز المتزايد على إدارة المخاطر (NDUKWE, 2016: p76). يؤكد التعريف الحديث للمراجعة الداخلية (IIA,2020) على دورها في تعزيز وحماية قيمة الشركة من خلال تقديم التوكيد والاستشارة والرؤية الموضوعية القائمة على المخاطر.

تُشير التوجهات الحديثة للمراجعة الداخلية إلى عدة تغييرات جوهرية أهمها: (النجار، ٢٠١٣، ٦٦)

١. يمكن الاستعانة بمصادر خارجية للقيام بأنشطة المراجعة الداخلية
٢. نطاق المراجعة الداخلية يشمل الأنشطة الاستشارية.
٣. تهدف المراجعة الداخلية إلى إضافة قيمة للمنشأة وتحسين عملياتها.
٤. المراجعة الداخلية تعمل على توسيع نطاق عملها ليشمل إدارة المخاطر والرقابة والحوكمة.

وقد اتسع مفهوم ونطاق وأهداف المهنة لتتضمن دوراً بنائياً استراتيجياً قائماً على تقييم مدى الالتزام بأطر الحوكمة وتقييم المخاطر وفعالية إدارتها (Nabulsi & Haidoura, 2018: p52). تُعزز المراجعة الداخلية من السمات الحديثة للمهنة ودورها الرئيسي في عمليات الحوكمة وإدارة المخاطر والرقابة (زيتون، ٢٠٢١: ص. ١٠).

على الرغم من وضوح تعريف المراجعة الداخلية، فإن إدراك الدور الفعلي الذي تلعبه هذه الوظيفة يُعد أمراً مهماً. تُحدد معايير المراجعة الداخلية مسؤولياتها الرئيسية في تقييم الحوكمة، وإدارة المخاطر، ومدى كفاية وفعالية الضوابط الرقابية في التعامل مع مخاطر المنشأة لتحقيق الأهداف الاستراتيجية، ومصداقية المعلومات، وكفاءة العمليات، وحماية الأصول، والامتثال للقوانين. ويُشدد البعض على أولوية الأدوار الاستشارية والتأكيدية للمراجعة الداخلية في مجال إدارة المخاطر (IIA,2018:48).

انشطة المراجعة الداخلية المرتبطة بمخاطر الأمن السيبراني:

الرقابة الداخلية للأمن السيبراني ضرورية لحماية بيانات الشركة وأنظمتها من التهديدات المتزايدة. تلعب المراجعة الداخلية دورًا حيويًا في تقييم فعالية هذه الضوابط.

١. تقييم المخاطر السيبرانية:

تُعد هذه المرحلة نقطة الانطلاق لأي عملية مراجعة داخلية (The Institute of Internal Auditor,IIA,2020). يهدف المراجع الداخلي إلى فهم وتحليل المخاطر التي تواجه المؤسسة في الفضاء السيبراني. وتتضمن المخاطر الأساسية ما يلي:

- **التهديدات الخارجية:** مثل هجمات البرامج الضارة (Malware)، وبرامج الفدية (Ransomware)، والتصيد الاحتيالي (Phishing).
- **التهديدات الداخلية:** قد تنجم عن أخطاء بشرية، أو سوء استخدام الصلاحيات، أو حتى نوايا خبيثة من قبل الموظفين.
- **نقاط الضعف الفنية:** تشمل الثغرات في الأنظمة، والتكوينات غير الصحيحة للشبكة، أو عدم تطبيق التحديثات الأمنية.

يُقيم المراجعون الداخليون هذه المخاطر بناءً على احتمالية حدوثها وتأثيرها المحتمل على الأصول الرقمية للمؤسسة. هذا التقييم يساعد في تحديد أولويات المراجعة وتوجيه الموارد نحو الأصول الأكثر أهمية وحساسية، لضمان عدم إضاعة الجهد والوقت في جوانب أقل أهمية.

٢. تخطيط المراجعة

بعد تحديد المخاطر، يضع المراجع الداخلي خطة مراجعة شاملة ومنهجية (IIA,2020). يضمن التخطيط الفعال أن تكون المراجعة منظمة وذات هدف واضح. تشمل هذه المرحلة الأنشطة الآتية:

- **تحديد النطاق** :(Scope Definition) يحدد المراجع الأنظمة والعمليات التي سيتم فحصها، مثل قواعد بيانات العملاء أو أنظمة الدفع الإلكتروني.

- **تخصيص الموارد** :(Resource Allocation) يتم تحديد الموارد البشرية والتقنية اللازمة لإجراء المراجعة، وقد يتطلب ذلك الاستعانة بخبراء خارجيين في الأمن السيبراني إذا لم تتوفر الخبرة الداخلية.
- **وضع الجدول الزمني** :(Scheduling) يتم تحديد المواعيد النهائية لكل مرحلة من مراحل المراجعة لضمان إنجازها في الوقت المناسب وتقديم تقرير مفصل للإدارة.

٣. مراجعة الضوابط الرقابية ووسائل الحماية

يجب على المراجع الداخلي التحقق من أن الإدارة تنفذ الضوابط اللازمة، وأنها تعمل بكفاءة وفاعلية (ÖZTÜRK,2018:220). يشمل ذلك مجموعة واسعة من الضوابط:

- **ضوابط إدارة الأصول:** حصر وتصنيف الأصول الرقمية.
- **ضوابط إدارة الهويات والصلاحيات:** التأكد من تطبيق مبدأ أقل الامتيازات.
- **ضوابط أمن الشبكات:** مراجعة جدران الحماية، وأنظمة كشف التسلل (Instruction Detection System IDS)، وقوائم التحكم في الوصول (Access Control Lists ACLs) (Jarison, Morris &, Wilkinson, 2018: 16)
- **ضوابط حماية البيانات:** التأكد من تشفير البيانات أثناء النقل والتخزين.

يُعد نقص المعرفة بالضوابط التقنية أحد التحديات التي تواجه المراجع الداخلي، مما قد يؤدي إلى عدم فعالية المراجعة (Agrafiotis, Nurse, Goldsmith, Creese & Upton,2019:2). لذلك، أصبح مطلوبًا من المراجع الداخلي فهم أساسيات تكنولوجيا المعلومات (IIA,2020).

الدراسة الميدانية:

منهج الدراسة:

اعتمدت الدراسة المنهج الوصفي التحليلي:

الوصفي: تم استخدام هذا الجزء من المنهج لوصف وتحليل الوضع الحالي لأنشطة المراجعة الداخلية ذات العلاقة بالأمن السيبراني ومستوى مخاطر الأمن

السيبراني في البنوك اليمنية من وجهة نظر المراجعين الداخليين. وتم ذلك من خلال جمع البيانات الكمية وتحليلها لوصف خصائص العينة وتوزيعات إجاباتهم حول متغيرات الدراسة.

التحليلي: تم استخدام هذا الجزء لتحليل العلاقة بين المتغير المستقل (انشطة المراجعة الداخلية المرتبطة بمخاطر الأمن السيبراني بأبعادها) والمتغير التابع (مخاطر الأمن السيبراني). تم تطبيق الأساليب الإحصائية الاستدلالية لتحديد طبيعة وقوة هذا الأثر واختبار فرضيات الدراسة. ويهدف هذا التحليل إلى فهم كيف تساهم انشطة المراجعة الداخلية ذات العلاقة بالأمن السيبراني المختلفة في الحد من مخاطر الأمن السيبراني في البنوك اليمنية.

مجتمع الدراسة

يشمل مجتمع الدراسة جميع المراجعين الداخليين العاملين في البنوك اليمنية في أمانة العاصمة صنعاء وعددها (١٩ بنكا).

عينة الدراسة

نظرا لصغر مجتمع الدراسة فقد تم تحديد حجم العينة باستخدام المسح الشامل، حيث تم توزيع (١٠٠) استبيانا على المراجعين الداخليين العاملين في المراكز الرئيسية والفروع للبنوك اليمنية التجارية والإسلامية بأمانة العاصمة صنعاء، كان عدد المسترد منها (٨٨) استبانة وأصبحت الاستبيانات الصالحة للتحليل الاحصائي (٨٢)استبياناً.

أداة جمع البيانات

تم استخدام الاستبيان لجمع البيانات من أفراد العينة. ويتضمن قسمين كما يلي

القسم الأول: المعلومات الشخصية (Demographic Information) تضمن هذا القسم (النوع، المؤهل العلمي، المسمى الوظيفي، سنوات الخبرة، الخبرة التكنولوجية، الشهادات المهنية، عدد موظفي المراجعة، وجود إدارة/قسم لتكنولوجيا المعلومات، وجود إدارة/قسم للأمن السيبراني).

القسم الثاني: أسئلة المتغيرات الرئيسية:

انشطة المراجعة الداخلية ذات العلاقة بالأمن السيبراني: يتضمن هذا القسم (٣٢) عبارة تقيس ثلاثة أبعاد تتعلق بأنشطة المراجعة الداخلية بمجال الأمن السيبراني (تقييم مخاطر الأمن السيبراني، الانشطة التخطيطية الفعلية للمراجعة الداخلية، وانشطة فحص المراجعة الداخلية للأدوات الرقابية المتعلقة بالأمن السيبراني،). اعتمد فيها مقياس ليكرت الخماسي (ابدا، نادرا، احيانا، غالبا، دائما) لقياس درجة ممارسة المستجيبين.

مخاطر الأمن السيبراني: يتضمن هذا القسم (٩) عبارات تقيس مستوى المخاطر في البنوك اليمنية. تم استخدام مقياس ليكرت الخماسي (ابدا، نادرا، احيانا، غالبا، دائما) لقياس درجة تكرار المخاطر والتهديدات وفق اراء المستجيبين.

صدق أداة الدراسة

بهدف التأكد من أن الاستبيان يقيس بالفعل المفاهيم التي صمم لقياسها. تم استخدام الاجراءات الآتية:

صدق المحتوى:(Content Validity) تم عرض الاستبيان على مجموعة من المحكمين المتخصصين في المراجعة وتكنولوجيا المعلومات وامن تكنولوجيا المعلومات والأكاديميين لتقييم مدى ملاءمة العبارات وشموليتها لأبعاد المتغيرات التي تقيسها. وقد تم إجراء التعديلات بناءً على ملاحظات المحكمين.

ثبات الاستبانة:

اعتمدت هذه الدراسة معامل ألفا كرونباخ (Cronbach's Alpha Coefficient)، الذي يأخذ قيما تتراوح بين الصفر والواحد الصحيح، فإذا لم يكن هناك ثبات في البيانات فإن قيمة المعامل تكون مساوية للصفر، وعلى العكس إذا كان هناك ثبات تام في البيانات فإن قيمة المعامل تساوي الواحد الصحيح، أي أن زيادة معامل ألفا كرونباخ تعني زيادة مصداقية البيانات من عكس نتائج العينة على مجتمع الدراسة، كما أن انخفاض القيمة عن (٦٠٪) دليل على انخفاض الثبات الداخلي، وتعتمد معادلة ألفا كرونباخ على تباينات فقرات الاختبار، وتشترط أن تقيس بنود الاختبار سمة واحدة فقط، ولذلك تم حساب معامل الثبات لكل مجال على " انفراد "، والجدول التالي يوضح قيم معاملات ألفا كرونباخ لمجالات الأداة:

جدول (١)معامل ألفا كرونباخ (Cronbach , s Alpha)

البعد (Dimension)	عدد الفقرات (N of Items)	معامل ألفا كرونباخ (Cronbach's Alpha)	مستوى الموثوقية (Reliability Level)
أنشطة تقييم مخاطر الأمن السيبراني	12	0.825	جيد جداً
الانشطة التخطيطية للمراجعة الداخلية	9	0.781	جيد
أنشطة فحص الأدوات الرقابية المتعلقة بالأمن السيبراني	11	0.851	جيد
الانشطة مجتمعة	32	0.925	ممتاز
مخاطر الامن السيبراني	9	0.789	جيد جدا
الاداة ككل	41	0.773	جيد

المصدر: نتائج التحليل الاحصائي لبيانات الدراسة الميدانية

كما يوضح جدول (١)، تجاوزت قيمة معامل ألفا كرونباخ لجميع الأبعاد ٠.٧٧٠، مما يُعد مؤشرًا قويًا على الاتساق الداخلي الجيد.

حصل بُعد "أنشطة تقييم مخاطر الأمن السيبراني" على معامل قدره ٠.٨٢٥، مما يعكس ثباتًا جيدًا جدًا، وحقق، بُعد أنشطة فحص الأدوات الرقابية المتعلقة بالأمن السيبراني" ثباتًا جيدًا جدًا بمعامل ٠.٨٥١، وحققت "الأنشطة مجتمعة" ثباتًا عالياً بقيمة ٠.٩٢٥، وهذا يؤكد وجود ترابط قوي بين فقراته. تُقدم هذه النتائج دليلًا على أن الاستبانة تُعد أداة موثوقة للقياس، وأن البيانات التي تم جمعها متسقة وذات مصداقية عالية، مما يدعم صحة النتائج التي توصلت إليها الدراسة.

طريقة تفسير نتائج الأداة:

تم تفسير قيم المتوسطات الحسابية لفقرات الاستبيان وفقا لقاعدة فيشر، بتقسيم تدريج القياس بحسب بدائل الاستبيان إلى خمس فئات يبلغ طول الفئة الواحدة (٠.٨٠)، وقد تم الحصول على طول كل فئة من الفئات الخمس من خلال حساب مدى أوزان الاستبيان والبالغ (٥- ١ = ٤) وتقسيم هذا المدى على عدد أوزان القياس، وبإضافة هذا الطول إلى الوزن الأدنى للقياس نحصل على الحد الأعلى للفئة الأولى وهو (١.٨٠)، لتكون القيمة (١.٨١) هي الحد الأدنى للفئة الثانية، وبإضافة الطول (٠.٨٠) إلى الحد الأدنى للفئة الثانية نحصل على الحد الأعلى لهذه الفئة والبالغ (٢.٦٠)، وهكذا بالنسبة لبقية الفئات. والجدول (٢) يوضح ذلك:

جدول (٢) تقدير بدائل أوزان القياس

درجة الموافقة	الفئة
ابدا	1 - 1.79
نادرا	1.80- 2.59
احيانا	2.60- 3.39
غالبا	3.40- 4.19
دائما	4.20- 5

الاحصاء الوصفي:

الخصائص الديموغرافية للمستجيبين

الإحصاء الوصفي لاستخراج التكرارات والنسبة المئوية لوصف خصائص عينة الدراسة، واستخلاص النتائج في الجداول الآتية:

جدول (٣)خصائص عينة الدراسة

الخاصية الديموغرافية	الفئة	العدد (ن)	النسبة المئوية (٪)	الخاصية الديموغرافية	الفئة	العدد (ن)	النسبة المئوية (٪)
الجنس	ذكر	68	83	الشهادات المهنية	محاسب قانوني معتمد (CPA)	12	14.6
					مراجع داخلي معتمد (CIA)	8	9.8
	أنثى	14	17		أخرى	28	34.1
	المجموع	82	100		لا يوجد	34	41.5
المؤهل العلمي	بكالوريوس	40	48.8		المجموع	82	100
	دبلوم عالي	7	8.5	عدد موظفي المراجعة	خمسة فأقل	30	36.6
	ماجستير	30	36.6		من ٦ - ١٠	28	34.1
	دكتوراه	5	6.1		من ١١ - ٢٠	15	18.3
	المجموع	82	100		من ٢١ - ٥٠	7	8.5
سنوات الخبرة	ثلاث سنوات فأقل	8	9.8		أكثر من ٥٠	2	2.4
	٤ - ٥ سنوات	15	18.3		المجموع	82	100
	٦ - ١٠ سنوات	25	30.5	وجود إدارة/قسم لتكنولوجيا المعلومات	متوفر	70	85.4
	١١ - ١٥ سنة	20	24.4		غير متوفر	12	14.6
	أكثر من ١٥ سنة	14	17.1		المجموع	82	100
	المجموع	82	100	وجود إدارة/قسم للأمن السيبراني	متوفر	17	20.7
الوظيفة	مدير مراجعة داخلية	10	12.2		غير متوفر	65	79.3
	رئيس قسم	20	24.4		المجموع	82	100
	مراجع أول	25	30.5	مستوى الخبرة في تكنولوجيا المعلومات	ضعيفة	10	12.2
	مراجع	22	26.8		متوسطة	35	42.7
	أخرى	5	6.1		جيدة	30	36.6
	المجموع	82	100		لا أعرف	7	8.5
					المجموع	82	100

المصدر: من إعداد الباحثين بناءً على نتائج التحليل الإحصائي لبيانات الدراسة الميدانية.

١. الجنس

تُظهر البيانات في الجدول (٣) أن الذكور يمثلون الغالبية العظمى من العينة بنسبة ٨٣٪ (ن=٦٨)، بينما تشكل الإناث ١٧٪ فقط (ن=١٤). يُعد هذا التوزيع متسقاً مع التركيبة الديموغرافية السائدة في القطاع المصرفي والمهني في اليمن، حيث لا يزال تمثيل الإناث في المناصب القيادية والتخصصية، مثل المراجعة الداخلية، محدوداً. يُشير هذا التفاوت إلى أن وجهات النظر التي تم جمعها في هذه الدراسة تعكس بشكل أساسي منظور الذكور في هذا القطاع.

٢. المؤهل العلمي

تتسم العينة في الجدول (٣) بمستوى تعليمي عالٍ، حيث يحمل ٤٨.٨٪ (ن=٤٠) من المستجيبين درجة البكالوريوس، و٣٦.٦٪ (ن=٣٠) درجة الماجستير. كما أن هناك نسبة من حملة الدبلوم العالي (٨.٥٪، ن=٧) والدكتوراه (٦.١٪، ن=٥). يُعزز هذا التوزيع من مصداقية البيانات، إذ يُفترض أن المستجيبين ذوي المؤهلات الأكاديمية المرتفعة يمتلكون فهماً أعمق للمفاهيم المعقدة المتعلقة بالمراجعة الداخلية ومخاطر الأمن السيبراني.

٣. سنوات الخبرة في العمل

يُظهر الجدول (٣) أن معظم المستجيبين يمتلكون خبرة عملية متوسطة إلى عالية: ٣٠.٥٪ (ن=٢٥) لديهم خبرة تتراوح بين ٦- ١٠ سنوات، و٢٤.٤٪ (ن=٢٠) بين ١١- ١٥ سنة، و١٧.١٪ (ن=١٤) أكثر من ١٥ سنة. يُشير هذا إلى أن غالبية المشاركين (حوالي ٧٢٪ لديهم ٦ سنوات خبرة فأكثر) لديهم معرفة عملية واسعة بالنظم المصرفية والمراجعة الداخلية، مما يُضيف قيمة لأجوبتهم حول القضايا المطروحة في الاستبيان.

٤. الوظيفة

تتوزع الوظائف في الجدول (٣) بشكل يُمثل مستويات إدارية مختلفة داخل إدارات المراجعة الداخلية. النسبة الأكبر هي للمراجعين الأول (٣٠.٥٪، ن=٢٥) والمراجعين (٢٦.٨٪، ن=٢٢)، يليهم رؤساء الأقسام (٢٤.٤٪، ن=٢٠) ومديرو المراجعة الداخلية

(١٢.٢٪، ن=١٠). يُمكن هذا التنوع الباحثين من الحصول على رؤى شاملة تغطي الجوانب التشغيلية والإشرافية والإدارية لدور المراجعة الداخلية.

٥. الشهادات المهنية

يُلاحظ من الجدول (٣) أن ٤١.٥٪ (ن=٣٤) من المستجيبين لا يمتلكون شهادات مهنية متخصصة في مجال المراجعة أو المحاسبة. من بين الحاصلين على شهادات، يُعد المحاسب القانوني المعتمد (CPA) الأعلى بنسبة ١٤.٦٪ (ن=١٢)، بينما يُشكل المراجع الداخلي المعتمد (CIA) نسبة ٩.٨٪ (ن=٨). وجود نسبة من فئة "أخرى" (٣٤.١٪، ن=٢٨) قد يشير إلى تنوع في الشهادات المهنية الأخرى غير المذكورة تحديداً. تُشير هذه النتائج إلى أن الخبرة العملية والمؤهل الأكاديمي قد يلعبان دوراً أكبر من الشهادات المهنية المتخصصة في هذا القطاع.

٦. عدد موظفي المراجعة

تُظهر البيانات في الجدول (٣) أن معظم المستجيبين يعملون في أقسام مراجعة داخلية ذات حجم صغير إلى متوسط: ٣٦.٦٪ (ن=٣٠) يعملون في أقسام تضم خمسة موظفين فأقل، و٣٤.١٪ (ن=٢٨) في أقسام تضم من ٦- ١٠ موظفين. هذه الأرقام تُشير إلى أن العديد من البنوك اليمنية لديها أقسام مراجعة داخلية بأعداد محدودة، وهو ما قد يؤثر على نطاق وعمق تغطية المراجعة لمخاطر الأمن السيبراني، خاصة مع محدودية الموارد البشرية المتخصصة.

٧. وجود إدارة/قسم لتكنولوجيا المعلومات والأمن السيبراني

وجود إدارة/قسم لتكنولوجيا المعلومات: تُشير البيانات في الجدول (٣) إلى أن ٨٥.٤٪ (ن=٧٠) من المستجيبين أفادوا بوجود إدارة أو قسم لتكنولوجيا المعلومات في بنوكهم، بينما ١٤.٦٪ (ن=١٢) أفادوا بعدم توفره. هذه النسبة المرتفعة تُعد مؤشراً إيجابياً على تطور البنية التحتية لتكنولوجيا المعلومات في البنوك اليمنية.

٨.وجود إدارة/قسم للأمن السيبراني:

على النقيض، أفاد ٧٩.٣٪ (ن=٦٥) من المستجيبين بعدم توفر إدارة أو قسم مخصص للأمن السيبراني في بنوكهم، بينما ٢٠.٧٪ (ن=١٧) فقط أكدوا توفره. تُعد

هذه النتيجة ذات أهمية بالغة، حيث تُشير إلى أن معظم البنوك لا تمتلك كياناً تنظيمياً منفصلاً ومخصصاً بشكل كامل للأمن السيبراني، بل قد تكون مسؤوليات الأمن السيبراني مدمجة ضمن مهام قسم تكنولوجيا المعلومات الأوسع. هذا الجانب يستدعي تحليلاً معمقاً لكيفية تأثير هذا الهيكل التنظيمي على فعالية إدارة مخاطر الأمن السيبراني ودور المراجعة الداخلية فيه.

٩. مستوى الخبرة في تكنولوجيا المعلومات

تُشير البيانات في الجدول (٣) إلى أن ٧٩.٣٪ من المستجيبين يمتلكون خبرة متوسطة (٤٢.٧٪، ن=٣٥) أو جيدة (٣٦.٦٪، ن=٣٠) في تكنولوجيا المعلومات. تُعد هذه النتيجة مشجعة جداً، ففهم المراجعين الداخليين للتكنولوجيا يُعتبر حجر الزاوية في قدرتهم على تقييم مخاطر الأمن السيبراني وضوابطها. على الرغم من أن نسبة ١٢.٢٪ أفادوا بخبرة ضعيفة، إلا أن الغالبية العظمى تتمتع بمستوى كافٍ من المعرفة التكنولوجية وهذا يدعم دورهم في مراجعة الأمن السيبراني.

تُظهر الخصائص الديموغرافية لعينة الدراسة أنها تتكون بشكل أساسي من ذكور يتمتعون بمؤهلات أكاديمية عالية وخبرة عملية واسعة في مجال المراجعة الداخلية. تُشير البيانات إلى وعي جيد بمفاهيم تكنولوجيا المعلومات بين المراجعين. ومع ذلك، تُبرز النتائج تحدياً يتمثل في محدودية وجود أقسام مخصصة للأمن السيبراني بشكل مستقل في معظم البنوك، مما قد يُلقي بظلاله على نطاق المراجعة الداخلية وقدرتها على التعامل مع التهديدات السيبرانية المتزايدة. تُقدم هذه البيانات الديموغرافية أساساً قوياً لفهم السياق الذي ستُحلل فيه متغيرات الدراسة الرئيسية.

التحليل الوصفي: إطار إدارة الأمن السيبراني المعتمد:

يُقدم جدول (٤) نظرة على الأطر المعتمدة لإدارة الأمن السيبراني في البنوك اليمنية. بما أن مجموع النسب المئوية الكلي (١٠٠٪) يُشير إلى مجموع الخيارات المختارة (٢٠٣)، فهذا يؤكد أن المستجيبين يُمكنهم اختيار أكثر من إطار واحد، مما يُفسر تجاوز مجموع الاستجابات لعدد المستجيبين الإجمالي (٨٢).

الجدول (٤) الأطر المعتمدة لإدارة الأمن السيبراني في البنوك اليمنية

إطار إدارة الأمن السيبراني المعتمد	العدد (ن)	النسبة المئوية (٪)
إطار المعهد الوطني الأمريكي للمعايير والتكنولوجيا (NIST)	40	19.7
معايير خدمة الثقة AICPA	15	7.4
إطار المنظمة الدولية لمعايير الجودة (ISO) ٢٧٠٠١	50	24.6
إطار (COSO ERM) للأمن السيبراني	25	12.3
إطار أهداف رقابة المعلومات والتقنيات ذات الصلة (COBIT)	35	17.2
إطار الجمعية الدولية لتدقيق ومراقبة الأنظمة (ISACA)	20	9.9
إطار عمل تم تطويره ذاتياً	10	4.9
لا يستخدم أي إطار	8	3.9
المجموع	203	100.0

المصدر: من إعداد الباحثين بناءً على نتائج التحليل الإحصائي لبيانات الدراسة الميدانية.

يشير الجدول رقم (٤) إلى أن البنوك اليمنية تتبنى مجموعة متنوعة من أطر إدارة الأمن السيبراني، مع ميل واضح لتبني عدة أطر في آنٍ واحد (مجموع الاستجابات ٢٠٣). هذا النهج المتعدد يُمكن أن يُعزز شمولية ومرونة إدارة المخاطر السيبرانية.

يبرز إطار المنظمة الدولية لمعايير الجودة (ISO27001) كالإطار الأكثر استخداماً بنسبة (٢٤.٦٪)، مما يعكس سعي البنوك للامتثال للمعايير الدولية في إدارة أمن المعلومات. يليه إطار المعهد الوطني الأمريكي للمعايير والتكنولوجيا (NIST) بنسبة (١٩.٧٪)، ويُشير تبنيه إلى اهتمام بالنهج القائم على المخاطر. كما يحتل إطار COBIT المرتبة الثالثة بنسبة (١٧.٢٪)، مما يؤكد التركيز على حوكمة تكنولوجيا المعلومات والرقابة.

كما كان اعتماد معايير خدمة الثقة(AICPA) بنسبة (٧.٤٪)، و (ISACA) بنسبة(٩.٩٪)، و (COSO ERM) بنسبة (١٢.٣٪)) وهي نسب تبني أقل، مما قد يُشير إلى أن الأولوية تُعطى لأطر أمن المعلومات وحوكمة تكنولوجيا المعلومات على حساب تلك التي تُركز بشكل خاص على المراجعة أو إدارة المخاطر المؤسسية الشاملة للأمن السيبراني. وجود إطار عمل تم تطويره ذاتياً بنسبة (٤.٩٪) يُبرز كذلك مرونة بعض البنوك في تكييف حلولها.

غياب الأطر الرسمية: تُعد نسبة (٣.٩٪) من الاستجابات التي تُفيد بعدم استخدام أي إطار رسمي (٨ بنوك من أصل ٨٢ مستجيباً). هذا القصور يُعرض هذه

البنوك لمخاطر سيبرانية أعلى بسبب الافتقار لنهج منظم ومتكامل في إدارة وحوكمة الأمن السيبراني.

وعليه تُظهر هذه البيانات أن البنوك اليمنية تُدرك أهمية أطر الأمن السيبراني، مع تفضيل واضح للمعايير الدولية المعروفة. ومع ذلك، يُعد استمرار عدد قليل من البنوك دون تبني أي إطار رسمي تحدياً يتطلب معالجة لضمان حصانة القطاع المصرفي اليمني ضد التهديدات السيبرانية.

الإحصاء الوصفي: الأدوار المتعلقة بتقييم مخاطر الأمن السيبراني

جدول (٥) المتوسطات الحسابية والانحراف المعياري والوزن النسبي والترتيب لفقرات الأدوار المتعلقة بتقييم مخاطر الأمن السيبراني

	العبارة	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي (٪)	الترتيب	درجة الممارسة
١	تعمل المراجعة الداخلية بشكل استباقي للتعرف على مدى إمكانية تعرض البنك لمخاطر الأمن السيبراني.	3.99	1.3	79.8	3	غالباً
	تعمل المراجعة الداخلية بشكل استباقي للتعرف على وضع الأمن السيبراني للبنك.	4.04	1.34	80.8	2	غالباً
٢	يتدرب المراجعون الداخليون على معايير الصناعة واتجاهات إدارة المخاطر السيبرانية.	3.93	1.5	78.5	4	غالباً
٣	تتفاعل المراجعة الداخلية بشكل استباقي مع المديرين التشغيليين الذين يمتلكون ويديرون المخاطر والضوابط وينفذون الإجراءات التصحيحية لمعالجة أوجه القصور في العمليات والرقابة.	3.98	1.34	79.5	5	غالباً
٤	تتفاعل المراجعة الداخلية بشكل استباقي مع وظائف إدارة مخاطر تكنولوجيا المعلومات والامتثال، والوظائف التي تلعب دوراً رئيسياً في وضع وتصميم برنامج الأمان السيبراني والمخاطر، والرقابة.	4.24	1.15	84.9	1	دائماً
٥	تتولى وظيفة المراجعة الداخلية عملية تقييم مدى نضج إدارة مخاطر الأمن السيبراني في البنك.	4.05	1.17	81	6	غالباً
٦	تناقش المراجعة الداخلية مدى نضج إدارة مخاطر الأمن السيبراني في البنك مع الإدارة العليا.	3.9	1.23	78	7	غالباً
٧	تناقش المراجعة الداخلية مدى نضج إدارة مخاطر الأمن السيبراني في البنك مع مجلس الإدارة/لجنة المراجعة.	3.44	1.44	68.8	8	غالباً
٨	تحدد المراجعة الداخلية عمليات إدارة المخاطر التي يحتاج مجلس الإدارة أو الإدارة العليا إلى ضمانها.	2.76	1.52	55.1	12	أحياناً
٩	تقدم المراجعة الداخلية مهام استشارية لدعم الإدارة في تحسين إدارة مخاطر الأمن السيبراني.	3.05	1.6	61	9	أحياناً
١٠	يستخدم المراجع الداخلي نهج المراجعة الداخلية القائم على المخاطر في مراجعة الأمن السيبراني.	3.13	1.4	62.7	10	أحياناً
١١	تقوم المراجعة الداخلية بتقييم التوافق بين استراتيجية الأمن السيبراني والاستراتيجية الشاملة لإدارة المخاطر في البنك.	3.01	1.36	60.1	11	أحياناً
	متوسط المحور	3.58	1.37	71.70%		غالباً

المصدر: من إعداد الباحثين بناءً على نتائج التحليل الإحصائي لبيانات الدراسة الميدانية.

يُظهر الجدول رقم (٥) أن المراجعين في البنوك اليمنية غالباً ما يمارسون أدوارهم المتعلقة بتقييم مخاطر الأمن السيبراني، حيث بلغ المتوسط الحسابي الكلي للمحور (٣.٥٨)، ووزن نسبي (٧١.٧٠٪)، وانحراف معياري (١.٣٧). تشير هذه النتيجة العامة إلى أن المراجعة الداخلية تضطلع بمهامها في هذا المجال بانتظام.

كما تظهر استجابات المستجيبين على فقرات المحور تفاوتاً، حيث تراوحت متوسطات العبارات بين (٢.٧٦) و (٤.٢٤)، تراوحت الانحرافات المعيارية بين (١.١٥) و (١.٦٠). هذا التباين يُشير إلى اختلاف في درجة ممارسة الأدوار، من الممارسة "أحياناً" إلى الممارسة "دائماً".

كما جاءت العبارة رقم (٥) ونصها "تتفاعل المراجعة الداخلية بشكل استباقي مع وظائف إدارة مخاطر تكنولوجيا المعلومات والامتثال، والوظائف التي تلعب دوراً رئيسياً في وضع وتصميم برنامج الأمان السيبراني والمخاطر، والرقابة" في المرتبة الأولى بمتوسط حسابي بلغ (٤.٢٤)، وبدرجة ممارسة "دائماً". هذا يُبرز التزام المراجعة الداخلية بالتعاون الفني والتشغيلي الوثيق مع الأقسام المتخصصة في تكنولوجيا المعلومات والأمن السيبراني، وهو ما يُعتبر أساساً لفهم المخاطر المعقدة وتطوير ضوابط رقابية فعالة. في المقابل، سجلت العبارة رقم (٩) ونصها "تحدد المراجعة الداخلية عمليات إدارة المخاطر التي يحتاج مجلس الإدارة أو الإدارة العليا إلى ضمانها" أدنى متوسط حسابي بلغ (٢.٧٦)، وبدرجة ممارسة "أحياناً". هذا التفاوت يسلط الضوء على فجوة في الدور الاستراتيجي للمراجعة الداخلية. فبينما هناك تفاعل جيد على المستوى الفني، يبدو أن قدرتها على ترجمة هذه التقييمات إلى متطلبات ضمان واضحة ومُوجهة لمستويات الحوكمة العليا (مجلس الإدارة والإدارة العليا) لا تزال بحاجة إلى تعزيز. هذا القصور قد يُعيق اتخاذ قرارات إستراتيجية مستنيرة بشأن إدارة مخاطر الأمن السيبراني على مستوى البنك ككل.

تُشير هذه النتائج إلى أن المراجعة الداخلية في البنوك اليمنية تقوم بجهود ملموسة في التقييم الفني لمخاطر الأمن السيبراني. ومع ذلك، هناك حاجة ملحة لتعزيز دورها في الحوكمة من خلال تفعيل آليات إيصال متطلبات الضمان بوضوح إلى صانعي القرار الرئيسيين. هذا التطور سيُسهم بشكل جوهري في رفع كفاءة إدارة المخاطر السيبرانية ويُعزز من القيمة المضافة لدور المراجعة الداخلية في حماية الأصول المصرفية.

محور: انشطة التخطيط :

جدول (٦)المتوسطات الحسابية والانحراف المعياري والوزن النسبي والترتيب لفقرات محور: انشطة التخطيط

	العبارة	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي (٪)	الترتيب	درجة الممارسة
١	تحدد المراجعة الداخلية ماهية الأصول الرقمية الأكثر قيمة للبنك (مثل التطبيقات وقواعد البيانات ومحركات أقراص الشبكة).	4.22	0.97	84.4	1	دائماً
٢	تحدد المراجعة الداخلية أماكن تخزين الأصول الرقمية الأكثر قيمة للبنك (مثل التطبيقات وقواعد البيانات ومحركات أقراص الشبكة).	4.02	1.1	80.4	2	غالباً
٣	تقيّم المراجعة الداخلية المخاطر السيبرانية للتعرف على نقاط الضعف المرتبطة بتخزين تلك الأصول.	3.4	1.14	68	5	غالباً
٤	تقيّم المراجعة الداخلية مدى احتمالية سرقة الأصول الرقمية للبنك أو اختراقها.	3.18	1.34	63.6	7	أحياناً
٥	تقيّم المراجعة الداخلية درجة تأثير سرقة الأصول الرقمية للبنك أو اختراقها.	2.92	1.31	58.4	9	أحياناً
٦	تحدد المراجعة الداخلية الأصول الرقمية الأخرى غير المستخدمة ومستويات الحماية التي تضمنها.	3.79	1	75.8	3	غالباً
٧	يقوم المراجعون الداخليون ببناء علاقات عمل جيدة مع الوظائف الأخرى للتحقق من فعالية الضوابط والعمليات بشكل كامل.	3.96	1.13	79.2	4	غالباً
٨	هناك تواصل متكرر بين المراجعة الداخلية مع مجلس الإدارة بشأن نتائج تقييم مخاطر الأمن السيبراني.	3.4	1.47	68	6	غالباً
٩	تصدر المراجعة الداخلية رأياً عاماً مستقلاً إلى مجلس الإدارة كجزء من تقديم ضمانات مستمرة بأن الضوابط الداخلية كافية وتعمل بفعالية.	3.16	1.16	63.2	8	أحياناً
	متوسط المحور	3.56	1.23	71.10%		غالباً

المصدر: من إعداد الباحثين بناءً على نتائج التحليل الإحصائي لبيانات الدراسة الميدانية.

يُظهر الجدول رقم (٦) أن المراجعين في البنوك اليمنية غالباً ما يمارسون الانشطة التخطيطية التي تتعلق بمراجعة الأمن السيبراني، حيث بلغ المتوسط الحسابي الكلي للمحور (٣.٥٦)، ووزن نسبي (٧١.١٠٪)، والانحراف المعياري بلغ (١.٢٣)، هذه النتيجة العامة تُشير إلى أن المراجعة الداخلية تضطلع بمهامها التخطيطية التي تتعلق بالأمن السيبراني بشكل منتظم.

تُظهر استجابات المستجيبين على فقرات المحور تبايناً، حيث تراوحت متوسطات العبارات بين (٢.٩٢) و (٤.٢٢)، وتراوحت الانحرافات المعيارية بين (٠.٩٧) و (١.٤٧). هذا

التفاوت يعكس اختلافاً في درجة الممارسة بين الانشطة التخطيطية المختلفة، من الممارسة "أحياناً" إلى الممارسة "دائماً". جاءت العبارة رقم (١) ونصها "تحدد المراجعة الداخلية ماهية الأصول الرقمية الأكثر قيمة للبنك (مثل التطبيقات وقواعد البيانات ومحركات أقراص الشبكة " في المرتبة الأولى بمتوسط حسابي بلغ (٤.٢٢)، وبدرجة ممارسة "دائماً". يُبرز هذا المستوى العالي من الممارسة إدراك المراجعة الداخلية لأهمية تحديد وحصر الأصول الرقمية الحيوية للبنك كخطوة أولى وأساسية في أي عملية تخطيط لمراجعة الأمن السيبراني. هذا يعكس نهجاً منهجياً في فهم نطاق المخاطر. في المقابل، سجلت العبارة رقم (٥) ونصها "تقيّم المراجعة الداخلية درجة تأثير سرقة الأصول الرقمية للبنك أو اختراقها" أدنى متوسط حسابي بلغ (٢.٩٢)، وبدرجة ممارسة "أحياناً".

هذا التباين يُشير إلى ضعف نسبي في قدرة المراجعة الداخلية على تقييم الأثر المالي أو التشغيلي الدقيق للخروقات الأمنية المحتملة. فبينما يتم تحديد الأصول، يبدو أن تقدير العواقب الفعلية لنقاط الضعف لا يزال يحتاج إلى تطوير. هذا القصور قد يؤثر على فعالية تخطيط المراجعة في تحديد الأولويات وتخصيص الموارد بناءً على حجم التأثير المحتمل للمخاطر.

تُشير هذه النتائج إلى أن المراجعة الداخلية في البنوك اليمنية تولي اهتماماً جيداً بالتخطيط لمراجعة الأمن السيبراني، خصوصاً فيما يتعلق بتحديد الأصول الرقمية الحيوية. ومع ذلك، هناك حاجة ملحة لتعزيز قدراتها في تقييم وتقدير تأثير المخاطر السيبرانية، وهو أمر بالغ الأهمية لتطوير خطط مراجعة قائمة على المخاطر بشكل أكثر فعالية وكفاءة. هذا التحسين سيُمكّن المراجعة الداخلية من توجيه جهودها نحو المجالات التي تحمل أعلى مستويات المخاطر والتأثير على البنك.

محور: انشطة فحص الأدوات الرقابية المتعلقة بالأمن السيبراني

جدول (٧)

المتوسطات الحسابية والانحراف المعياري والوزن النسبي والترتيب لفقرات محور: انشطة فحص الأدوات الرقابية المتعلقة بالأمن السيبراني

	العبارة	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي (٪)	الترتيب	درجة الممارسة
١	جدار الحماية	3.77	0.71	75.4	1	غالباً
٢	برامج مكافحة الفيروسات	3.68	1.12	73.6	2	غالباً
٣	أدوات مراقبة أمن الشبكة	3.12	1.08	62.4	7	أحياناً
٤	اختبار الاختراق	3.49	1.31	69.8	3	غالباً
٥	أدوات التشفير	3.14	1.31	62.8	6	أحياناً
٦	أدوات فحص ثغرات الويب	3.49	1.36	69.8	4	غالباً
٧	أدوات الدفاع عن الشبكة اللاسلكية (مثل نظام كشف التسلل اللاسلكي (WIDS) لتحديد الأجهزة اللاسلكية غير المصرح بها اكتشاف الهجمات واكتشاف الاختراقات الناجحة)	3.2	1.45	64	5	أحياناً
٨	نظام كشف التسلل (نظام كشف التسلل اللاسلكي (WIDS) لتحديد الأجهزة اللاسلكية غير المصرح بها، واكتشاف الهجمات واكتشاف الاختراقات الناجحة.)	3.2	1.49	64	5	أحياناً
٩	حماية نقطة النهاية (تعليمات تتعلق بالتزام مستخدمي الوصول عن بعد بالإجراءات والتعليمات الصادرة من البنك بهذا الشأن)	3.39	1.39	67.8	8	أحياناً
١٠	خدمات البنية التحتية للمفاتيح العمومية PKI (إجراءات للتحقق من انه يتم السماح لكل جهاز لاسلكي مشروع متصل بالشبكة للقيام متطلبات العمل المشروعة، ورفض الوصول إلى جميع الأجهزة اللاسلكية الأخرى، بما في ذلك أجهزة البلوتوث)	3.39	1.39	67.8	9	أحياناً
١١	أدوات الهندسة الاجتماعية	2.4	1.46	48	10	نادراً
	متوسط المحور	3.27	1.3	65.40%		أحياناً

المصدر: من إعداد الباحثين بناءً على نتائج التحليل الإحصائي لبيانات الدراسة الميدانية.

يُظهر الجدول رقم (٧) (أن المراجعين في البنوك اليمنية أحياناً ما يفحصون الأدوات الرقابية المتعلقة بالأمن السيبراني، بمتوسط حسابي كلي للمحور بلغ

(٣.٢٧) ووزن نسبي (٦٥.٤٠٪)، وانحراف معياري (١.٣). هذا يُشير إلى أن نطاق فحص المراجعة الداخلية لهذه الأدوات لا يزال يتطلب تعزيزاً.

تُظهر استجابات افراد العينة على فقرات المحور تفاوتاً كبيراً، حيث تراوحت متوسطات العبارات بين (٢.٤٠) و (٣.٧٧)، بينما تراوحت الانحرافات المعيارية بين (٠.٧١) و (١.٤٩). هذا التباين يعكس اختلافاً في درجة فحص الأدوات الرقابية، من الممارسة "النادرة" إلى الممارسة "غالباً". جاءت العبارة رقم (١) والتي تتعلق بفحص "جدار الحماية" في المرتبة الأولى بمتوسط حسابي بلغ (٣.٧٧) وبدرجة ممارسة "غالباً". تُشير هذه النتيجة إلى أن المراجعة الداخلية تُركز بشكل كبير على فحص الضوابط الأمنية الأساسية والمعروفة جيداً مثل جدران الحماية وبرامج مكافحة الفيروسات (متوسط ٣.٦٨، ترتيب ٢)، والتي تُعد خطوط دفاعية أولية في أي بنية أمنية. هذا يعكس اهتماماً بالأساسيات الأمنية المعترف بها. في المقابل، سجلت العبارة رقم (١١) والتي تتعلق بفحص "أدوات الهندسة الاجتماعية" أدنى متوسط حسابي بلغ (٢.٤٠) وبدرجة ممارسة "نادراً" هذا يُشير إلى ضعف في فحص المراجعة الداخلية للجوانب غير التقنية من التهديدات السيبرانية، خاصة تلك المرتبطة بالعنصر البشري واستغلال الثغرات الاجتماعية. هذا القصور يُعد نقطة ضعف، حيث أن الهندسة الاجتماعية تُشكل واحدة من أبرز وأنجح طرق الاختراق الحديثة، وتركيز المراجعة على الجوانب التقنية فقط قد يُغفل مخاطر جوهرية.

تُشير هذه النتائج إلى أن المراجعة الداخلية في البنوك اليمنية تركز في فحصها للأدوات الرقابية السيبرانية على الضوابط التقنية التقليدية والملموسة. ومع ذلك، تبرز فجوة كبيرة في فحص أدوات وتهديدات الهندسة الاجتماعية، بالإضافة إلى محدودية فحص أدوات متقدمة أخرى مثل أدوات مراقبة أمن الشبكة وأدوات التشفير. هذا التباين يُسلط الضوء على ضرورة توسيع نطاق فحص المراجعة الداخلية ليشمل أبعاداً أوسع من التهديدات السيبرانية، خاصة تلك التي تستهدف العنصر البشري والتقنيات الأقل شيوعاً في الفحص، وذلك لضمان تغطية شاملة وفعالة لمخاطر الأمن السيبراني المتطورة.

محور مخاطر الأمن السيبراني:

جدول (٨)

المتوسطات الحسابية والانحراف المعياري والوزن النسبي والترتيب لفقرات مخاطر الأمن السيبراني

	العبارة	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي (٪)	الترتيب	درجة التكرار
١	تتكرر حالات عدم الامتثال لسياسات وتعليمات الأمن السيبراني.	2.24	0.97	44.8	5	نادراً
٢	تتكرر حالات عدم الامتثال لمعايير الأمن السيبراني.	2.23	1.04	44.6	6	نادراً
٣	تتكرر حالات الإبلاغ عن نقاط الضعف في الرقابة الداخلية المتعلقة بالأمن السيبراني من قبل المراجعين الخارجيين و/أو مجلس الإدارة و/أو الإدارة التنفيذية.	2.47	1.83	49.4	1	نادراً
٤	تتكرر حالات أو حوادث أو تهديدات الأمن السيبراني التي يتم اكتشافها وإيقافها قبل أن تتسبب في خسائر مالية.	2.37	1.47	47.4	2	نادراً
٥	تتكرر حالات أو حوادث أو تهديدات الأمن السيبراني التي يتم اكتشافها وإيقافها قبل أن تتسبب في تعطيل الأعمال.	2.32	1.29	46.4	3	نادراً
٦	تتكرر حالات أو حوادث أو تهديدات الأمن السيبراني التي يتم اكتشافها وإيقافها قبل أن تؤدي إلى فقدان معلومات مهمة.	2.22	1.23	44.4	8	نادراً
٧	تتكرر هجمات الأمن السيبراني التي يتم اكتشافها وإيقافها بعد أن تتسبب في خسائر مالية.	2.29	1.22	45.8	4	نادراً
٨	تتكرر هجمات الأمن السيبراني التي يتم اكتشافها وإيقافها بعد أن تتسبب في تعطيل الأعمال.	2.29	1.41	45.8	4	نادراً
٩	تتكرر هجمات الأمن السيبراني التي يتم اكتشافها وإيقافها بعد أن تؤدي إلى فقدان معلومات مهمة.	2.23	0.74	44.6	7	نادراً
	متوسط المحور	2.28	1.21	45.60%		نادراً

المصدر: من إعداد الباحثين بناءً على نتائج التحليل الإحصائي لبيانات الدراسة الميدانية.

يُظهر الجدول رقم (٨) أن تكرار مخاطر الأمن السيبراني في البنوك اليمنية يُصنف "نادراً"، بمتوسط حسابي كلي للمحور بلغ (٢.٢٨) ووزن نسبي (٤٥.٦٠٪)، وانحراف معياري (١.٢١). هذه النتيجة العامة تُشير إلى أن المستجيبين لا يرون أن حوادث ومخاطر الأمن السيبراني تتكرر بشكل كبير في بيئة عملهم.

تُظهر استجابات المستجيبين على فقرات المحور تقارباً ملحوظاً، حيث تراوحت متوسطات العبارات بين (٢.٢٢) و (٢.٤٧)، بينما تراوحت الانحرافات المعيارية بين (٠.٧٤) و (١.٨٣). هذا التقارب يُشير إلى اتساق في تصور المراجعين حول التكرار المنخفض لهذه المخاطر.

جاءت العبارة رقم (٣) ونصها "تتكرر حالات الإبلاغ عن نقاط الضعف في الرقابة الداخلية المتعلقة بالأمن السيبراني من قبل المراجعين الخارجيين و/أو مجلس الإدارة و/أو الإدارة التنفيذية" في المرتبة الأولى بمتوسط حسابي بلغ (٢.٤٧)، ونادراً ما تتكرر، إلا أنها تُعد الأكثر تكراراً ضمن هذا المحور، مما قد يُشير إلى أن نقاط الضعف في الرقابة الداخلية يتم اكتشافها والإبلاغ عنها بشكل أكثر وضوحاً، ربما بسبب عمليات المراجعة الخارجية أو الرقابة الداخلية المعنية.

سجلت العبارة رقم (٦) ونصها "تتكرر حالات أو حوادث أو تهديدات الأمن السيبراني التي يتم اكتشافها وإيقافها قبل أن تؤدي إلى فقدان معلومات مهمة" أدنى متوسط حسابي بلغ (٢.٢٢)، ونادراً ما تتكرر، وحلت في المرتبة الاخيرة. يُشير هذا إلى أن حالات فقدان المعلومات المهمة الناتجة عن حوادث الأمن السيبراني، حتى تلك التي يتم اكتشافها وإيقافها مبكراً، تُعد الأقل تكراراً في تصور المستجيبين. وهذا يمكن أن يكون مؤشراً إيجابياً على فعالية الضوابط الوقائية والكاشفة في حماية البيانات المهمة.

تُشير هذه النتائج إلى أن المراجعين الداخليين في البنوك اليمنية ينظرون إلى ان مخاطر وحوادث الأمن السيبراني تتكرر بمستوى منخفض بشكل عام "نادراً". هذا التصور قد يعكس فعالية جزئية للضوابط الحالية أو قد يُشير إلى تحديات محتملة في رصد وكشف جميع حوادث الأمن السيبراني والإبلاغ عنها بشكل كامل وشفاف. وهنا من الضروري فهم ما إذا كان هذا الانخفاض في التكرار يعود إلى قوة أنظمة الدفاع، أو إلى طبيعة التهديدات التي قد تكون غير مرئية أو لا تُبلغ عنها بالكامل، وهو ما يستدعي مزيداً من التحليل في سياق فعالية المراجعة الداخلية.

ثانيا اختبار فرضيات الدراسة:

لاختبار فرضيات الدراسة تم استخدام تحليل الانحدار الخطي المتعدد Analysis Multiple Linear Regression **بطريقة** (Enter).

جدول (٩)

نتائج تحليل الانحدار المتعدد لأثر أنشطة المراجعة الداخلية على مخاطر الامن السيبراني

المتغيرات المستقلة	Beta (β)	T	Sig.	R	R مربع	F	Sig.	القرار
الثابت	5.523	23.063	0.000	0.877	0.769	86.539	0.000	
انشطة تقييم مخاطر الأمن السيبراني	-0.347	-4.426	0.000					رفض فرضية العدم
الانشطة التخطيطية للمراجعة الداخلية	-0.308	-3.320	0.001					رفض فرضية العدم
فحص الأدوات الرقابية المتعلقة بالأمن السيبراني	-0.319	-3.339	0.001					رفض فرضية العدم

المصدر: من إعداد الباحثين بناءً على نتائج التحليل الإحصائي لبيانات الدراسة الميدانية.

بناءً على نتائج تحليل الانحدار المتعدد بطريقة (Enter) **لأثر أنشطة المراجعة الداخلية على مخاطر الأمن السيبراني في الجدول (٩)، يتضح ما يلي:**

الفرضية الرئيسية:

تشير قيمة (Sig.) **لنموذج الانحدار ككل إلى وجود أثر ذي دلالة إحصائية لأبعاد انشطة المراجعة الداخلية مجتمعة على مخاطر الأمن السيبراني** (F = 86.539، Sig = ٠.٠٠٠ < ٠.٠٥). **ويوضح معامل التحديد** (R^2 = ٠.٧٦٩) **أن ٧٦.٩٪ من التباين في مخاطر الأمن السيبراني يمكن تفسيره من خلال أبعاد أنشطة المراجعة الداخلية المدرجة في النموذج. لذلك، يتم رفض الفرضية الرئيسية التي تنص على " لا يوجد أثر ذو دلالة احصائية عند مستوى معنوية** (α≥٠.٠٥) **لأنشطة المراجعة الداخلية**

المرتبطة بالأمن السيبراني (أنشطة تقييم المخاطر، أنشطة التخطيط، أنشطة فحص الادوات الرقابية) على مخاطر الأمن السيبراني في البنوك اليمنية"، وقبول الفرضية البديلة التي تشير إلى وجود هذا الأثر.

الفرضيات الفرعية:

١. الفرضية الفرعية الأولى:" لا يوجد أثر ذو دلالة احصائية عند مستوى معنوية (α≤٠.٠٥) لأنشطة تقييم مخاطر الأمن السيبراني على مخاطر الأمن السيبراني في البنوك اليمنية.

تشير قيمة (Sig.) لمتغير " انشطة تقييم مخاطر الأمن السيبراني " بالجدول (٩) إلى وجود أثر ذي دلالة إحصائية لهذا البعد على مخاطر الأمن السيبراني (t=-4.426، Sig.=٠.٠٠٠<٠.٠٥). يشير معامل بيتا (Beta = - ٠.٣٤٧) إلى أن الأثر **سلبي وذو دلالة إحصائية**، مما يعني أن زيادة ممارسة المراجعة الداخلية لأنشطة تقييم مخاطر الأمن السيبراني تؤدي إلى **انخفاض** مخاطر الأمن السيبراني. لذلك، يتم **رفض فرضية العدم** المتعلقة بهذا البعد وقبول الفرضية البديلة التي تنص على " يوجد أثر ذو دلالة إحصائية عند مستوى معنوية (α≤٠.٠٥) لأنشطة تقييم مخاطر الأمن السيبراني على مخاطر الأمن السيبراني ".

٢. الفرضية الفرعية الثانية: " لا يوجد أثر ذو دلالة احصائية عند مستوى معنوية (α≤٠.٠٥) لأنشطة التخطيط على مخاطر الأمن السيبراني في البنوك اليمنية"

تشير قيمة (Sig.) لمتغير "الأنشطة التخطيطية للمراجعة الداخلية" بالجدول (٩) إلى وجود أثر ذي دلالة إحصائية لهذا البعد على مخاطر الأمن السيبراني (t=-3.320، Sig.=٠.٠٠١<٠.٠٥). يشير معامل بيتا (Beta = - ٠.٣٠٨) إلى أن الأثر **سلبي وذو دلالة إحصائية**، مما يعني أن زيادة ممارسة لمراجعة الداخلية لأنشطتها التخطيطية تؤدي إلى **انخفاض** مخاطر الأمن السيبراني. لذلك، يتم **رفض فرضية العدم** المتعلقة بهذا البعد وقبول الفرضية البديلة التي تنص على " يوجد أثر ذو دلالة

احصائية عند مستوى معنوية (α≤٠.٠٥) لأنشطة التخطيط على مخاطر الأمن السيبراني في البنوك اليمنية.

٣. الفرضية الفرعية الثالثة:" لا يوجد أثر ذو دلالة احصائية عند مستوى معنوية (α≤٠.٠٥) لأنشطة فحص الادوات الرقابية على مخاطر الأمن السيبراني في البنوك اليمنية.

تشير قيمة (Sig.) لمتغير " فحص الأدوات الرقابية المتعلقة بالأمن السيبراني" بالجدول (٩) إلى وجود أثر ذي دلالة إحصائية لهذا البعد على مخاطر الأمن السيبراني ((t=−-3.339، Sig).=٠.٠٠١<٠.٠٥) يشير معامل بيتا (Beta = - ٠.٣١٩) إلى أن الأثر سلبي وذو دلالة إحصائية، مما يعني أن زيادة ممارسة المراجعة الداخلية لفحص الأدوات الرقابية المتعلقة بالأمن السيبراني من قبل المراجعة الداخلية تؤدي إلى **الحد من** مخاطر الأمن السيبراني. لذلك، يتم **رفض فرضية العدم** المتعلقة بهذا البعد وقبول الفرضية البديلة التي تنص على " يوجد أثر ذو دلالة احصائية عند مستوى معنوية (α≤٠.٠٥) لأنشطة فحص الادوات الرقابية على مخاطر الأمن السيبراني في البنوك اليمنية.

مناقشة النتائج

تهدف هذه الدراسة إلى تحليل أثر انشطة المراجعة الداخلية على مخاطر الأمن السيبراني بالبنوك اليمنية. لقد أظهرت النتائج الإحصائية، وجود علاقة عكسية وذات دلالة إحصائية بين أبعاد المراجعة الداخلية (تقييم المخاطر، الأدوار التخطيطية، تدقيق الأدوات الرقابية) ومستوى مخاطر الأمن السيبراني. هذه النتيجة ترفض الفرضيات الصفرية للدراسة وتؤكد أن المراجعة الداخلية تلعب دوراً محورياً في تخفيف هذه المخاطر، وهو ما ينسجم مع التحديات المتزايدة التي يواجهها القطاع المصرفي في اليمن والعالم من الهجمات السيبرانية كما أبرزتها مشكلة الدراسة.

مستوى مخاطر الأمن السيبراني

أظهر التحليل الوصفي أن مستوى تكرار مخاطر الأمن السيبراني في البنوك اليمنية يعتبر منخفضاً نسبياً (متوسط كلي ٢.٢٨). قد يُشير هذا إلى فعالية نسبية للضوابط القائمة، أو قد يُفسر في ضوء ما أشارت إليه دراسة AL-KHULAIDI, et. Al,2022) حول غياب التنسيق الأمني وعدم توفر آليات مستمرة لمعالجة المعلومات الأمنية. هذا يعني أن الوعي بمدى تكرار الحوادث قد يكون محدوداً لدى المستجيبين بسبب ضعف آليات الكشف والإبلاغ، مما يُلقي بمسؤولية إضافية على المراجعة الداخلية لضمان فعالية هذه الآليات نفسها.

أثر انشطة تقييم مخاطر الأمن السيبراني

أظهرت النتائج أن لتقييم المراجعة الداخلية لمخاطر الأمن السيبراني أثراً سلبياً وذا دلالة إحصائية على مستوى هذه المخاطر. هذا يعني أنه كلما زاد تركيز المراجعة الداخلية على تحديد وتقييم المخاطر السيبرانية، انخفضت هذه المخاطر. هذه النتيجة تتوافق بشكل كبير مع دراسات سابقة مثل دراسة Islam, et. al. (٢٠١٨) التي أكدت العلاقة بين كفاءة المراجعة الداخلية وتقييم المخاطر السيبرانية، ودراسة Darmawati (٢٠٢٢) التي أشارت إلى تأثير تقييم المخاطر الإيجابي على فعالية الأمن السيبراني. ومع ذلك، كشف التحليل الوصفي عن أن هذا الأثر يمكن تعزيزه بشكل أكبر، حيث لوحظ ضعف في تحديد العمليات الاستراتيجية التي يحتاجها مجلس الإدارة (متوسط ٢.٧٦) وتقديم المهام الاستشارية (متوسط ٣.٠٥). هذا يتقاطع مع ما أشارت إليه دراسة (Nasser, et. al.، ٢٠٢٠) حول ضعف تقييم نقاط الضعف وعدم كفاية مراجعة الالتزام في البنوك اليمنية، مما يشير إلى ضرورة تطوير الدور الاستشاري للمراجعة الداخلية لرفع تقارير أكثر عمقاً للإدارة العليا ومجلس الإدارة، بما يتماشى مع أفضل الممارسات.

أثر أنشطة التخطيط لمراجعة الامن السيبراني:

كما بينت النتائج أن للأنشطة التخطيطية للمراجعة الداخلية أثراً سلبياً وذا دلالة إحصائية على مخاطر الأمن السيبراني هذا يؤكد أن التخطيط الفعال لأنشطة المراجعة الداخلية يساهم في الحد من المخاطر، وهو ما ينسجم مع استنتاجات دراسة (الزيود، ٢٠٢١) التي أكدت أثر التخطيط في تقليل المخاطر

السيبرانية. على الرغم من هذا الأثر الإيجابي، أشار التحليل الوصفي إلى تحديات في تقدير احتمالية وقوع الهجمات أو تأثيرها (متوسط ٣.١٨ و٢.٩٢ على التوالي). هذه الفجوة في التخطيط القائم على تقدير دقيق للمخاطر قد تحد من الفاعلية الكلية للمراجعة، ويتوافق ذلك مع ما توصلت إليه دراسة Slapničar, et. al, (٢٠٢٢) بأن التخطيط وحده، وإن كان إيجابياً، قد لا يرتبط دائماً بكفاءة الإبلاغ عن المخاطر لمجلس الإدارة. هذا يستلزم تعميق قدرات المراجعين في تحليل المخاطر بشكل كمي وشمولي.

أثر انشطة فحص الأدوات الرقابية المتعلقة بالأمن السيبراني

كان لأنشطة فحص المراجعة الداخلية للأدوات الرقابية التأثير الأكبر بين المتغيرات المستقلة في خفض مخاطر الأمن السيبراني هذا يُبرز الدور الحاسم لمراجعة فعالية الضوابط والأدوات الأمنية. هذه النتيجة تتفق مع دراسة Shamsuddin, et. al. (٢٠٢٠) التي أكدت فعالية المراجعة الداخلية في إدارة الأمن السيبراني في المؤسسات المصرفية. ومع ذلك، كشف التحليل الوصفي عن نقطة ضعف بالغة الأهمية في ضعف فحص أدوات الهندسة الاجتماعية (متوسط ٢.٤٠) إضافة إلى بعض جوانب المراقبة والتشفير. هذا النقص يتوافق مع ما ذكرته دراسة AL-KHULAIDI, et. al. (٢٠٢٢) حول الافتقار إلى برامج التدريب والتوعية، وتقرير كاسبر سكاي عن انتشار برامج التجسس والفدية في اليمن. يُشكل هذا التفاوت تحدياً، حيث أن إغفال مراجعة التهديدات الحديثة والمتطورة مثل الهندسة الاجتماعية قد يُضعف من الحصانة الكلية للبنوك، ويقلل من فعالية المراجعة الداخلية في مواجهة المشهد المتغير للمخاطر، وهو ما أكدته دراسة Simić (٢٠٢٢) حول ضرورة مراعاة وعي العاملين.

بناءً على ما تقدم، تدعم النتائج بقوة أن أنشطة المراجعة الداخلية المتعلقة بالأمن السيبراني لها أثر ذو دلالة إحصائية ومعنوية على مخاطر الأمن السيبراني في البنوك اليمنية. هذه النتيجة تدحض الفرضيات الصفرية المطروحة وتُرسخ الدور الحيوي للمراجعة الداخلية كخط دفاع أول في بيئة المخاطر السيبرانية المتزايدة. الدراسة الحالية لا تؤكد فقط ما توصلت إليه دراسات سابقة مثل (Usman, et. al.، ٢٠٢٣) حول أهمية دور المراجعة الداخلية وخصائصها، بل تُقدم أدلة قوية في السياق اليمني، مما يُسهم في سد فجوة بحثية ويُعزز الفهم العالمي لدور المراجعة الداخلية في إدارة الأمن السيبراني.

النتائج:

بناءً على تحليل البيانات واختبار الفرضيات، تم التوصل إلى النتائج الآتية:

١. تُظهر النتائج أن المراجعة الداخلية في البنوك اليمنية غالباً ما تمارس انشطتها المتعلقة بتقييم مخاطر الأمن السيبراني والأنشطة التخطيطية. حيث يتضح تركيز عالٍ على التفاعل الاستباقي مع وظائف تكنولوجيا المعلومات وإدارة المخاطر، بالإضافة إلى تحديد الأصول الرقمية الأكثر قيمة للبنك. ومع ذلك، توجد فجوة واضحة في الدور الاستراتيجي للمراجعة الداخلية، تحديداً في تحديد متطلبات الضمان لمجلس الإدارة والإدارة العليا، كما يُلاحظ ضعف نسبي في تقييم درجة تأثير الحوادث السيبرانية المحتملة.

٢. فيما يتعلق بالأدوات الرقابية، تفحص المراجعة الداخلية هذه الأدوات أحياناً، مع تركيز أساسي على الضوابط الأمنية التقليدية مثل جدران الحماية. لكن، هناك نقطة ضعف حرجة في فحص أدوات الهندسة الاجتماعية، مما يشير إلى إغفال جانب حيوي من التهديدات.

٣. أما بالنسبة لتكرار مخاطر الأمن السيبراني، فيُصنف في البنوك اليمنية بـ "نادراً"، على الرغم من أن الإبلاغ عن نقاط الضعف في الرقابة الداخلية كان الأكثر تكراراً نسبياً. هذا التصور قد يعكس فعالية جزئية للضوابط، أو تحديات في رصد وكشف الحوادث أو الإبلاغ عنها.

٤. فيما يخص الأطر المعتمدة، تتبنى البنوك اليمنية مجموعة متنوعة من أطر إدارة الأمن السيبراني (غالباً أكثر من إطار واحد)، مع تفضيل ISO ٢٧٠٠١ و NIST و COBIT. لكن، يُثير القلق أن عدداً قليلاً من البنوك لا تستخدم أي إطار رسمي، مما يُشكل نقطة ضعف أمنية محتملة.

٥. الأهم من ذلك، أظهرت نتائج اختبار الفرضيات وجود أثر ذي دلالة إحصائية لأنشطة المراجعة الداخلية بأبعادها مجتمعة على مخاطر الأمن السيبراني. هذا يعني أن زيادة ممارسة المراجعة الداخلية لأنشطتها المتعلقة بتقييم المخاطر،

الانشطة التخطيطية، وفحص الأدوات الرقابية، تسهم بشكل مباشر في خفض مخاطر الأمن السيبراني.

التوصيات

بناءً على النتائج والمناقشة السابقة، تُقدم الدراسة التوصيات الآتية:

أولاً/ توصيات لمجالس الإدارة والإدارة العليا في البنوك اليمنية:

١. تعزيز الدور الاستراتيجي للمراجعة الداخلية من خلال إشراكها بشكل أعمق في وضع استراتيجيات الأمن السيبراني وتقييم المخاطر على مستوى الإدارة العليا ومجلس الإدارة، مع ضمان تقديم تقارير دورية وواضحة حول مدى نضج إدارة المخاطر السيبرانية.

٢. توفير الموارد الكافية والدعم اللازم لإدارات المراجعة الداخلية، بما في ذلك الميزانيات المخصصة للتدريب المتخصص على أحدث التهديدات والتقنيات، وتوفير الأدوات التقنية الحديثة اللازمة لتدقيق الأمن السيبراني.

ثانياً/ توصيات لإدارات المراجعة الداخلية في البنوك اليمنية:

١. الاستثمار في برامج تدريب مكثفة ومتخصصة للمراجعين الداخليين في مجال الأمن السيبراني، مع التركيز على أحدث التهديدات (مثل الهندسة الاجتماعية)، والمنهجيات المتقدمة لتقييم المخاطر (تقدير الاحتمالية والتأثير)، وتقنيات مراجعة الأدوات الأمنية المتطورة (مثل أنظمة كشف التسلل، أدوات التشفير)

٢. توسيع نطاق المراجعة ليشمل بشكل فعال مخاطر الهندسة الاجتماعية، من خلال تقييم برامج التوعية والتدريب للموظفين، واختبار مدى وعيهم بهذه التهديدات، لتعزيز خط الدفاع البشري.

٣. تعزيز التعاون والتنسيق الفعال بين المراجعة الداخلية وإدارة أمن المعلومات (أو قسم تكنولوجيا المعلومات) لضمان فهم شامل للمخاطر، وتبادل المعلومات بانتظام حول نقاط الضعف والحوادث الأمنية المكتشفة.

٤. تطبيق نهج المراجعة القائم على المخاطر بشكل أعمق، وتحديد الأصول الحرجة بدقة أكبر ووضع خطط مراجعة تستهدف الثغرات الأكثر حساسية وذات الأثر المحتمل الأكبر.

ثالثاً/ توصيات للجهات الرقابية (مثل البنك المركزي اليمني)

١. إصدار توجيهات ومعايير واضحة تلزم البنوك بتعزيز دور المراجعة الداخلية في الأمن السيبراني، وتحديد الحد الأدنى من متطلبات الخبرة والتدريب للمراجعين في هذا المجال.

٢. تشجيع البنوك على تبني الأطر العالمية للأمن السيبراني مثل NIST و ISO ٢٧٠٠١، ودمجها في ممارسات المراجعة الداخلية لضمان أفضل الممارسات.

٣.١٧ دراسات مستقبلية مقترحة:

١. إجراء دراسات مستقبلية تستكشف العوامل النوعية التي تؤثر على قدرات المراجعين الداخليين في مجال الأمن السيبراني، مثل مدى توفر برامج التدريب المتخصصة، والشهادات المهنية ذات الصلة، والموارد التقنية المتاحة لهم.

٢. التركيز على دراسة العلاقة بين ثقافة الأمن السيبراني التنظيمية وفعالية المراجعة الداخلية، مع الأخذ في الاعتبار أن الجانب البشري يُمثل تحدياً كبيراً في إدارة المخاطر السيبرانية.

مصادر الدراسة ومراجعها:

أولا/ المراجع العربية

١. أميرهم، جيهان عادل ناجى. (٢٠٢٢). أثر جودة المراجعة الداخلية في الحد من مخاطر الامن السيبراني وانعكاساته على ترشيد قرارات المستثمرين (دراسة ميدانية). **مجلة البحوث المالية والتجارية**، 23(3)، 325-377.

٢. رشوان، عبد الرحمن محمد سليمان، وقاسم، زينب عبد الحفيظ أحمد. (٢٠٢٢). **أثر إدارة مخاطر الأمن السيبراني على دعم الاستقلال والاستقلال الشمولي المالي في البنوك**. في المؤتمر العلمي الدولي الأول بعنوان "**أثر الأمن السيبراني على الأمن الوطني**"، ٢٠- ٢١ كانون الأول، جامعة عمان العربية، الأردن.

٣. الزيود، محمود سليمان سعود. (٢٠٢١). **أثر المراجعة الداخلية في الحد من المخاطر السيبرانية في البنوك التجارية الأردنية** (رسالة ماجستير). جامعة آل البيت، كلية الاقتصاد والعلوم الإدارية، الأردن.

٤. زيتون، محمد خميس جمعة خطاب، (يناير ٢٠٢١)، **أثر استخدام وظيفة المراجعة الداخلية كحقل للتدريب على الإدارة ودورها الاستشاري في مجال إدارة المخاطر على قرار اعتماد مراقب الحسابات عليها:** دراسة تجريبية. المجلة **العلمية للدراسات والبحوث المالية والتجارية**. جامعة دمياط. مصر. المجلد الثاني- العدد الأول–الجزء الثاني– ص ١ ــ ٦٨.

٥. شحاته، شحاته السيد. (٢٠٢٢). **نحو دور فعال للمراجع الداخلي في إدارة مخاطر الأمن السيبراني في الشركات المقيدة بالبورصة المصرية**. المجلة العلمية للدراسات والبحوث المالية والإدارية، 13(2)، 26-37.

٦. الغزي، غزي علي محمد، (٢٠٢٥) " **الإطار النظري والعملي للمراجعة واتجاهاتها المعاصرة**"، ط١، الأمين للنشر والتوزيع: صنعاء.

٧. منظمة سام للحقوق والحريات. (٢٠٢٢). الأمن الرقمي في اليمن: الواقع والمهددات. تم الاسترجاع من www.samrl.org.

٨. النجار، دعاء محمد حامد. (٢٠١٣). **إطار مقترح لتحقيق التكامل بين المراجعة الداخلية على أساس الخطر وأدوات إدارة التكلفة لدعم عملية اتخاذ القرارات الاستراتيجية** (رسالة دكتوراه). كلية التجارة، جامعة طنطا، مصر.

ثانيا/ المراجع الأجنبية

Accenture Security. (2017). *Accenture Building Confidence Facing Cybersecurity Conundrum*. Retrieved from https://www.accenture.com/t20170406T052041Z__w__/us-en/_acnmedia/PDF-35/Accenture-Building-Confidence-Facing-Cybersecurity-Conundrum-Transcript.pdf#zoom=50.

Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, ٤(1),tyy006.

AICPA. (2017). Description Criteria for Management's Description of the Entity's Cybersecurity Risk Management Program. American Institute of Certified Public Accountants.

Al-Fahim, N. H., JUSOH, W. J. W., & ABIDEEN, A. (2016). An examination factors influencing the intention to adopt internet banking among SMEs in Yemen: Using an extension of the technology acceptance model (TAM). *The Journal of Internet Banking and Commerce*.

Al-Khulaidi, A. A., Al-Ashwal, M. M., Nasser, A. A., & Al-Anesi, N. K. (2023). Information Security Risk Management in Yemeni Banks: An Evaluation of Current Practices. *International Journal of Engineering Trends and Technology* 71 (4) 225-237.

AL-KHULAIDI, A. A., NASSER, A. A., ALANESI, N. K., HAZAA, M. A., & ALJOBER, M. (2022). Information Security Governance: An Exploration Study of Yemeni Banks' Information Security Management Systems. *The Seybold Report Journal*.

Basel Committee on Banking Supervision. (2018). *Supervision Publishes Report on Cyber-Resilience Practices.* Retrieved from. https://www.bis.org/bcbs/publ/d454.htm

Center for Audit Quality. (2018). *Cybersecurity Risk Management Oversight: A Tool for Board Members*. Retrieved from https://www.thecaq.org/wp-content/uploads/2019/03/caq_cybersecurity_risk_management_oversight_tool_2018-04.pdf.

Crisanto, J. C., Ehrentraud, J., Fabian, M., & Monteil, A. (2024). Regulating AI in the financial sector: recent developments and main challenges. *FSI insights*. Retrieved from https://www.dirittobancario.it/wp-content/uploads/2025/01/Documento-di-ricerca-BIS-dicembre-2024-n.-63.pdf.

Darmawati, D. (2022). Pengaruh auditor internal dan kebijakan manajemen terhadap efektivitas keamanan siber. *Jurnal Ekonomi Trisakti*, 2(2), 515-528 .

Doerr, S., Gambacorta, L., Leach, T., Legros, B., & Whyte, D. (2022). Cyber risk in central banking. BIS Working Papers.

Efijemue, O., Obunadike, C., Taiwo, E., Kizor, S., Olisah, S., Odooh, C., & Ejimofor, I. (2023). Cybersecurity Strategies for Safeguarding Customers Data and Preventing Financial Fraud in the United States Financial Sectors. *International Journal of Soft Computing*,14(3), 10-21

Eisenach, T. M., Kovner, A., & Lee, M. J. (2022). Cyber risk and the US financial system: A pre-mortem analysis. *Journal of Financial Economics*, 145(3), 802-826 .

European Confederation of Institutes of Internal Auditors. (2020). *Risk in focus 2023: more risky, uncertain, and volatile times ahead*. Retrieved from https://www.eciia.eu/2022/09/risk-in-focus-2023-more-risky-uncertain-and-volatile-times-ahead./

Friedman, M., Akaaboune, O., & Margolis, D. M, (2013), *Internal audit: A new lens for cost management, Journal of Corporate Accounting & Finance*, 24.(٤)

Gaidosch, T., Adelmann, F., Morozova, A., & Wilson, C. (2019). Cybersecurity Risk Supervision. *Journal Issue*, 15, 88-133.

Gavėnaitė-Sirvydienė, J. (2024). *Development of cyber security assessment tool for financial institutions* (Doctoral dissertation). Vilnius Gediminas Technical University.

Goh, J., Kang, M. H., Koh, Z. X., Lim, J. W., Ng, C. W., Sher, G., & Yao, C. (2020). Cyber risk surveillance: A case study of Singapore. *International Monetary Fund*.

Gyun No, W., & Vasarhelyi, M. A. (2017). Cybersecurity and continuous assurance. *Journal of Emerging Technologies in Accounting, 14, (1), 1-12.*

Hasanefendioglu Bulent. (2018). *Cyber Security Management and Control Framework With 101 Questions.* Retrieved from https://technologydevelopmentgroup.net./

Hoffmann, R., Napiórkowski, J., Protasowicki, T., & Stanik, J. (2020). Risk based approach in scope of cybersecurity threats and requirements. *Procedia Manufacturing, 44*, 655-662.

IIA. (2020). *Assessing Cybersecurity Risk Roles of the Three Lines of Defense*. Retrieved from: https://www.iia.nl/SiteFiles/vakpub/GTAG%20Assessing%20Cybersecurity%20Risk.pdf

IIA's Audit Executive Center. (2019). *Cybersecurity and the Internal Audit Function*. Retrieved from: https://www.theiia.org/en/resources/technology/cybersecurity/

Institute of Internal Auditors (IIA). (2018). *The future of cybersecurity in internal audit: A joint research report by the internal audit foundation and crowe horwath*. Retrieved from https://bookstore.theiia.org/the-future-of-cybersecurity-in-internal-audit.

Institute of Internal Auditors (IIA). (2020). *The IIA's Three Lines Model: An update of the Three Lines of Defense.* Retrieved from https://global.theiia.org/about/about-internal-auditing/Public%20Documents/Three-Lines-Model-Updated.pdf.

Institute of Internal Auditors (IIA). (2023). *Internal Audit Leaders Identify Technology as a Primary Driver of Risk in New IIA Survey*. Retrieved from

https://www.theiia.org/en/content/communications/press-releases/2023/march/internal-audit-leaders-identify-technology-as-a-primary-driver-of-risk-in-new-iia-survey./

Islam, M. S., Farah, N., & Stafford, T. F. (2018). Factors associated with security/cybersecurity audit by internal audit function: An international study. *Managerial Auditing Journal*٣٣ ،(4).٤٠٩-٣٧٧ ،

Jarison, E., Morris, M., & Wilkinson, T. (2018). The Internal Audit Function's Role in Cybersecurity. *The Journal of Internal Audit*, 33(4), 1-20.

Krykliy, O., & Pavlenko, L. (2019). Internal Audit as a Preventive Component in the Bank's Cybersecurity System. *Accounting and Finance* ،(2).١٣٣-١٢٤.

Kshetri, N. (2013). Cybercrime and Cybersecurity in the Middle East and North African Economies. In *Cybercrime and Cybersecurity in the Global South* (pp. 119-134). Palgrave Macmillan.

Lehmann, D., & Thor, M. (2020). The Next Generation of Internal Audit: Harnessing Value from Innovation and Transformation. *The CPA Journal*, 90(1), 60-61 .

Li, H. (2017). *Three essays on cybersecurity-related issues* (Doctoral dissertation). Rutgers University-Graduate School-Newark.

Masuch, K., Greve, M., Trang, S., & Kolbe, L. M. (2022). Apologize or justify? Examining the impact of data breach response actions on stock value of affected companies? *Computers & Security*, 112, 102-502.

Möller, D. P. F., & Haas, R. E. (2019). Automotive Cybersecurity. In Guide to *Automotive Connectivity and Cybersecurity* (p. 377). Springer.

Morshed, A., & Khrais, L. T. (2025). Cybersecurity in Digital Accounting Systems: Challenges and Solutions in the Arab Gulf Region. *Journal of Risk and Financial Management*, 18(1), 41. https://doi.org/10.3390/jrfm18010041

Nasser, A. A., Al Ansi, N. K. A., & Al Sharabi, N. A. (2020). On The Standardization Practices of the Information Security Operations in

Banking Sector: Evidence from Yemen. Int. *J. Sci. Res. in Computer Science and Engineering, 8(6), 8-18.*

National Institute of Standards and Technology (NIST). (2013*). Glossary of key information security terms (NISTIR 7298*, Rev. 2). Retrieved from http://csrc.nist.gov/publications.

National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Oyewole, A. T., Okoye, C. C., Ofodile, O. C., & Ugochukwu, C. E. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies applicatio. *World Journal of Advanced Research and Reviews*٢١ ،(3).٦٤٣-٦٢٥ ،

ÖZTÜRK, M. S. (2018). Cyber Security Audit in Institutions. The Turkish. *Journal of Internal Auditing*, 13(38), 213-228.

Peihani, M. (2022). Regulation of Cyber Risk in the Banking System: A Canadian Case Study. *Journal of Financial Regulation*, 8(2), 139-161.

Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on the cyber security. *International Journal of Scientific Research and Management*٩ ،(12).٧١٠-٦٦٩ ،

PWC. (2018). *Cybersecurity: The Internal Audit Perspective*. Retrieved from: https://www.pwc.com/gx/en/services/audit-assurance/internal-audit/publications/assets/pdf/pwc-internal-audit-cybersecurity-perspective.pdf

PwC. (2018). *Moving at the speed of innovation: The foundational tools and talents of technology-enabled Internal Audit: 2018 State of the Internal Audit Profession Study*. Retrieved from https://www.pwc.com/sg/en/publications/assets/state-of-the-internal-audit-2018.pdf.

Rosati, P., Gogolin, F., & Lynn, T. (2020). Cyber-Security Incidents and Audit Quality. *European Accounting Review, 1-28.*

Shamsuddin, A., Adam, M. A., Adnan, S. A., & Yasin, Y. M. (2020). *The Effectiveness of Internal Audit Functions in Managing Cybersecurity in Malaysia's Banking Institutions*.

Simić, N. (2022). *The Internal Auditor's Role in Cybersecurity Governance: A qualitative study about the internal auditor's influence on the people factor of cybersecurity*.

Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cyber security audit,. *International Journal of Accounting Information Systems*, 100548

The Institute of Internal Auditors (IIA). (2017). *The Internal Audit Role in Cybersecurity*. Retrieved from: https://www.iia.nl/SiteFiles/vakpub/GTAG%20Assessing%20Cybersecurity%20Risk.pdf

Tosun, O. K. (2021). Cyber-attacks and stock market activity. *International Review of Financial Analysis*.١٥-١ ،٧٦ ،

Tušek, B., Sačer, I. M., & Halar, P. (2018). The Internal Audit Function as an Effective Tool for Increasing Business Success in Digital Economy Era. In An Enterprise Odyssey, *International Conference Proceedings* (pp. 79-80). University of Zagreb.

Ursillo, S., & Arnold, C. (2019). *Cyber security Is Critical for all Organizations Large and Small. International Federation of Accountants (IFAC)*. Retrieved from https://www.ifac.org/knowledge-gateway/preparing-future-ready-professionals/discussion/cybersecurity-critical-all.

Usman, A., Che-Ahmad, A., & Abdulmalik, S. O. (2023). The role of internal auditors characteristics in cyber security risk assessment in Financial-Based business organizations: a conceptual review. *International Journal of Professional Business Review* ، ٨(8) ، e02922.

World Bank. (2018). *Cyber security, Cyber Risk and Financial Sector Regulation and Supervision*. https://www.worldbank.org/en/topic/financialsector/brief/cybersecurity-cyber-risk-and-financial-sector-regulation-and-supervision.