دور لجان المراجعة كأحد آليات الحوكمة لمواجهة مخاطر الهجمات السيبرانية في البنوك المصرية: دراسة ميدانية

إعداد

د. عماد محمد صدقي

مدرس المحاسبة

المعهد العالي للألسن

للسياحة والفنادق والحاسب الآلي

مدينة نصر القاهرة

emadsadky33@gmail.com

مجلة البحوث التجارية ـ كلية التجارة جامعة الزقازيق

المجلد الخامس والأربعين ـ العدد الرابع أكتوبر 2023

رابط المجلة: https://zcom.journals.ekb.eg/

المستخلص:

تهدف الدراسة إلى تعزيز دور لجان المراجعة كأحد آليات الحوكمة لمواجهة مخاطر الأمن السيبراني في البنوك المصرية. وفي سبيل تحقيق أهداف الدراسة واختبار فروضها قام الباحث بتصميم دراسة نظرية وأخري ميدانية حيث اشتملت الدراسة النظرية على ثلاثة محاور تناول الباحث فيها كل من الإطار العام للدراسة ومخاطر الأمن السيبراني وطرق مواجهتها بالبنوك المصرية والدراسات السابقة والمتعلقة بمشكلة البحث.

ومن أجل اختبار صحة فروض الدراسة قام الباحث بتصميم دراسة ميدانية تناولها في المحور الرابع حيث تناول الباحث في هذا المحور قائمة الإستقصاء والتي تكونت من ثلاثة محاور رئيسية، وبلغ حجم عينة الدراسة (388) رد تم اختيارهم بصورة عشوائية من مجتمع الدراسة، وتم إجراء الاختبارات والتحليلات الإحصائية لتحقيق ذلك.

وتوصلت الدراسة النظرية إلى وجود زيادة مستمرة في مخاطر الأمن السيبراني، وتسببت الهجمات السيبرانية في أضرار وخسائر كبيرة لمنظمات الأعمال والاقتصاد القومي؛ بالإضافة إلى ان الأمن السيبراني يهدف إلى المساعدة على حماية أصول المنظمات ومواردها من النواحي التنظيمية والبشرية والمالية والتقنية والمعلوماتية، ويسمح لها بمواصلة مهماتها. وهدفه الأسمى هو أن يضمن عدم تضررها ضرراً دائماً، ويتمثل ذلك في تقليل احتمالات سوء الأداء أو ظهور أي تهديد والحد من الأضرار الناجمة عنها، وضمان رجوع العمليات العادية إلى حالتها السابقة خلال إطار زمني مقبول وبتكلفة مقبولة في أعقاب وقوع حادث أمني.

في حين توصلت الدراسة الميدانية إلى رفض كافة فروض الدراسة، حيث أوضحت نتائج التحليل الإحصائي وجود فروق معنوية ذات دلالة إحصائية بين متوسطات الرتب لعينة الدراسة وفقاً لمتغير جهة العمل ولصالح العاملين بقطاع البنوك بشأن آرائهم حول ما يلي: أولاً مخاطر الأمن السيبراني وطرق مواجهتها، ثانياً حول دور خصائص تشكيل لجان المراجعة في تعزيز قدرة البنوك المصرية على مواجهة مخاطر الأمن السيبراني وثالثاً حول دور آليات عمل لجان المراجعة في تعزيز قدرة البنوك المصرية على مواجهة مخاطر الأمن السيبراني.

وفي النهاية، اقترح الباحث مجموعة من التوصيات منها زيادة الاهتمام بتوعية العاملين بقطاع البنوك بأهمية الأمن السيبراني حتى يتسنى لهم مواجهة التحديات والمخاطر الناتجة عن بيئة تكنولوجيا المعلومات، وإعداد برامج توعية مجتمعية للمواطنين للتعرف على أهمية الأمن السيبراني، بالإضافة إلى تطوير البنية التحتية السيبرانية داخل المؤسسات المصرفية للحد من الاختراق والتجسس والقرصنة الالكترونية، وضرورة إنشاء إدارة للتطبيقات الإلكترونية لمراجعة كل جديد واختباره قبل إطلاقه بالسوق، مع ضرورة تقييم أنظمة المؤسسات المصرفية بشكل دوري ووضع خطط لعلاج الثغرات الموجودة بها ومتابعة تنفيذها

المصطلحات الأساسية: لجان المراجعة، الأمن السيبراني، مخاطر الأمن السيبراني، طرق مواجهة مخاطر الأمن السيبراني.

المحور الأول: الإطار العام للدراسة

1/1مقدمة

سلطت الانهيارات المؤسسية السابقة والتي مثلتها شركةأنرونوورلد كوم وزيروكس الضوء على آليات الحوكمة، وقد حاولت أغلب المؤسسات تحسين حوكمة الشركات لحماية ثروة المساهمين، كما أُعتبر سوء الإدارة واحداً من الأسباب الرئيسية للإنخفاض الهائل في قيمة ثروة المساهمين، وطورت العديد من الدول عدة آليات من أجل حوكمة الشركات بطريقة مناسبة، وتعتبر لجان المراجعة هي واحدة من هذه الآليات التي تستخدم لضمان إدارة الشركات بشكل صحيح (Lemmon andLins, 2003).

وتمثل الجريمة الالكترونية مخاطر متطورة وسريعة التغيير، نتيجة قيام المتسللين بإنشاء برامج جديدة لإرسال رسائل غير مرغوب فيها كل يوم، وبالتالي فهناك حاجة للجنة المراجعة أن تبحث عن تحديثات روتينية للمخاطر المتزايدة للجرائم الالكترونية، وهو ما يعني أن تكون لجنة المراجعة على إطلاع دائم بالمخاطر، وأن تكون استراتيجية مكافحة الجرائم الالكترونية جزءً لا يتجزأ من استراتيجية الأمن السيبراني (Ojekaet al., 2017).

لجنة المراجعة لديها واجبات تجاه إدارة المخاطر لأصحاب المصالح، وبسبب تعقيد العالم السيبراني وتحقيق مصلحة البنوك هناك حاجة أن تكون لجنة المراجعة مستقلة، لزيادة درجة الرقابة

وضمان تصرف أعضائها بموضوعية في تقييم ممارسات الرقابة الداخلية واعداد التقارير لضمان استمرارية الشركة وقت الأزمات، وكذلك تمتعها بالخبرة التكنولوجية لتكون قادرة على مواكبة الاتجاه المتنامي للمجتمع العالمي، وكذلك امتلاكها للمعرفة المحاسبية من أجل تحقيق الفهم المتعمق للآثار المالية للجرائم الإلكترونية على أداء البنوك وسعر السهم، وسمعة البنك، وكذلك الحاجة الملحة لفهم المحتويات المالية وغير المالية للتقارير المالية حتى يمكن إبقاء اصحاب المصالح على اطلاع دائم بكل ما هو مالي وغير مالي. وأخيراً أن تمتلك لجنة المراجعة الحجم المناسب حتى تستطيع تحقيق الدور الرقابي الأساسي في البنك واكتشاف المشاكل في التقارير المالية (Ojekaet al., 2017).

الأمن السيبراني في الوقت الحاضر يعتبر موضوعاً مهماً داخل المنظمات فمنذ حوالي 25 عاماً، تطورت أصول الشركات من الأصول المادية إلى الأصول الرقمية (Clinton, 2017)، وامتلاك البنوك قدراً كبيراً من المعلومات السرية حول عملائها ووضعهم المالي، والتي يجب حفظها في مكان آمن بعيداً عن الدخلاء، وتستخدم جميع المؤسسات في العالم الانترنت لتنفيذ أعمالها والترويج والبيع والدعاية واكتشاف أسواق جديدة والمشترين والعاملين والتواصل مع العملاء والموردين، وتنفيذ المعاملات المالية، فالإنترنت يولد بوابات تجارية وأرباح ضخمة، ومع ذلك، فهو ينطوي على مخاطر عديدة، تتمثل في الهجمات اليومية على أنظمة تكنولوجيا المعلومات كالقرصنة أو الوصول إلى الحسابات وسرقة المعلومات والأموال وتعطيل العمليات التجارية، وبالتالي تظهر الحاجة لطريقة شاملة لإدارة مخاطر الأمن السيبراني (Al-Alawi and Al-Bassam, 2020). وبناءً على ما سبق تتناول هذه الدراسة تعزيز دور لجان المراجعة- من حيث خصائص تشكيلهاوآلياتها- كأحد آليات الحوكمة في مواجهة مخاطر الأمن السيبراني بالبنوك المصرية.

2/1 مشكلة الدراسة

يشهد قطاع الخدمات المالية هجمات سيبرانية تفوق القطاعات الأخرى بنسبة 65% وفق تقديرات البنك الدولي، وقد تصل التكلفة المترتبة على الهجمات السيبرانية في قطاع الخدمات المالية إلى ما يقدر بنحو 270 مليار دولار إلى 350 مليار دولار سنوياً حال اتساع نطاق انتشارها، وذلك وفقاً لتقديرات صندوق النقد الدولي، الأمر الذي دفع البنوك المركزية بالدول العربية إلى تشديد التعليمات الرقابية على البنوك لكي تصدر التعليمات التي تعزز قدرتها لمواجهة الهجمات السيبرانية (البغدادي،2021)، إن

مواجهة المخاطر السيبرانية ليست بالأمر السهل ويتزايد تأثير هذه المخاطر بمرور الوقت مع زيادة الاعتماد على التكنولوجيا، لذلك أصبح من الضروري الكشف عن هذا الخطر الكبير لأنه يؤدي لفقدان المعلومات وفقدان الثقة، وبالتالي يؤدي إلى الإفلاس (Putte andVerhelst,2014)، ولذلك فقد دعت الحاجة إلى تحديد تأثير خصائص تشكيل لجان المراجعةوآليات عملهافي مواجهة مخاطر الأمن السيبراني بالبنوك المصرية

وبناءً على ما سبق تتناول هذه الدراسة تعزيز دور لجان المراجعة كأحد آليات الحوكمة لمواجهة مخاطر الأمن السيبراني في البنوك المصرية؛ وبالتالي تتمثل مشكلة الدراسة الحالية في الإجابة عن السؤال الرئيسي التالي: ماهية التعزيزات اللازمة للجان المراجعة والتي تؤدي إلى مواجهة مخاطر الأمن السيبراني والحد منها في البنوك المصرية؟

وينبثق عن هذا التساؤل مجموعة من التساؤلات الفرعية هي:

أ. هل هناك إدراك ووعي كافي لعينة الدراسة بمخاطر الأمن السيبراني وطرق مواجهتها بالبنوك المصرية؟

ب. ما مدى التوافق لدى عينة الدراسة حول دور خصائص تشكيل لجان المراجعة في مواجهة مخاطر الأمن السيبراني بالبنوك المصرية؟

ج. ما مدى التوافق لدى عينة الدراسة حول دور آليات عمل لجان المراجعة في مواجهة مخاطر الأمن السيبراني بالبنوك المصرية؟

3/1 أهداف الدراسة

تستهدف الدراسة التعرف على التعزيزات اللازمة للجان المراجعة والتي تؤدي إلى مواجهة مخاطر الأمن السيبراني والحد منها في البنوك المصرية، وذلك من خلال تحقيق مجموعة من الأهداف الفرعية تتمثل في:

- التعرف على مخاطر الأمن السيبراني وطرق مواجهتها بالبنوك المصرية.
- بيان أهمية خصائص تشكيل لجان المراجعة في مواجهة مخاطر الأمن السيبراني بالبنوك المصرية.

- بيان أهمية آليات عمل لجان المراجعة في مواجهة مخاطر الأمن السيبراني بالبنوك المصرية.
- تقديم مجموعة من التوصيات والمقترحات بناءً على نتائج الدراسة تساعد متخذي القرار في البنوك المصرية للاسترشاد بها في مواجهة مخاطر الأمن السيبراني.

4/1 أهمية الدراسة

تنبع أهمية الدراسة من أهمية المشكلة التي تتناولها الدراسة والتي تتمثل في دراسة التعزيزات اللازمة للجان المراجعة والتي تؤدي إلى مواجهة مخاطر الأمن السيبراني والحد منها في البنوك المصرية، وذلك على النحو التالي:

- **الأهمية العلمية للدراسة** تتمثل في أنهعلى الرغم من اهتمام الدراسات بموضوع إدارة مخاطر الأمن السيبراني، إلا أن هذه الدراسات لم تربط بشكل مباشر بين خصائص تشكيل لجان المراجعة وآليات عملها ومواجهة مخاطر الأمن السيبراني في البنوك المصرية، ولذلك ظهرت الحاجة الملحة لتضييق الفجوة البحثية في ذلك الصدد.
- **الأهمية العملية للدراسة** تتمثل في توفير أدلة تجريبية من البيئة المصرية تساعد في التعرف على دور خصائصتشكيل لجان المراجعة وآلياتها في مواجهة مخاطر الأمن السيبراني في البنوك المصرية، وتقييم أداء لجان المراجعة في مواجهة هذه المخاطر.

5/1 منهج الدراسة

يعتمد الباحث على الجمع بين المنهج الاستقرائي والمنهج الاستنباطي في إعداد الاطار النظري للبحث في ضوء تحليل وتقييم الدراسات السابقة في مجال لجان المراجعة ومخاطر الأمن السيبراني ودور آليات وخصائص تشكيل لجان المراجعة في مواجهة مخاطر الأمن السيبراني، وكذلك من خلال الاعتماد على قواعد البيانات والمواقع المتخصصة وعلى ما صدر من المنظمات المهنية والمراجع والدوريات العلمية المتخصصة في مجال المحاسبة ذات الصلة بموضع البحث، والتي تمثل المصادر الثانوية لجمع البيانات، وتنتهي الدراسة النظرية بصياغة الفروض المطلوب اختبارها، أما الدراسة الميدانية فتهتم باختبار الفروض باستخدام الاختبارات الإحصائية المناسبة لتحليل ردود فعل المستقصي منهم حول تساؤلات قائمة الإستقصاء المصممة لجمع البيانات من عينة الدراسة.

6/1 تنظيم الدراسة

لتحقيق أهداف الدراسة تم تقسيمها إلى المحاور التالية:

المحور الأول: الإطار العام للدراسة.

المحور الثاني: تحليل العلاقة بين لجان المراجعة ومواجهة مخاطر الأمن السيبراني.

المحور الثالث: مراجعة أدبيات الدراسة واشتقاق فروض الدراسة.

المحور الرابع: الدراسة الميدانية.

المحور الخامس: النتائج والتوصياتومقترحات الدراسات المستقبلية.

المحور الثاني: تحليل العلاقة بين لجان المراجعة ومواجهة مخاطر الأمن السيبراني

1/2 مخاطر الأمن السيبراني:

يشير الأمن السيبراني إلى حماية الأصول الرقمية من المخاطر الموجودة نتيجة استخدام تكنولوجيا المعلومات والاتصالات التي تشكل الفضاء السيبراني، وقد عرف إطار NISTالأمن السيبراني بأنه عملية حماية المعلومات من خلال منع واكتشاف والرد على الهجمات السيبرانية، كما تم تعريف حادثة الأمن السيبراني بأنه الحادثة التي يكون لها تأثير على المؤسسة مما يستدعي الحاجة للرد والتعافي، وتتعلق حوادث الأمن السيبراني باختراق البيانات وفشل نظم المعلومات وقد يترتب عليها خسائر ضخمة في بيانات المؤسسة وممتلكاتها، وأضراراً جسيمة بسمعتها وبنيتها الأساسية (محروس، 2022).

وهناك أنواع مختلفة من الهجمات السائدة في الأمن السيبراني والتي يمكن تصنيفها بناءً على نية المهاجمين والمعلومات المطلوبة للمتطفلين، البرامج الضارة التي يتم تنشيطها عندما ينقر المستخدم على رابط غير مصرح به أو بريد الكتروني مرفق، التصيد وهو التهديد الالكتروني الشائع وهو عملية إرسال اتصالات احتيالية من مصدر مصرح به عبر البريد الالكتروني لسرقة المعلومات الحساسة، رجل في الوسط Maninthe middle وهو هجوم مثير للاهتمام حيث سيهاجم أحد الدخلاء من خلال الشبكة، لذلك سيرسل المرسل الرسالة دون أن يعرف المخترق في الوسط يتلقى المعلومات، هجوم Zero day

هو تهديد أمني غير معروف في تطبيق البرامج الذي لم يتم إصدار التصحيح له أو لم يكن مطوري البرامج على دراية بالهجوم، وهو أحد أشهر هجمات (DOS) حيث يغمر النظام والخادم بحركة المرور لاستغلال الموارد المتاحة وعرض النطاق الترددي، هجوم لغة الاستعلام الهيكلية (SQL) بإدراج التعليمات البرمجية الضارة في الخادم ويجبره على الكشف عن معلومات حساسة من قاعدة البيانات(Alazabet al.,2021).

ويمكن تصنيف تدابير الأمن السيبراني إلى خمسة أنواع رئيسية هي: التدابير التي تركز على أمن التطبيقات، وأمن الشبكة، والأمن التشغيلي، وأمن السحابة، وتدريب المستخدمين وأمن المعلومات، وقد تتضمن بعض الإجراءات بروتوكولات كلمة المرور والمصادقة، وجدران الحماية ومنهجيات تشفير البيانات والماسحات الضوئية للبرامج الضارة واستخدام برامج مكافحة الفيروسات (KrishnasamyandVenkatachalam,2021).

تدور الأهداف الرئيسية للأمن السيبراني حول ضمان السرية أي الحفاظ على البيانات آمنة، والنزاهة أي الحفاظ على البيانات نظيفة، والتوافر بمعنى الحفاظ على إمكانية الوصول للبيانات بالقدر والمكان والشخص المناسب (Akintoyeet al., 2022).

تواجه البنوك العديد من مخاطر الجرائم الالكترونية، إلا أنه يمكن التقليل من تلك المخاطر ببضع خطوات، تتمثل في: رفع مستوى الوعي بالمخاطر السيبرانية، تقييد النسخ الاحتياطي للبيانات والوصول إليه، الإستفادة من الأنظمة التي تمنع اختراق البيانات، تحديد استراتيجيات إدارة المخاطر السيبرانية، والحصول على تأمين الكتروني (Randazzo et al., 2005)، وهناك ثلاث سمات رئيسية لممارسة دفاع الكتروني فعال ومتوازن: أن تكون آمناً، وأن تكون مدركاً، ومقاوماً: (Yıldırım,2019)

- **أن تكون آمناً**: من خلال التركيز على توفير الحماية ضد المخاطر، أي تتضمن المخاطر الأصول الأكثر قيمة للأعمال من وجهة نظر كل من الشركة ومنافسيها.
- **أن تكون مدركاً**: من خلال زيادة الوعي في كل مستوى من مستويات المنظمة وتطوير القدرة على اكتشاف أي سلوك محفوف بالمخاطر مرتبط بالأصول المهمة قبل حدوث مثل هذا السلوك.

- **أن تكون مقاوماً**: بمعنى القدرة على الاستجابة بسرعة للضرر، لضمان عدم تأثيره على العمليات الأخرى، والقدرة على استخدام الادوات الضرورية والمتعددة من أجل تقليل الأضرار التي تنطوي على تكاليف مباشرة، وفقدان عبء العمل والإضرار بالسمعة وفقدان قيمة العلامة التجارية.

ولضمان وظائف الأمن السيبراني، تم تطوير إطار عمل من قبل المعهد الوطني للمعايير والتكنولوجيا (NIST) ووكالة الاتحاد الأوربي لأمن الشبكات والمعلومات (ENISA) لإنشاء خمس وظائف رئيسية حاسمة لحماية الأصول الرقمية وتشمل الأنشطة التالية:-(Al-Alawi and Al-Bassam, 2020)

- **التحديد:** استخدام الفهم التنظيمي لتقليل المخاطر على الأنظمة والأصول والبيانات والقدرات.
- **الحماية:** ضمانات التصميم للحد من تأثير الأحداث المحتملة على الخدمات والبنية التحتية الحيوية.
- **الكشف:** تنفيذ الأنشطة لتحديد وقوع حدث خطر الأمن السيبراني.
- **الاستجابة**: اتخاذ الإجراءات المناسبة بعد التعرف على الحدث الأمني.
- **التعافي**: التخطيط للقدرة على الصمود وإصلاح القدرات والخدمات المعرضة للخطر في الوقت المناسب.

ولرفع درجة الوعي الأمني بالمؤسسات والشركات يجب وضع برنامج تدريبي داخلي متخصص للكوادر الفنية القائمة على إدارة الأنظمة التكنولوجية لرفع درجة الوعي بأمن المعلومات، والتأكد من جاهزيتها لمجابهة الهندسة الاجتماعية وكيفية تجنب التصيّد الاحتيالي، وذلك بصفة دورية لمواكبة كل جديد في هذا المجال سريع التغيّر، يجب تثقيف وتدريب جميع الموظفين وإرسال رسائل توعوية دورية للعملاء في الوقت ذاته لرفع درجة الوعي لديهم تجاه محاولات الاختراق والاحتيال الإلكتروني (https://cbe.org.eg). ويجب على الإدارة أن تركز على تثقيف الموظفين من خلال التدريبات المتعلقة بالتعريف بالتهديدات السيبرانية والمضاعفات المرتبطة بها، واستخدام المحاكاة السيبرانية كأحد التدابير الفعالة لتسهيل استجابة الكترونية شاملة وفعالة، حيث تتطلب محاكاة الحدث السيبراني انشاء هجوم يستجيب له الموظفون من خلال العمل باستخدام اجراءات الاستجابة للحوادث، حيث يوفر نظرة ثاقبة لنقاط الضعف في البرنامج والتي تحتاج إلى تعزيز، والسماح لفريق عمل تكنولوجيا المعلومات والإدارة والموظفين الآخرين بفهم دور كل واحد منهم بشكل فردي في حالة حدوث هجوم الكتروني

ناجح، حيث قد يؤدي فهم دورهم إلى تقليل الضرر الناجم عن الهجوم من خلال استجابات أكثر كفاءة وتثقيفاً لتخفيف التهديدات(Johnson, 2016).

وقد خصص البنك المركزي المصري عبر مركز الاستجابة لطوارئ الحاسب الآلي للقطاع المالي (EG-FinCIRT) العديد من الوسائل والآليات التي يمكن من خلالها الإبلاغ عن حوادث الأمن السيبراني، والتصيّد أو الاحتيال الإلكتروني، أو أي صورة أخرى من صور الهجمات الإلكترونية التي تشكل تهديدًا لاستقرار المنظومة الأمنية لأي مؤسسة أو كيان داخل القطاع المالي والمصرفي، وذلك بهدف المساعدة في الوقاية والتصدي للمخاطر والحوادث الأمنية ومنع تكرار حدوثها داخل القطاع المالي والمصرفي، كما انه يقوم بالكشف عن العديد من الهجمات السيبرانية استباقياً أيضاً عن طريق توظيف منظومة تكنولوجية غير نمطية، يمكنها من خلال الترابط الشبكي مع البنوك والمؤسسات المالية المساعدة في الكشف عن المخاطر الأمنية، وإبلاغ الجهة المهددة مبكرًا لاتخاذ الإجراءات الاحترازية اللازمة، بالإضافة إلى تحذير جميع البنوك والمؤسسات المالية بالإجراءات الواجب اتخاذها في ضوء تحليل وتصنيف مختلف الاستخبارات الأمينة من حيث حِدتها وخطورتها، وذلك بالاستفادة من العديد من المنصات الدولية المخصصة للتحذير والابلاغ عن أية هجمات سيبرانية محتملة مشفوعًة بمؤشرات الاختراق (IOCs) والإجراءات العكسية الموصي باتخاذها(https://cbe.org.eg).

ويستخلص الباحث مما سبق أن مخاطر الأمن السيبراني يترتب عليها خسائر ضخمة في بيانات البنوك وأضراراً بسمعتها، وبالتالي يجب عليها رفع مستوى الوعي بالمخاطر السيبرانية وتقييد النسخ الاحتياطي للبيانات والوصول إليها، وتحديد استراتيجيات واضحة في إدارة هذه المخاطر، وانشاء وظائف التحديد والحماية والكشف والاستجابة والتعافي لحماية الأصول الرقمية بالبنوك، وأن البنك المركزي المصري اتخذ خطوات ناجحة في مواجهة المخاطر السيبرانية من خلال تشجيع البنوك للإبلاغ عن حوادث الأمن السيبراني، والمساعدة في مواجهة هذه المخاطر ومنع تكرارها، والكشف عن المخاطر السيبرانية استباقياً وإبلاغ البنوك مبكراً لاتخاذ التدابير والاحتياطيات اللازمة(Uzay, 2003).

2/2 خصائص تشكيل لجان المراجعة ومخاطر الأمن السيبراني

تعرف لجان المراجعة بأنها هيكل إداري يدعم استقلالية المراجعين ويقدم المساعدة لمراجعي الحسابات المستقلين (Uzay, 2003)، وفي قانون Sarbanes-Oxley توصف لجان المراجعةبأنها هيئة

داخلية يتم أنشاؤها من أجل الإشراف على المحاسبة وإعداد التقارير المالية ومراجعة البيانات المالية (Pashkoffand Miller, 2002).

وقد أشار (Dezoortet al., 2002) إلى معايير فعالية أداء لجان المراجعة من خلالامتلاكها للأعضاء المؤهلون الذين يتمتعون بالسلطة والموارد اللازمة لحماية مصالح المساهمين، من خلال ضمان ضوابط داخلية موثوقة وإدارة المخاطر وإعداد التقارير المالية الموثوق فيها، والتي تتكون من مكونات مختلفة تتمثل في: (استقلالية الأعضاء وخبرتهم العملية والتأهيل العلمي، السلطة من خلال المسئولية والتأثير، الموارد من خلال الحجم، والاجتهاد من خلال الدوافع والمثابرة أي بذل العناية اللازمة، ودورية الاجتماعات).

وتشير استقلالية لجان المراجعة إلى تكوينها من المديرين غير التنفيذيين، والاستقلالية مهمة في ضمان نزاهة عملية إعداد التقارير المالية وأداء الشركة، وذلك لأن الإدارة قد تميل للتلاعب في الحسابات من أجل مصلحتهم الشخصية. أما خبرة لجان المراجعة فتشير لوجود أعضاء باللجنة تتمتع بالخبرة المالية والمحاسبية أما حجم لجنة المراجعة فتتكون عادة من3 إلى 5 أعضاء كحد أقصى. أما اجتماعات لجان المراجعة فتشير لعدد المرات التي تجتمع فيها اللجنة في العام، ومن الشائع أن تكون 4 مرات في العام. التنوع بين الجنسين يشير لوجود عدد من النساء في تشكيل اللجنة، فعديد من الدراسات تشير إلى أن النساء أكثر حيادية في الأحكام والسلوك الأخلاقي من الرجال (Gbenyiet al.,2023).

وقد أشارت شركة KPMG إلى أنه يجب اعتبار التهديدات السيبرانية جزء من عملية إدارة مخاطر الشركة، ويكون دور لجنة المراجعة تحديد ما إذا كانت الشركة، تقوم بالآتي:

- تحديد أصول المعلومات الهامة التي ترغب الشركة في حمايتها من الهجمات الالكترونية، سواء كانت بيانات مالية أو بيانات تشغيلية أو بيانات العملاء أو الموظفين أو الملكية الفكرية.
- فهم ومعرفة التهديدات التي تتعرض لها أصول الشركة.
- طريقة تحديد المستوى المقبول من مخاطر الهجوم السيبراني والموافقة عليه والتي تكون الشركة على استعداد لتحمله فيما يتعلق بأصل معلومات معين.
- الضوابط المعمول بها لإعداد وحماية واكتشاف والرد على الهجوم الالكتروني، بما في ذلك إدارة عواقب حادثة الأمن السيبراني.

- الوسيلة المستخدمة لرصد فعالية ضوابط الأمن السيبراني، واختبارها ومراجعتها.
- برنامج التحسين المستمر، لمطابقة التهديد السيبراني المتغير بمؤشرات أداء مناسبة.

كما أوضحت شركة Deloitte أنه لا يجب على لجان المراجعة الاكتفاء بتعليم انفسهم فقط، ولكن ضرورة ارتفاع مستوى التفاعل مع قسم تكنولوجيا المعلومات، وتشجيع مديري تقنية وأمن المعلومات على المشاركة في تبادل المعلومات بين الزملاء في العمل، والاستعانة بخبرات مكاتب المراجعة الخارجية وتبادل المعلومات مع البنوك الأخرى، وتقييم الأمن السيبراني من خلال العلم باتجاهات الأمن السيبراني والتطورات التنظيمية والتهديدات الرئيسية للشركة، حيث يمكن أن يترتب عليها عواقب اقتصادية وتجارية تؤثر بشكل كبير على المساهمين، وبصفة عامة هناك مجموعة من العمليات التي يجب على لجان المراجعة أن تكون على معرفة بها: كالخطط الاستراتيجية العامة لحماية الأصول، مدى استجابة المنظمة للحوادث وخطط الاتصال، الأصول الهامة للمنظمة والمخاطر المرتبطة بها التي يتعين تأمينها، تحديد نقاط الضعف، وكيفية الكشف عن المخاطر وتلبية البنية التحتية الحيوية والمتطلبات التنظيمية، الضوابط الموجودة لمراقبة أجهزة الشركة، المعلومات الرقمية التي تغادر المنظمة، وكيفية تعقبها، مدى وجود موظفين مدربين وذوي خبرة للتنبؤ بالمخاطر السيبرانية، الأشخاص الذين يقومون بتسجيل الدخول لشبكة البنك، ومدى مناسبة المعلومات التي يصلون إليها لدورهم بالبنك.

وتؤثر ثلاث مكونات رئيسية على الأمن السيبراني في كل مؤسسة، مخاطر العوامل التقنية ومخاطر العوامل البشرية ومخاطر العوامل التنظيمية، وبالتالي فإن سوء فهم المخاطر الالكترونية أو التقليل من شأنها يمثل خطراً على الشركة يجب مراعاته بشكل كبير، وذلك لأن المخاطر السيبرانية ليست افتراضية بل فعلية، وبالتالي فإن الوضع السيبراني يجب أن يؤخذ على مستوى لجنة المراجعة حتى يتم تقييم المستويات الثلاثة السابقة (EndsleyandGarland,2000)، ويتم تقييم القضايا السيبرانية من قبل لجان المراجعة، ويكون ذلك من خلال مدى وجود وعي لدى أعضاء لجنة المراجعة بالوضع السيبراني ووجود مشاركة وتفاعل لرؤساء أقسام تقنية المعلومات خلال اجتماعات لجان المراجعة، وجود دراسة متعمقة من قبل لجنة المراجعة للأشخاص الذين قد يكون لديهم وصول غير مقيد إلى النظام، مدى نشر الوعي السيبراني من خلال الإدارة الوسطى التشغيلية وتوفير التدريب وتأمين وصولهم وسلوكياتهم (ThiéryandFass ,2020).

ويجب أن تكون لجان المراجعة على دراية باتجاهات الأمن السيبراني والتطورات التنظيمية والتهديدات الرئيسية التي تواجه الشركة، حيث من الممكن أن تكون المخاطر المرتبطة بالتهديدات شديدة

ويترتب عليها عواقب وخيمة على المساهمين، وهناك عدد من الموضوعات التي قد ترغب لجان المراجعة في الاهتمام بها عند الإشراف على مخاطر الأمن السيبراني، تتمثل في (1) معرفة البيانات التي تغادر الشركة، وأنشطة المراقبة المرتبطة بها، ومدى وجود برنامج فعال لمنع فقدان البيانات، (2) مدى وجود خطة استجابة للحوادث السيبرانية ومحدثة، ومدى تطبيقها من عدمه، فخطة الأمن السيبراني تتضمن وجود ضوابط للحماية من التهديدات المعروفة والناشئة، ووجود يقظة لاكتشاف الأنشطة الخبيثة أو غير المصرح بها، ووجود مرونة للتصرف والتعافي بسرعة لتقليل التأثير،(3) معرفة من يقوم بتسجيل الدخول إلى شبكتنا وموقعه،(4) التهديدات الالكترونية ونقاط الضعف التي تشكل أكبر خطر على اعمال الشركة وسمعتها،(5) مدى وجود الأنظمة لحماية المعلومات المنقولة عبر تقنيات الهاتف المحمول،(6) مدى وجود المسئولية فيما يتعلق بمسئوليات كل موظف في استخدام الأجهزة المحمولة،(7) معرفة مدى تركيز الإدارة على جعل المخاطر الالكترونية جزءً من وظيفة الجميع، وليس فقط تكنولوجيا المعلومات،(8) مدى وجود المقاييس الصحيحة لقياس نجاح برنامج إدارة التهديدات الالكترونية،(9) مدى وجود خطط لرسم سياسة وإطار عمل الأمن السيبراني،(10) مدى توفير البرامج التدريبية التي تثقف الموظفين حول المخاطر السيبرانية(Galligan, 2014).

ويستنتج الباحث مما سبق أن خصائص تشكيل لجان المراجعة المتمثلة في الاستقلالية والخبرة المالية والمحاسبية ودورية الاجتماعات وبذل العناية المهنية الواجبة والتنوع في تشكيل اللجان، لها دور فعال ومؤثر في مواجهة المخاطر السيبرانية والتي يترتب عليها النزاهة في إعداد التقارير المالية ووجود حيادية في الاحكام والسلوك الاخلاقي، وتمكنها من فهم ومعرفة التهديدات السيبرانية وتحديد المستوى المقبول من مخاطر الهجوم السيبراني، والاستعانة بخبرات مكاتب المراجعة المتخصصة، ووجود التفاعل والمشاركة بينها وبين رؤساء أقسام تقنية المعلومات، وبما يحقق تعظيم دور معايير لجان المراجعة في مواجهة مخاطر الأمن السيبراني بالبنوك.

3/2 آليات عمل لجان المراجعة ومخاطر الأمن السيبراني

تتكون آليات عمل لجان المراجعة من إدارة المراجعة الداخلية والإشراف عليها، ودراسة نظام الرقابة الداخلية، والتوصية لمجلس الإدارة بتعيين المحاسبين القانونيين وفصلهم وتحديد أتعابهم ومتابعة أعمالهم، وكذلك دراسة القوائم المالية الأولية والسنوية قبل عرضها على مجلس الإدارة وإبداء الرأي على السياسات المحاسبية المتبعة والتوصية لمجلس الإدارة في شأنها (القرموطي، 2020).

وقد أشارت دراسة هاشم (2012) إلى مجموعة من الإجراءات العامة التي يجب أخذها في الاعتبار فيما يتعلق بدور لجان المراجعة في إدارة المخاطر المصرفية الالكترونية، من خلال تمكين الإدارة من التعرف على مخاطر العمل والتعامل معها وتوفير تقييم مستقل للمخاطر، تقييم الامتثال للقوانين والسياسات والتعليمات التشغيلية، تقييم فعالية العمليات وكفاءتها واقتصادها، ويتحقق ذلك من خلال لجان المراجعة.

1/3/2 فعالية المراجعة الداخلية:

توصى مبادئ الإدارة السليمة للمخاطر بأن يتم تنظيم إدارة مخاطر الأمن السيبراني في ثلاث خطوط، الخط الأول مديري وحدات الأعمال ووظيفة تكنولوجيا المعلومات الذي يعتبر مخاطر الأمن السيبراني جزءً لا يتجزأ من عملهم ويضع الهياكل والضوابط المناسبة لإدارة المخاطر، الخط الثاني وظيفة أمن المعلومات الذي توفر الخبرة لتنفيذ ومراقبة فعالية ضوابط الأمن السيبراني، الخط الثالث هو فعالية المراجعة الداخلية، حيث توفر للجنة المراجعة ومجلس الإدارة ضماناً مستقلاً بأن استراتيجية إدارة مخاطر الأمن السيبراني وسياساتها وإجراءاتها فعالة، وذلك من خلال مراجعة مدى كفاية أدوار العمل الذي قام به الخط الأول والثاني (Deloitte, 2017; IIA, 2020d).

تتطلب فعالية المراجعة الداخلية مراجعة ما إذا كانت مخاطر وضوابط الأمن السيبراني متوافقة مع قابلية المخاطر للمؤسسة، وما إذا كانت حوكمة تكنولوجيا المعلومات تدعم استراتيجيات وأهداف تلك المؤسسة، ويحتاج المراجعين الداخليين كذلك النظر في إطار عمل الأمن السيبراني، والإرشادات المهنية وأفضل الممارسات، حيث يحدد إطار عمل الأمن السيبراني العمليات التي يجب أن يتبعها الخط الأول والثاني بشكل منهجي ويفترض أن يقوم المراجعين الداخليين بمراجعتها (IT Governance Institute, 2006, 2007; IIA, 2016; Deloitte, 2017).

ويمكن تصنيف فعالية مراجعة الأمن السيبراني من خلال معايير الممارسة المهنية للمراجعة الداخلية، والتي تتطلب أن تتكون كل مهمة مراجعة من التخطيط، الأداء، والإبلاغ عن النتائج، فالتخطيطيعنى أن يكون المراجع الداخلي استباقي في فهم المؤسسة والأمن السيبراني والتطلع للأمام في تقيمه للتهديدات الحالية والناشئة (استباقي) والتغييرات في التنظيم واتجاهات الصناعة (KahyaogluandÇaliyurt, 2018)، فالعمل الإستباقي يستلزم التفاعل مع مجلس الإدارة وخطي الدفاع الأوليين.

يعتبر النشاط الأكثر أهمية في إجراء تقييم مخاطر الأمن السيبراني هو تحديد الأصول الرقمية الأكثر قيمة للمؤسسة، وتحديد ما يعنيه إذا تم اختراقها، الخطوة التالية في مرحلة التخطيط هي تقييم نقاط الضعف المرتبطة بهذه الأصول، أي تقييم احتمالية سرقة هذه الأصول أو اختراقها (AHIA and Deloitte, 2017). أداء المهمة هو البعد الثاني ولا يتعلق فقط بكيفية جمع أدلة المراجعة الشاملة ولكن أيضاً بمدى شمولها، فيتم جمع أدلة المراجعة بشكل منهجي للمجالات المحددة في إطار عمل الأمن السيبراني مثل إدارة الهوية والوصول وحماية البيانات وأمان السحابة والبرامج وإدارة الجهات الخارجية والقوى العاملة على سبيل المثال لا الحصر، ولكي يتم اعتبار مراجعة الأمن السيبراني فعالة يجب جمع أدلة كافية لبناء قرار مستنير (El-Masryand Hansen, 2008). الإبلاغ عن النتائج يعتبر تقديم تقرير لمجلس الإدارة ولجنة المراجعة هو البعد النهائي لضمان الأمن السيبراني الفعال، ويجب أن يكون التقرير دقيقاً وموضوعياً وبناءً وكاملاً وفي الوقت المناسب، ويكون ذلك من خلال إصدار رأي عام على النحو المحدد في المعايير (Pelletier, 2020).

2/3/2 الرقابة الداخلية:

يوفر إطار(COBIT) معياراً قابلاً للتطبيق ومقبولاً من أجل تحقيق أمان جيد للأمن السيبراني، وممارسات الرقابة من أجل تدعيم احتياجات الإدارة في تحديد ومتابعة المستوى المناسب لتأمين تكنولوجيا المعلومات، كما يزود المراجعة الداخلية بمجموعة من القياسات والمؤشرات المقبولة للحصول على حوكمة جيدة، تساعد في إبداء الرأي في المؤسسة، كما يعتبر (COBIT) إطار عمل لإدارة مخاطر تكنولوجيا المعلومات ويساعد المديرين والمراجعين والمستخدمين في فهم أنظمة تكنولوجيا المعلومات التي تخص شركاتهم، وكذلك يساعد في تطوير نموذج الحوكمة ويرشد في اختيار مستوى الأمان والسيطرة الضرورية لحماية أصول البنك بشكل فعال (زيود وآخرون،2014).

3/3/2 القوائم والتقارير المالية:

تميل تقارير المخاطر الي أن تكون معلومات غير مالية أكثر من كونها معلومات مالية، وتاريخية وليست مستقبلية، ونوعية وليست كمية، وتحتاج هذه التقارير أن تكون أكثر تكامل وشمول للإبلاغ، وأن تدمج المعلومات المالية وغير المالية بطريقة هادفة ومتكاملة، وتسبب حوادث الأمن السيبراني اضراراً جسيمة بالمؤسسة ومكانتها وثقة العملاء، ويمكن تقسيم تأثير الهجوم السيبراني إلى ثلاث فئات، يتم أخذها في الاعتبار عند الإفصاح: الإضرار بالسمعة، الخسائر المالية، والإجراءات أو الآثار القانونية (Duvenhage et al., 2022).

4/3/2 العلاقة مع مجلس الإدارة:

يعتبر موضوع الأمن السيبراني من الموضوعات الصعبة التي يجب على مجالس إدارة الشركات مراعاتها، وذلك لأنها مخاطر غير مرئية ومتغيرة باستمرار ومنتشرة، مما يجعل من الصعب على مجالس الإدارة إدارتها، وتعتبر مخاطر الأمن السيبراني واحدة من العديد من المخاطر التي تشرف عليها مجالس الإدارة، ويمكن الاعتماد على الإدارة والخبراء الخارجيين للحصول على المشورة والمعلومات فيما يتعلق بإدارة مخاطر الأمن السيبراني، ويجب تقديم تقارير إلى مجلس الإدارة بشأن الخطوات التي تتخذها المؤسسة للتخفيف من التهديدات السيبرانية، ويجب على أعضاء مجلس الإدارة النظر فيما اذا كانت المؤسسة تقوم بتقييم مخاطرها بشكل مناسب وتكريسها للموارد الكافية لهذه القضية (KatzandMcIntosh,2012).

تحتاج مجالس الإدارة إلى فهم الأمن السيبراني وكيفية التعامل معه باعتباره مشكلة إدارة مخاطر على مستوى المؤسسة، وليس مشكلة تتعلق بتكنولوجيا المعلومات، وأن تفهم مجالس الإدارة الآثار القانونية للمخاطر السيبرانية، وتتمتع مجالس الإدارة بإمكانية الوصول للخبرة الكافيةفي مجال الأمن السيبراني، وإعطاء المناقشات حول إدارة المخاطر السيبرانية الوقت المناسب والمنتظم على جدول أعمال مجلس الإدارة، ويجب تحديد كيفية قيام الإدارة بإنشاء إطار عمل لإدارة المخاطر السيبرانية على مستوى المؤسسة من موظفين وميزانية مناسبة، وبأن تتضمن مناقشات الإدارة التنفيذيةومجلس الإدارة تحديد المخاطر السيبرانية التي يجب تجنبها، والمخاطر التي يجب قبولها، والتي يجب التخفيف منها أو نقلها من خلال التأمين، بالإضافة إلى الخطط المحددة المرتبطة بكل نهج(Cerin,2020).

ويجب إسناد مسئولية الأمن السيبراني صراحة إلى لجنة المراجعة، لتقدم المشورة لمجلس الإدارة، وتكون برئاسة مدير مستقل وتتألف اللجنة من مديرين مستقلين من ذوي الخبرة، حتى يستطيعوا تقييم مهارات وخبرات المديرين التنفيذيين الذين يتحملون مسئولية الأمن السيبراني للشركة ومتابعة عملية المراجعة سواء المراجعة الداخلية أو المراجعة الخارجية، وتقييم البنية التحتية التي تطبقها الشركة لمنع وإدارة أحداث الأمن السيبراني المحتملة، والتدابير الأمنية المتمثلة في السياسات والاجراءات المطبقة لتوعية الموظفين والعملاء لمخاطر الأمن السيبراني، ومناقشة حوادث البنية التحتية و الخسائر والغرامات المترتبة عليها(McGrath et al., 2022).

وهنا يبرز دور لجان المراجعة ومجالس الإدارة في إدارة المخاطر السيبرانية، من خلال الإشراف على برنامج الأمن السيبراني والمشاركة الفعالة والاستباقية من مجلس الإدارة ولجنة

المراجعة، وتلعب لجنة المراجعة دور في الإشراف على أنشطة إدارة المخاطر ومراقبة سياسات الإدارة وإجراءاتها، وتنسيق سياسات ومبادرات المخاطر الالكترونية وتأكيد فعاليتها، وتشمل هذه المسئوليات تحديد التوقعات والمساءلة للإدارة، وكذلك تقييم كفاية الموارد والتمويل والتركيز لأنشطة الأمن السيبراني، ويمكن أن يكون رئيس لجنة المراجعة هو جهة اتصال فعالة بشكل خاص مع المجموعات الأخرى في فرض وابلاغ التوقعات بالأمن وتخفيف المخاطر(Yewet al.,2015)

ويستنتج الباحث مما سبق أن آليات عمل لجان المراجعةمتمثلة في المراجعة الداخلية والرقابة الداخلية والتقارير والقوائم المالية والعلاقة مع مجلس الإدارة، فالمراجعة الداخلية توفر للجنة المراجعة ضمان بأن استراتيجية إدارة المخاطر السيبرانية فعالة، أما بخصوص الرقابة الداخليةفيتم تقييم مدى فعالية وقدرة الرقابة الداخلية بالبنك على الإشراف على التطبيقات والخدمات المصرفية الرقمية، في حين يتم الإفصاح في التقارير والقوائم المالية عن المعلومات المالية وغير المالية المتعلقة بحوادث الهجوم السيبراني، أما العلاقة مع مجلس الإدارة فتكون من خلال تقديم المشورة والمعلومات المتعلقة بإدارة مخاطر الأمن السيبراني وتقديم التقارير له بشأن الخطوات المتخذة للتخفيف من الهجمات السيبرانية، وبما يحقق تعظيم دور آليات عمل لجان المراجعة في مواجهة مخاطر الأمن السيبراني بالبنوك.

المحور الثالث: مراجعة أدبيات الدراسة واشتقاق فروض

يمكن تقسيم الدراسات السابقة التي تناولت موضوع الدراسة الحالية إلى ثلاثة أقسام كما يلي:

1/3 دراسات تناولت مخاطر الأمن السيبراني:

هدفت دراسة (Al-AlawiandAl-Bassam, 2019)إلي تحديد عوامل الأمن السيبراني في القطاع المصرفي البحريني، وتوصلت إلى أن التزام الإدارة العليا بدعم الوعيبالأمن السيبراني، ووجود ميزانية كافية لتنفيذ الأمن السيبراني، والأمتثال لسياسة الأمن السيبراني من خلال المتطلبات الإلزامية التي تحددها السياسات الداخلية والالتزامات التعاقدية، وثقافة الأمن السيبراني من خلال الاهتمام بتوعية الموظفين بالقضايا الأمنية والعواقب، تعد أمور ضرورية للوعي بالأمن السيبراني، واحتل الامتثال لسياسة الأمن السيبراني المرتبة الأولى، يليه دعم الإدارة العليا، ثم الميزانية، وأخيراً ثقافة الأمن السيبراني في المرتبة الأخيرة من حيث درجة الأهمية، وأوصت بضرورة وجود دعم من مجلس الإدارة بخصوص الأمن السيبراني.

وتناولت دراسة (البغدادي، 2021) إبراز التحديات التي تواجه المجتمع من أجل تحقيق الأمن السيبراني، وتوصلت إلى أن ادراج المخاطر السيبرانية ضمن المخاطر التشغيلية للبنوك يعتبر أمر غير كافي، حيث أن المعايير الرقابية على المصارف تتطلب أهمية تضمين الاستراتيجيات والسياسات بتلك المصارف جزء خاص بإدارة المخاطر السيبرانية، فالطبيعة المتطورة للمخاطر السيبرانية ليست قابلة للتنظيم بشكل محدد، كما أن القضايا الخاصة بالأنترنت يمكن معالجتها من خلال اللوائح المتعلقة بالمخاطر التشغيلية والتقنيات.

وركزت دراسة (GatzertandSchubert, 2022) على درجة الوعي بالمخاطر السيبرانية في البنوك وشركات التأمين الامريكية من خلال فحص التقارير السنوية خلال الفترة من 2011-2018، وتوصلت لوجود وعي متزايد بالمخاطر السيبرانية في البنوك وشركات التأمين، وأن الشركات التي تنتمي للصناعة المصرفية على درجة وعي أعلى بالمخاطر السيبرانية وتنفيذ إدارة المخاطر السيبرانية، ووجود علاقة ايجابية بين إدارة المخاطر السيبرانية وقيمة الشركات المصرفية وشركات التأمين، كما تلاحظ أن الشركات المربحة أقل تنفيذاً لإدارة المخاطر السيبرانية، وأوصت بضرورة وضع استراتيجية للمخاطر السيبرانية وإطار عمل ولجنة للأمن السيبراني.

وناقشت دراسة (الخرينجوآخرون، 2022) دور حوكمة تكنولوجيا المعلومات في إدارة المخاطر السيبرانية للقطاع المصرفي، وتوصلت إلى أن أهم المعوقات في تطبيق حوكمة تكنولوجيا المعلومات في أنه لا توجد لجنة لتكنولوجيا المعلومات تابعة لمجلس إدارة القطاع المصرفي، والسماح لغير المصرح لهم بالدخول إلى برامج القطاع المصرفي المختلفة. تسهم حوكمة تكنولوجيا المعلومات في إدارة المخاطر السيبرانية بالقطاع المصرفي من خلال الاعتماد على مصادر موثوقة ومرخصة لإدارات تطوير التطبيقات وتقديم الاستشارات اللازمة عند تصميم وتحسين استراتيجيات إدارة المخاطر السيبرانية في ظل حوكمة تكنولوجيا المعلومات، وأوصت بقيام إدارات المصارف بإنشاء لجنة متخصصة للأمن السيبراني.

في حين بحث دراسة (أبو الخير، 2023) أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية لدعم الاستقرار المالي بالبنوك الالكترونية، وتوصلت إلى أن التطور الحادث في المخاطر السيبرانية يحفز البنوك الالكترونية على البحث المستمر والمكثف لاتخاذ اجراءات رقابية لمواجهة هذه المخاطر ويكون ذلك من خلال اللوائح التي تجعل تلك الاجراءات أكثر وضوحاً أمام مجالس إدارات

البنوك، الأمر الذي يؤدي لدعم الاستقرار المالي في تلك البنوك. وأوصت بتكثيف التوعية للعملاء من خلال البرامج المسموعة والمرئية لرفع ثقافة الأمن السيبراني لديهم.

وتناولت دراسة (JohriandKumar, 2023)موضوع وعي العملاء ورضاهم عن الأمن السيبراني (الهجمات الإلكترونية، التصيد الاحتيالي، القرصنة) في سياق التحول الرقمي المصرفي في السعودية، كما تم دراسة التوقعات الخاصة بالدعم الفني والخدمات المتعلقة بالأمن السيبراني، وتظهر النتائج أن التحول الرقمي قد عزز قطاع البنوك السعودية، ويستفيد العملاء من الخدمات عبر الانترنت، ومع ذلك فإن زيادة وعي العملاء بأنشطة الهجمات الالكترونية والتصيد والقرصنة ستؤثر على رضا العملاء عن المعاملات الرقمية، وأن العملاء بحاجة إلى مزيد من الرضا عن جوانب مستوى الأمان من جانب البنك، ويجب على البنوك أن توفر برامج تدريب منتظمة لحماية العملاء من الهجمات الإلكترونية، وكذلك ضرورة إعداد إدارة للأمن السيبراني لتحقيق أهداف الاستدامة طويلة الاجل بسهولة.

وبناءً على ما سبق، يصيغ الباحث الفرض الأول للدراسة كما يلي:"لا توجد فروق معنوية ذات دلالة إحصائية بين أراء عينة الدراسة بشأن مخاطر الأمن السيبراني وطرق مواجهتها".

2/3 دراسات تناولت خصائص تشكيل لجان المراجعة ومخاطر الأمن السيبراني

ركزت دراسة (Ojekaet al.,2017) على العلاقة بين فعالية لجنة المراجعة والأمن السيبراني لعدد من البنوك المدرجة بالبورصة النيجيرية، وتوصلت إلى أن استقلالية لجنة المراجعة والخبرة المالية والتكنولوجية لها علاقة سلبية غير مهمة بالأمن السيبراني في البنوك النيجيرية، ما يعني أن لجنة المراجعة غير قادرة على توفير وظائف الإشراف والرقابة على الأمن السيبراني في القطاع المصرفي، ولذلك توصي الدراسة بضرورة وجود الخبرة التكنولوجية والمالية بلجنة المراجعة.

وتناولت دراسة (الشواربي، 2018) موضوع أثر دوران أعضاء لجان المراجعة على فعالية لجان المراجعة من حيث الاستقلالية والخبرة المالية والمحاسبية لأعضائها، وطول فترة التعيين لأعضاء لجنة المراجعة على أتعاب المراجع الخارجي، وتوصلت الدراسة إلى أن اتعاب المراجعة مرتبطة سلبياً بطول مدة تعيين أعضاء مجلس الإدارة في لجنة المراجعة المستقلة، بمعنى أن عضوية أعضاء لجنة المراجعة لفترة طويلة في اللجنة يؤدي لإنخفاض أتعاب المراجعة الخارجية. وأوصت بضرورة إصدار

تشريع يلزم الشركات بضرورة دوران أعضاء لجان المراجعة، وتحديد مدة العضوية لزيادة الفعالية والمصداقية في التقارير المالية.

واختبرت دراسة (Badawy, 2020) العلاقة بين فعالية لجنة المراجعة والنمو المستدام للشركات في مصر، وتوصلت لعدم وجود علاقة ايجابية معنوية بين حجم لجنة المراجعة والنمو المستدام للشركات، ولكنها خلصت لوجود علاقة ايجابية ومعنوية بين استقلال واجتماعات لجنة المراجعة والنمو المستدام للشركات، وهو ما يعني أن لجان المراجعة تلعب دوراً حوكمياً ورقابياً مهماً في النمو المستدام للشركات غير المالية المسجلة في البورصة المصرية.

وقامت دراسة (Bepari, 2023)ببحث أثر خصائص لجنة المراجعة (جنس أعضاء اللجنة، الخبرة المالية والمحاسبية، الخبرة الصناعية، الخبرة القانونية) على عدد ومحتوى إفصاحات مسائل المراجعة الرئيسية التي تم الكشف عنها من قبل المراجعين الخارجيين بأستراليا، وتوصلت إلى أن أعضاء لجنة المراجعة من الإناث يقللن من عدد ومحتوى إفصاحات مسائل المراجعة الرئيسية من قبل المراجعين الخارجيين، وأن أعضاء لجنة المراجعة من الذكور يفصحون عن معلومات أكثر تحديداً، ويحددون معايير إدارة الأداء أكثر دقة، وينتجون إفصاحات عن مسائل المراجعة الرئيسية أكثر قابلية للقراءة في وجود عضوات في لجنة المراجعة، ونفس النتائج بالنسبة للخبرة المالية والمحاسبية والخبرة الصناعية لأعضاء لجنة المراجعة. الخبرة القانونية لأعضاء لجنة المراجعة تقلل من خصوصية الإفصاح وقابلية القراءة لمسائل المراجعة الرئيسية، وتوصي الدراسة بضرورة تنوع لجنة المراجعة من حيث النوع والخبرة المحاسبية والمالية والخبرة الصناعية والخبرة القانونية بما يعزز شفافية التقارير المالية وتقارير المراجعة الخارجية.

وبحثت دراسة (Gbenyiet al.,2023) تأثير خصائص لجنة المراجعة على أسعار أسهم بنوك الإيداع المالية النيجيرية، وتوصلت للتأثير الضار لاستقلالية لجنة المراجعة وحجمها وتكرار الاجتماعات والتنوع بين الجنسين على أسعار أسهم بنوك الإيداع المدرجة بالبورصة النيجيرية، كما توصلت إلى أن الخبرة المالية للجنة المراجعة تؤثر ايجابياً ولكن بشكل ضئيل على أسعار أسهم بنوك الإيداع المدرجة بالبورصة النيجيرية، لذلك أوصت الدراسة بضرورة منح الخبرة المالية لأعضاء لجنة المراجعة أقصى درجات اهتمام مجلس الإدارة.

هدفت دراسة (LiuandChin, 2023) إلي فحص العلاقة بين الخبرة المالية والمصرفية للجنة المراجعة على التعاقد على القروض المصرفية، وتوصلت إلى أن الشركات ذات الخبرة المصرفية

لأعضاء لجنة المراجعة تميل إلى أن يكون لديها حجم قروض أكبر، وأن البنوك تقدر الخبرة المصرفية للشركات، تقدم لهم معدلات فائدة وشروط ميسرة (احتمالية تقديم ضمانات وتعهدات مالية واستحقاق أطول) للمقترضين الذين يتمتع أعضاء لجنة المراجعة بالخبرة المصرفية.

وبناءً على ما سبق، يصيغ الباحث الفرض الثاني للدراسة كما يلي:"لا توجد فروق معنوية ذات دلالة إحصائية في أراء عينة الدراسة حول دور خصائص تشكيل لجان المراجعة في تعزيز قدرة البنوك المصرية على مواجهة مخاطر الأمن السيبراني".

3/3 دراسات تناولت آليات عمل لجان المراجعة ومخاطر الأمن السيبراني

تناولت دراسة (هاشم، 2012) العلاقة بين وجود لجنة المراجعة الفعالة والحد من مخاطر البنوك الالكترونية في عدد من البنوك المصرية، وتوصلت الدراسة لوجود علاقة بين دور لجان المراجعة والحد من مخاطر البنوك الالكترونية، وأوصت الدراسة بضرورة التأكد من مكافحة مخاطر توقف الأجهزة، مخاطر الفقد الكلي أو الجزئي للبيانات أو تغييرها، كفاءة الأجهزة الإلكترونية بما يسمح بتقبل أي تطورات، ووجود رقم وحيد لكل صفقة تتم من خلال قاعدة البيانات.

وركزت دراسة (KatzandMcIntosh, 2012) على بحث العلاقة بين مخاطر الأمن السيبراني ومجلس الإدارة، وتوصلت إلى أن فشل مجلس الإدارة في إدارة مخاطر الأمن السيبراني يعتبر اخلال بواجب الوكالة، وأوصت بضرورة وجود معايير صادرة عن معهد المعايير والتكنولوجيا (NIST) والمنظمة الدولية للمقاييس والمعايير (ISO) في ظل تزايد الاهتمام بقضايا الأمن السيبراني والاعتماد على التكنولوجيا، وضرورة قيام مجلس الإدارة بخلق ثقافة ترى الأمن السيبراني مسئولية الجميع وتشجيع الإبلاغ عن المخاطر الأمنية.

وهدفت دراسة (Shamsuddinet al.,2018) إلى استكشاف فاعلية المراجعة الداخلية في إدارة الأمن السيبراني في المؤسسات المصرفية الماليزية، وتوصلت لوجود أهمية لفعالية المراجعة الداخلية الذي تم قياسها من خلال: (وعي المراجعين الداخليين، السياسة التنظيمية للأمن السيبراني، وإدارة المخاطر التنظيمية للأمن السيبراني) في إدارة الأمن السيبراني للمؤسسات المصرفية الماليزية، وما يترتب على ذلك من ارشادات هامة تساعد المراجعين الداخليين لتقليل الإرهاب السيبراني.

وبحثت دراسة (Vukoet al.,2018) مدى فعالية المراجعة الداخلية لضمان الأمن السيبراني بالتطبيق على مراجعي تكنولوجيا المعلومات والرؤساء التنفيذيين للمراجعة لعدد من مختلف الصناعات

والمنظمات من مختلف الدول، وتوصلت لعدم وجود علاقة سببية واضحة بين فعالية ضمان الأمن السيبراني واحتمال وقوع هجوم الكتروني جديد، كما توصلت الي وجود ارتباط ايجابي قوي للتخطيط والأداء وإعداد التقارير لكل مهمة مراجعة بنضج مخاطر الأمن السيبراني.

وناقشت دراسة (Kartalet al.,2018) مدى كفاية لجان المراجعة في القطاع المصرفي التركي، وتوصلت لوجود تأثير للجان المراجعة على القطاع المصرفي التركي، باعتبارها المسؤولة عن الإشراف على الرقابة الداخلية، المراجعة الداخلية، إدارة المخاطر، قواعد السلوك والأخلاق، المحاسبة والتقارير المالية، المراجعة الخارجية، خدمات الدعم، خدمات التقييم، ومكاتب التصنيف. وفيما يتعلق بتحليل القضايا المتعلقة بلجان المراجعة، تم فحص هيكل وفعالية وكفاءة وأداء لجان المراجعة، فبالنسبة لهيكل لجان المراجعة، كان ميثاق لجنة المراجعة غير موجود، ولم يتم تشكيل لجان الترشيح لاختيار أعضاء لجان المراجعة، ولم يتضمن خطط التعاقب والتناوب، ولا يوجد تدريبات منتظمة لأعضاء لجان المراجعة في بعض البنوك، ولم يكن أعضاء لجان المراجعة المتفرغين حاضرين، وفيما يتعلق بعنصر الفعالية والكفاءة في التزامات المراجعة، لم تحدد لجان المراجعة مسئوليات الرقابة الداخلية والمراجعة الداخلية بوضوح، ولم تتسق أنشطة المراجعة بين الرقابة الداخلية والمراجعة الداخلية والمراجعة الخارجية، عدم دعوة كبار مديري الوحدات التشغيلية فيما يتعلق بالموضوعات التي تمت مناقشتها في اجتماعات اللجان في بعض البنوك، وفيما يتعلق بمكون أداء لجان المراجعة، لم يتم قياس أداء لجان المراجعة، معايير قياس الأداء لم يتم تحديدها في بعض البنوك. كما تم نقل صلاحيات لجان المراجعة إلى المراجعة الخارجية، وخدمات الدعم والتقييم وعملية مكتب التصنيف لإدارات الأنظمة الداخلية، وأوصت الدراسة بإجراء تغييرات تشريعية من أجل تعزيز موقف لجان المراجعة في البنوك، ووجود دليل يحتوي على الممارسات الجيدة للجان المراجعة في البنوك.

واستهدفت دراسة (القرموطي، 2020) التعرف على المتطلبات الأساسية لتعزيز لجان المراجعة التي تؤدي لتفعيل حوكمة الشركات داخل الشركات المساهمة، وتوصلت لوجود ارتباط معنوي قوي ذو دلالة معنوية بين متطلبات تعزيز لجان المراجعة لتحقيق الدور الملائم لزيادة فاعلية حوكمة الشركات، وأوصت بإصدار دليل استرشادي لتنظيم لجان المراجعة وبيان معاييرها وآلياتها يتم إلزام كافة الشركات المقيدة في سوق الأوراق المالية به.

وتناولت دراسة (غلام الله، 2020) الدور الذي تلعبه لجنة المراجعة فيما يتعلق بالأمن الالكتروني للحد من مخاطر الجريمة الإلكترونية في المؤسسات الجزائرية، وتوصلت إلى أن السياسات المتعلقة بالأمن الالكتروني ومحاربة الجريمة غائبة، وذلك لعدم وجود لجان مراجعة بالمؤسسات الجزائرية، وعدم وجود اهتمام من طرف لجان المراجعة بموضوع الجرائم الالكترونية وسياسات الأمن الإلكتروني، وأوصت بضرورة اصدار تشريعات تفرض على المؤسسات الإلتزام بمستوى معين من تجهيزات الأمن الالكتروني، وضرورة الاسراع في إنشاء لجان المراجعة واعطائها الصلاحيات وفقاً للمعايير الدولية.

كما تناولت دراسة (ThiéryandFass, 2020) تحديد مستوى الوعي بالموقف السيبراني لأعضاء لجنة المراجعة بفرنسا، وتوصلت إلى أنه يجب أن تكشف التقارير السنوية عن المخاطر بما في ذلك المشكلات السيبرانية في حالة حدوثها ولكن فقط إذا كانت جوهرية، وهذا يعني أنه بدون أي تأثير مادي لا يتم الكشف عن المشكلات السيبرانية للجمهور، وأن الكشف عن المشكلات السيبرانية ليس واضحاً ويعتمد على معرفة وخبرة مجلس الإدارة، وسلطت الدراسة الضوء على أنه عندما يتم التعامل مع المشكلات السيبرانية من قبل لجنة المراجعة من خلال ثلاث مستويات تتمثل في المستوى الاول: الإدراك الأساسي للوعي بالوضع السيبراني(مخاطر عالية على نقاط معينة يمكن عرضها ودراستها بعمق من قبل لجنة المراجعة). المستوى الثاني: وجود بعض الاشخاص لديهم وصول غير مقيد إلى النظام، وبالتالي يجب أن تتناول اجتماعات لجنة المراجعة عرض تقديمي ودراسة متعمقة لهذا الموضوع، المستوى الثالث: الحاجة لتدريب الموظفين على تحسين الوعي بالأنترنت وتأمين وصولهم وسلوكياتهم، أي نشر الوعي السيبراني من خلال الإدارة الوسطى التشغيلية.

وركزت دراسة (Farihaet al.,2022) على بحث تأثير خصائص لجنة المراجعة ومجلس الإدارة على أداء البنوك التجارية المدرجة ببورصة بنجلاديش، وتوصلت إلى وجود مشاكل في القطاع المصرفي تتمثل في زيادة القروض المتعثرة وسوء جودة الإدارة مما ترتب عليه انخفاض الأرباح، ووجود قصور للجنة المراجعة التي تعيق النمو العام للصناعة المصرفية، حيث كانت أهم النتائج : أن استقلالية مجلس الإدارة لها علاقة هامة سلبية مع العائد على الأصول، وله علاقة ايجابية وهامة مع العائد على المخزون، تنوع مجلس الإدارة لها علاقة سلبية وهامة مع العائد على الأصول والعائد على حقوق الملكية، مما يعني عدم كفاءة أعضاء مجلس الإدارة، حجم لجنة المراجعة له تأثير هام وسلبي مع العائد على الأصول، واستقلالية لجنة المراجعة له علاقة سلبية وهامة مع العائد على الأسهم، وأوصت

بضرورة تحسين أعضاء مجلس الإدارة المستقلين وتشكيل لجنة التدقيق مما يساعد الصناعة المصرفية في تحسين الأداء العام.

وسعت دراسة (أماني، 2022) إلى التعرف على واقع الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وأثره على قرارات الاستثمار ومنح الائتمان بالشركات المصرية المسجلة بالبورصة وأثره على سعر السهم وحجم التداول، وأظهرت الدراسة عدم إفصاح الشركات المقيدة عن مخاطر الأمن السيبراني وما يحمله ذلك من آثار سلبية أسعار الأسهم وأحجام التداول، وأوصت بضرورة قيام البنك المركزي المصري بسرعة إصدار الضوابط والارشادات التي تدعم الإفصاح عن أنشطة الأمن السيبراني وبرامج إدارة الأمن السيبراني، وإصدار معيار ينظم جوانب الإفصاح المحاسبي عن أنشطة ومخاطر الأمن السيبراني للشركات.

وقامت دراسة (Duvenhage et al., 2022) ببحث الإفصاح عن المخاطر الالكترونية بالبنوك في الصين وجنوب افريقيا، وتوصلت إلى وجود اختلاف جوهري في البلدين بالنسبة للإفصاح عن المخاطر السيبرانية، حيث نجد أن البنوك الصينية لا تشير صراحة إلى المخاطر السيبرانية، ولكن يتم الإفصاح عنها ضمن المخاطر التشغيلية بالتقارير السنوية، ولا يوجد ترتيب أو تصنيف محدد لتلك المخاطر، ولكن على النقيض نجد أن البنوك في جنوب افريقيا تفصح بشكل واضح وتحدد المخاطر السيبرانية ويتم تصنيفها ضمن أعلى المخاطر بالتقارير السنوية.

وهدفت دراسة (AdrianandWang, 2023) إلي قياس فعالية الرقابة الداخلية للأمن السيبراني بإستخدام إطار (COBIT) وإطار (NIST) بالصناعة المصرفية، وتوصلت لمجموعة من الإرشادات لتنفيذ حوكمة تكنولوجيا المعلومات لحماية الشركات من حوادث الأمن السيبراني، بما يساعد على زيادة انتاجية الشركات من خلال خلق التوافق بين الأعمال وتكنولوجيا المعلومات من أجل التحسين المستمر، وأوصت بتحسين ثقافة توثيق الأنشطة المختلفة التي يتم تنفيذها وتوثيق أشكال التواصل من وإلى الأقسام المختلفة، انشاء نظام لتقليل الاعمال الورقية اليدوية، تدريب العاملين على تحسين مهاراتهم وكفاءتهم، والبدء في تطوير سياسة الأمن السيبراني لحماية البيانات بالصناعة المصرفية.

كما هدفت دراسة (Al-KhasawnehandRazouk, 2023) إلي قياس مدى فعالية وقدرة الرقابة الداخلية على الإشراف على التطبيقات والخدمات المصرفية الرقمية بالبنوك الأردنية خلال جائحة كورونا، وتوصلت إلى أن التطبيقات والخدمات المصرفية الرقمية المستخدمة بالبنوك قد ساهمت في تحقيق أهداف نظام الرقابة الداخلية، كما تتميز هذه التطبيقات والخدمات الرقمية تتميز بخصائص

معلوماتية تجعل الرقابة الداخلية أكثر فاعلية وكفاءة خلال جائحة كورونا، وقد أثرت إجراءات وأنظمة وسلامة البيانات بشكل كبير على فعالية التطبيقات المصرفية الرقمية، وأوصت بضرورة توفير بيئة آمنة لتشجيع العملاء على التعامل مع التطبيقات الرقمية وانتباه البنوك لضوابط أمن وسرية البيانات.

وقامت دراسة (MazumderandHossain, 2023) بقياس مدى الإفصاح عن المخاطر السيبرانية بالتقارير السنوية للبنوك المدرجة في بنجلاديش، وفحص العلاقة بين خصائص تشكيل مجلس الإدارة(الحجم، الاستقلالية، التنوع بين الجنسين) والإفصاح عن المخاطر السيبرانية وتوصلت الدراسة لارتفاع مستويات الإفصاح عن المخاطر السيبرانية خلال فترة الدراسة(2014 : 2020)، ووجود علاقة ايجابية ذات دلالة احصائية بين استقلالية مجلس الإدارة والإفصاح عن المخاطر السيبرانية، والحضور الأعلى للأعضاء الإناث بالمجلس مرتبط بارتفاع الإفصاح عن المخاطر السيبرانية، ولا توجد علاقة بين حجم مجلس الإدارة والإفصاح عن المخاطر السيبرانية.

وبناءً على ما سبق، يصيغ الباحث الفرض الثالث للدراسة كما يلي:"لا توجد فروق معنوية ذات دلالة إحصائية في أراء عينة الدراسة حول دور آليات عمل لجان المراجعة في تعزيز قدرة البنوك المصرية على مواجهة مخاطر الأمن السيبراني ".

4/3 التعليق على الدراسات السابقة

توصلت الدراسات التي تناولت لجان المراجعة إلي وجود أهمية لها في تحقيق النمو المستدام وتفعيل حوكمة الشركات وزيادة عدد ومحتوى الإفصاح عن مسائل المراجعة الرئيسية (القرموطي،2020؛ Kartal et al., 2018; Badawy, 2020; Bepari, 2023)، بإستثناء دراسة (Gbenyiet al.,2023) التي توصلت لوجود علاقة سلبية للجنة المراجعة على أسعار أسهم البنوك النيجيرية المدرجة.

وتوصلت بعض الدراسات إلى وجود أهمية لوجود سياسة ولجنة للأمن السيبراني، بما يعزز قيمة البنوك يحسن استراتيجيات في مواجهة مخاطر الأمن السيبراني. (الخرينجوآخرون،2022؛ Al-AlawiandAl-Bassam,2019; JohriandKumer,2023;Gatzertand Schubert,2022)

وتوصلت إحدى الدراسات إلى وجود أهمية للجنة المراجعة في الحد من مخاطر البنوك الالكترونية

(هاشم،2012)، في حين توصلت بعض الدراسات لوجود علاقة سلبية لدور لجنة المراجعة في الاشراف والرقابة على الأمن السيبراني.(غلام الله،2020 ;Ojeka etal., 2017)

هذا، وقد توصلت الدراسات السابقة التي تناولت العلاقة بين المخاطر السيبرانية ومجلس الإدارة إلى أهمية دوره في نشر ثقافة الأمن السيبراني، ووجود علاقة ايجابية بين مجلس الإدارة والإفصاح عن الأمن السيبراني بالتقارير السنوية (Mazumder and Hossain,2023; Katzand McIntosh,2012).

وخلصت الدراسات السابقة المتعلقة بالإفصاح عن المخاطر السيبرانية إلى ضرورة وجود ارشادات وسياسات ومعيار ينظم الإفصاح عن تصنيفات وأنواع أنشطة الأمن السيبراني بالتقارير السنوية للشركات (أماني،2022; Duvenhageet al.,2022)

في حين توصلت الدراسات السابقة التي تناولت الرقابة الداخلية للأمن السيبراني إلى أهمية وجود تطبيقات تتمتع بخصائص معلوماتية تحقق أهداف الرقابة الداخلية، وتدريب العاملين وتطوير سياسات الأمن السيبراني لحماية البيانات، بما ينعكس على زيادة انتاجية الشركات (AdrianandWang,2023;Al-KhasawnehandRazouk,2023)

وكذا توصلت الدراسات السابقة التي تناولت المراجعة الداخلية والأمن السيبراني إلى أهمية وجود وعي لدى المراجعين الداخليين بالمخاطر السيبرانية، ووجود علاقة مهمة بين فعالية المراجعة الداخلية وإدارة الأمن السيبراني (Vukoet al.,2018 ;Shamsuddinet al.,2018).

وفي النهاية ساعدت الدراسات السابقة سالفة الذكر الباحث في تحديد الفجوة البحثية، وبيان مدي اختلاف دراسته عن تلك الدراسات السابقة، كما ساعدته في تحديد محاور دراسته، وتكوين الإطار النظري لها، وبناء أداة الدراسة (قائمة الاستقصاء).

وقد تمثلت الفجوة البحثية في عدم تناول الدراسات السابقة لدور خصائص تشكيل لجان المراجعة وآلياتها بهدف تعزيز دور لجنة المراجعة في مواجهة مخاطر الأمن السيبراني في البنوك المصرية، حيث تناولت أغلب هذه الدراسات خصائص تشكيل لجان المراجعة وآلياتها منفردة، بالإضافة إلى أن أغلبها تم في بيئات أجنبية، في حين تناقش الدراسة الحالية كيفية تعزيز دور لجان الراجعة كأحد آليات الحوكمة لمواجهة مخاطر الامن السيبراني في البنوك المصرية، بهدف استخلاص مجموعة من النتائج التي يمكن الاعتماد عليها مستقبلاً في منهج إدارة المخاطر السيبرانية بالبنوك المصرية.

المحور الرابع: الدراسة الميدانية

حتي تتحقق قيمة البحث العلمي وتكتمل أهداف الدراسة فأنه يجب ربط الاطار النظري بالممارسة العلمية، ويتم ذلك من خلال التأكد من صحة ما توصل إليه الاطار النظري بالإضافة إلى اختبار فروض الدراسة، ولتحقيق ذلك يقوم الباحث بأجراء دراسة ميدانية من خلال تصميم قائمة استقصاء لاستطلاع آراء وتوجهات عينة من المتخصصين في مجال الدراسة وتحليل هذه الآراء بغرض التوصل إلى مدي صحة فروض الدراسة، ويهدف هذا المحور إلى عرض منهجية الدراسة الميدانية التي اتبعها الباحث والتي تتضمن مجتمع وعينة الدراسة وحدود الدراسة والاختبارات الإحصائية وأخيرا النتائج والتوصيات.

1/4 مجتمع وعينة الدراسة الميدانية:

يتكون مجتمع الدراسة من أعضاء لجان المراجعة بالبنوك المصرية والعاملين بها وأعضاء هيئة التدريس ومعاونيهم بالجامعات المصرية.

ولتحديد حجم العينة قام الباحث باستخدام المعادلة التالية: $N=PQ(Z)^2/E^2$

حيث أن N حجم العينة، P نسبة المجتمع المراد دراسته، Q النسبة المكملة، Z الدرجة المعيارية، E خطأ المعاينة سواء عند (0.05 أو 0.01)، وعند افتراض نسبة المجتمع المتاح 50%، والنسبة المكملة 50%، والدرجة المعيارية (1.96)، وخطأ المعاينة 0.05 فأن حجم العينة يكون 384 مفردة. وقام الباحث بإعداد قائمة الاستقصاء وتوزيعها وحصل على ردود بلغت 388 رد، وقد تم اختيار العينة بطريقة عشوائية من مجتمع الدراسة.

وقد قام الباحث بمراجعة قوائم الإستقصاء المستلمة (الردود) للتأكد من اكتمالها وصلاحيتها لإدخال البيانات وإجراء التحليل الإحصائي، ثم قام بترميز قيم جميع العبارات الواردة بقائمة الإستقصاء بعد مراجعتها على الحاسب الالي باستخدام كلاً من برنامج (Microsoft Excel) وبرنامج الحزمة الإحصائية للعلوم الاجتماعية (SPSS (version 29، وقد تم ترميز الإجابات من خلال إعطاء مجموعة من الأوزان التي يعبر كل منها عن الآراء المختلفة وفقا لمقياس ليكرت الخماسي الاتجاه (Likert Scale)، وهو مقياس فئوي مكون من خمسة درجات لتحديد درجة استجابة أفراد عينة الدراسة على كل فقرة وتحويلها إلى بيانات كمية، يمكن قياسها عملياً كما هو مبين بالجدول رقم (1).

جدول رقم (1): مقياس ليكرت الخماسي

التصنيف	موافق جداً	موافق	محايد	غير موافق	غير موافق جداً
الدرجة	5	4	3	2	1

وقد بلغ عدد قوائم الإستقصاء الصالحة والمستخدمة للتحليل الإحصائي (388) رد، وقد راعى الباحث أن تكون عينة الدراسة ذات خبرة علمية وعملية وعلى دراية بموضوع البحث.

وتوضح الجداول التالية توصيف عينة الدراسة:

1/1/4 النوع:

جدول رقم (2): توزيع عينة الدراسة وفقا لمتغير (النوع)

م	التوزيع	العدد	النسبة المئوية
1	ذكر	250	%64
2	أنثي	138	%36
	المجموع	388	%100

2/1/4 الدرجة العلمية:

جدول رقم (3): توزيع عينة الدراسة وفقا لمتغير (الدرجة العلمية)

م	التوزيع	العدد	النسبة المئوية
1	دكتوراه	61	%16
2	ماجستير	93	%24
3	دبلوم دراسات عليا	54	%14
4	بكالوريوس	180	%46
	المجموع	388	%100

ويتضح من الجدول السابق ما يلي: إن توزيع مفردات عينة الدراسة وفقاً لمتغير "الدرجة العلمية" يشير إلى أن اعلي فئة علمية هي البكالوريوس حيث يحوزون على نسبة 46%، يليها فئة الماجستير بنسبة 24%، ثم يليها فئة الدكتوراه بنسبة 16%، وأخيراً فئة دبلوم الدراسات العليابنسبة 14%، وفقاً لردود مفردات عينة الدراسة والنسب السابقة تزيد من اطمئنان الباحث لنتائج الدراسة.

3/1/4 حاصل على شهادة مهنية:

جدول رقم (4): توزيع عينة الدراسة وفقا لمتغير (حاصل على شهادة مهنية)

م	حاصل على شهادة مهنية	العدد	النسبة المئوية
1	غير حاصل	234	%60
2	جمعية المحاسبين والمراجعين المصرية	34	%9
3	شهادة CIA	19	%5
4	شهادة CMA	54	%14
5	دبلوم IFRS	47	%12
المجموع		388	%100

ويتضح من الجدول السابق ما يلي: أن توزيع مفردات عينة الدراسة وفقاً لمتغير "حاصل على شهادة مهنية" يشير إلى أن الأغلبية لم يحصلوا على شهادة مهنية حيث بلغت نسبتهم 60%، بينما جاءت فئة الحاصلين على شهادة مهنية في المرتبة الثانية بنسبة 40% وفقا لردود مفردات عينة الدراسة.

4/1/4 جهة العمل:

جدول رقم (5): توزيع عينة الدراسة وفقا لمتغير (الوظيفة)

م	التوزيع	العدد	النسبة المئوية
1	قطاع البنوك المصرية	221	%57
2	أعضاء هيئة التدريس ومعاونيهم	167	%43
المجموع		388	%100

ويتضح من الجدول السابق ما يلي: إن توزيع مفردات عينة الدراسة وفقاً لمتغير "جهة العمل" يشير إلى أن فئة العاملين بقطاع البنوك المصرية بنسبة 57%، يليها فئة أعضاء هيئة التدريس ومعاونيهم بإحدى الجامعات المصرية بلغت نسبة 43%وفقا لردود عينة الدراسة.

5/1/4 الوظيفة:

جدول رقم (6): توزيع عينة الدراسة وفقا لمتغير (الوظيفة)

م	التوزيع	العدد	النسبة المئوية
1	موظف بقسم الائتمان والاعمال المصرفية	64	%16.5
2	موظف IT	53	%13.7
3	محاسب بالإدارة المالية بالبنك	42	%10.8
4	مراجع داخلي بالنبك	54	%14
5	عضو لجنة مراجعة بالبنك	8	%2
6	أعضاء هيئة التدريس ومعاونيهم	167	%43
المجموع		388	%100

ويتضح من الجدول السابق ما يلي: إن توزيع مفردات عينة الدراسة وفقاً لمتغير "الوظيفة" يشير إلى أن أعلى فئة وظيفية هي أعضاء هيئة التدريس ومعاونيهم بإحدى الجامعات المصرية بنسبة 43% يليها فئة موظف بقسم الائتمان والأعمال المصرفية بنسبة 16.5%، ثم فئة مراجع داخلي بنسبة 14%، ... ثم في النهاية فئة عضو لجنة مراجعة بالبنك بنسبة 2% وفقا لردود عينة الدراسة.

6/1/4 سنوات الخبرة:

جدول رقم (7): توزيع عينة الدراسة وفقا لمتغير (سنوات الخبرة في مجال العمل)

م	التوزيع	العدد	النسبة المئوية
1	أقل من 5 سنوات	78	%20
2	من 5 سنوات إلى 15 سنة	72	%18.6
3	من 15 سنة إلى 20 سنة	89	%23
4	أكثر من 20 سنة	149	%38.4
	المجموع	388	%100

ويتضح من الجدول السابق: أن نحو (80%) من عينة البحث تزيد خبرتهم عن 5 سنوات مما يدل على توافر الخبرة العملية لغالبية عينة البحث، وبالتالي يمكن الاعتماد على إجابات عينة البحث بدرجة مرتفعة وزيادة ثقة الباحث في آرائهم.

2/4 تصميم قائمة الاستقصاء:

تتكون استمارة الاستقصاء من ثلاثة محاور حيث تم استخدام مقياس ليكرت الخماسي بغرض تحديد آراء واتجاهات المستقصي منهم نحو مدى الموافقة على استفسارات القائمة وذلك على النحو التالي:

المحور الأول: يختص ببيان مدي وجود إدراك ووعيلدي فئات عينة الدراسة بمخاطر الأمن السيبراني وطرق مواجهتها بالبنوك المصرية.

المحور الثاني: يستهدف استطلاع آراء المستقصي منهم عندور خصائص تشكيل لجان المراجعة في مواجهة مخاطر الأمن السيبراني بالبنوك المصرية.

المحور الثالث: يتناول التعرف على آراء المستقصي منهم فيدور آليات عمل لجان المراجعة في مواجهة مخاطر الأمن السيبراني بالبنوك المصرية، وقد تم الاعتماد في ذلك على عدد من الفقرات موضحة بالجدول رقم (8).

جدول رقم (8): الفقرات المستخدمة في قياس متغيرات الدراسة

رقم السؤال	البيـــــــــــــــان
المحور الأول: هل هناك إدراك ووعي كافي لدي فئات عينة الدراسة بمخاطر الأمن السيبراني وطرق مواجهتها بالبنوك المصرية؟	
.1	تعد الخدمات المالية الإلكترونية أكثر الصناعات التي تتعرض للمخاطر المتعلقة بالأمن السيبراني؟
.2	تستهدف مخاطر الأمن السيبراني المؤسسات المالية الكبرى (البنوك)، مما يجعلها تعاني من عدم الاستقرار، وفقدان الثقة لدى العملاء، مما يدفعهم لإلغاء حساباتهم، أو التوقف عن استخدام الخدمات المالية الالكترونية؟
.3	يوجد 3 مخاطر رئيسية تؤثر على الأمن السيبراني بالبنوك المصرية هي المخاطر التكنولوجية، ومخاطر العوامل البشرية ومخاطر العوامل التنظيمية؟
.4	تتعدد أنواع وأشكال مخاطر الأمن السيبراني ومن أهمها ما يلي: التصيّد الاحتيالي عبر البريد الإلكتروني، الفيروسات / البرامج الضارة، الصفحات الإلكترونية المزيفة، كلمات المرور الضعيفة، برامج الفدية، تسرب البيانات الهامة مثل اسم المستخدم وكلمات المرور؟
.5	لا يوجد تشريعات أو لوائح كافية للأمن السيبراني بهدف حماية البيانات ولحماية الأنظمة والشبكات؟
.6	لا تلزم التشريعات أو اللوائح البنوك المصرية بتنفيذ تدابير للأمن السيبراني واجراء مراجعات للأمن السيبراني؟
.7	لا يوجد تشريعات أو لوائح كافية تتناول بالتفصيل حماية الخصوصية والتوقيعات الرقمية والمعاملات الإلكترونية؟
.8	يوجد تدريب على الأمن السيبراني لموظفي البنوك وغيرهم من العاملين في القطاع المصرفي؟
.9	يوجد لدي البنوك في مصر فريق للاستجابة للحوادث الحاسوبية (CIRT) أو فريق للاستجابة للحوادث الأمنية الحاسوبية (CSIRT) أو فريق للاستجابة للطوارئ الحاسوبية بمسئولية وطنية (CERT)؟
.10	يوجد إطار لتنفيذ معايير الأمن السيبراني بالنسبة لقطاع البنوك في مصر؟
.11	يوجد أدوات وتدابير تقنية معينة متعلقة بتوفير الأمن السيبراني، مثل برمجيات مكافحة الفيروسات والرسائل الأقتحامية، متاحة لعملاء قطاع البنوك المصرية؟
.12	يوجد لدي البنوك المصرية أي تدابير تنظيمية لمواجهة مخاطر الأمن السيبراني؟
.13	تم تجميع أفضل ممارسات الأمن السيبراني أو تم إعداد مبادئ توجيهية في هذا الصدد؟
.14	تستثمر البنوك المصرية في برامج البحث والتطوير الخاصة بالأمن السيبراني؟
.15	يتم إطلاق وتنفيذ حملات للوعي العام بالأمن السيبراني؟ وفي هذا الإطار، هل يحاط الجمهور علماً بفوائد استعمال البرمجيات أو الاجهزة أو الحلول القائمة على الخدمة للأمن السيبراني؟
.16	تقوم منظمتكم بوضع أي من مناهج التدريب المهني في مجال الأمن السيبراني أو تدعم وضع هذه المناهج؟
.17	تقوم منظمتكم بوضع أي برامج تعليمية أو مناهج أكاديمية في مجال الأمن السيبراني أو تدعم وضع هذه البرامج والمناهج؟
.18	يوجد آليات لتقديم حوافز حكومية من أجل تشجيع بناء القدرات في مجال الأمن السيبراني؟
.19	لا توجد شراكة بين بنوك القطاع العام وبنوك القطاع الخاص أو تدابير تعاونية سواء اتفاقات ثنائية أو متعددة الأطراف أو دولية بشأن التعاون في مجال الأمن السيبراني؟

جدول رقم (8): الفقرات المستخدمة في قياس متغيرات الدراسة

رقم السؤال	البيـــــــــــــــان
المحور الثاني: ما مدى توافق عينة الدراسة حول دور خصائص تشكيل لجان المراجعة في مواجهة مخاطر الأمن السيبراني بالبنوك المصرية؟	
.20	يؤدي تشكيل لجان المراجعة من 3: 5 أعضاء من الأعضاء غير التنفيذيين بمجلس الإدارة إلى مساعدة البنك في الحد من مخاطر الأمن السيبراني من خلال العمل على تحديدها والتصدي لها ومتابعتها والتقرير عنها؟
.21	تؤثر استقلالية أعضاء لجان المراجعة بشكل إيجابي في قدرتها على التقرير عن مخاطر الأمن السيبراني التي تواجه البنك والافصاح عن أوجه القصور في أداء إدارة البنك لمواجهة تلك المخاطر؟
.22	توافر الخبرة التكنولوجية في مجال الأمن السيبراني لدى لجان المراجعة يدعم دورها في مواجهة مخاطر الأمن السيبراني والحد منها؟
.23	يؤدي التنوع بين الجنسين (أناث وذكور) في تكوين لجان المراجعة إلى تحسين أداء لجان المراجعة في مواجهة مخاطر الأمن السيبراني بالبنوك المصرية؟
.24	بذل العناية المهنية الواجبة من قبل لجان المراجعة اللازمة للموضوعات المعروضة عليها يؤدي إلى تحسين أداء لجان المراجعة في مواجهة مخاطر الأمن السيبراني بالبنوك المصرية؟
.25	تؤدي دورية اجتماعات لجان المراجعة بصفة مستمرة خلال العام (4 مرات على الأقل في العام) إلى تخصيص الوقت الكافي لمتابعة مخاطر الأمن السيبراني بالبنوك المصرية والعمل على مواجهتها والحد منها؟
المحور الثالث: ما مدى توافق عينة الدراسة حول دور آليات عمل لجان المراجعة في مواجهة مخاطر الأمن السيبراني بالبنوك المصرية؟	
.26	مشاركة رؤساء تقنية المعلومات في اجتماعات لجان المراجعة الدورية لتقييم الأمن السيبراني بالبنك يؤدي إلى تحسين أداء لجان المراجعة في مواجهة مخاطر الأمن السيبراني بالبنوك المصرية؟
.27	يساهم إشراف لجان المراجعة على إدارة المراجعة الداخلية بالبنوك في سرعة تحديد مخاطر الأمن السيبراني والتعامل معها؟
.28	تؤدي متابعة لجان المراجعة لنظام الرقابة الداخلية بالبنوك إلى تحديد نقاط الضعف به وتعزيزها مواجهة مخاطر الأمن السيبراني بالبنوك المصرية؟
.29	إسناد مسئولية الأمن السيبراني إلى لجنة المراجعة لتقديم المشورة لمجلس الإدارة يعطي لجان المراجعة الاختصاصات اللازمة لتحديد مخاطر الأمن السيبراني بالبنوك المصرية ومواجهتها؟
.30	يوجد دليل ارشادي لتنظيم آليات لجان المراجعة بالبنوك المصرية فيما يتعلق بالأمن السيبراني يساعدها على أداء دورها؟

المصدر: من إعداد الباحث في ضوء الدراسات السابقة.

3/4 حدود الدراسة:

- **الحدود الزمنية:** تقتصر بيانات الدراسة الميدانية على البيانات التي قام الباحث بجمعها خلال الفترة من يناير2023 حتى يوليو 2023.
- **الحدود المكانية**: اقتصرت الدراسة على البنوك المصرية.

- **الحدود الموضوعية:** اقتصرت الدراسة على التعرف على دور لجان المراجعة في تعزيز قدرة البنوك المصرية في مواجهة مخاطر الأمن السيبراني بقطاع البنوك المصرية، وذلك في محاولة من الباحث لتوسيع دور لجان المراجعة في إضافة قيمة للبنوك المصرية.
- **الحدود البشرية:** اقتصرت الدراسة الميدانية على وحدات للمعاينة تمثلت في: أعضاء لجان المراجعة والمراجعين الداخليين والعاملين بأقسام الائتمان والاعمال المصرفية والإدارة المالية بالبنوك المصرية وأعضاء هيئة التدريس بالجامعات المصرية، وذلك لكونهم الأكثر دراية بممارسات لجان المراجعة بقطاع البنوك.

4/4 الاختبارات الإحصائية:

1/4/4 إجراء إختبارات الثبات والصدق:

يتم إجراء إختبارات الثبات والصدق عادةً بهدف معرفة مدى صدق وصحة وصلاحية قائمة الإستقصاء تمهيداً لإجراء التحليلات الإحصائية، وفيما يلي توضيحاً لكل من معاملي الثبات والصدق.

أ. معامل الثبات:

ويشير إلى مدى استقرار عبارات قائمة الإستقصاء وعدم تناقضها، بمعنى أن تعطي قائمة الإستقصاء نفس النتائج تقريباً باحتمال مساوي لقيمة معامل الثبات في حالة تم إعادة توزيعها أكثر من مرة تحت نفس الظروف والشروط (على عينة أخرى من نفس المجتمع وبنفس الحجم).

وتم استخدام اختبار (Cronbach's Alpha) وهو معامل يأخذ قيماً تتراوح بين الصفر والواحد الصحيح، علماً بأن أقل قيمة مقبولة لمعامل الثبات في البحوث العلمية هي 0.7، وما يزيد عن هذه القيمة يعطي مؤشراً قوياً للحكم على مدى ثبات قائمة الإستقصاء.

ب. معامل الصدق:

يقصد بصدق قائمة الإستقصاء أن العبارات الواردة بها تمثل المجتمع محل الدراسة بشكل جيد، بمعنى أن الإجابات الواردة بالقائمة تعطي المعلومات التي وضعت من أجلها تلك العبارات (قائمة الإستقصاء تقيس ما وضعت لقياسه)، أي أن معامل الصدق يشير لمدى صدق الأداة، والاعتماد على نتائجها، وهو يساوي الجذر التربيعي لمعامل الثبات (ألفا كرونباخ).

وقد بلغ معامل الثبات ألفا كرونباخ لقائمة الإستقصاء (0.96) الأمر الذي انعكس أثره على الصدق الذاتي (الذي يمثل الجذر التربيعي للثبات)، حيث بلغ (0.98).

ويظهر الجدول التالي رقم معاملي الصدق والثبات لمحاور الدراسة:

جدول رقم (9): معامل الثبات والصدق الذاتي باستخدام معامل ألفا كرونباخ

	محاور الدراسة	عدد العبارات	معامل الثبات	معامل الصدق
الأول	وعي وإدراك فئات عينة الدراسة بمخاطر الأمن السيبراني وطرق مواجهتها بالبنوك المصرية.	19	0.92	0.96
الثاني	دور خصائص تشكيل لجان المراجعة في مواجهة مخاطر الأمن السيبراني بالبنوك المصرية	6	0.87	0.93
الثالث	دور آليات عمل لجان المراجعة في مواجهة مخاطر الأمن السيبراني بالبنوك المصرية	5	0.78	0.88
	إجمالي محاور الدراسة	26	0.92	0.96

المصدر: إعداد الباحث في ضوء نتائج التحليل الإحصائي

وتشير النتائج السابقة إلى أن قائمة الإستقصاء تقيس ما وضعت لقياسه ومن ثم فإنها تمثل مجتمع الدراسة بشكل جيد وبالتالي يمكن الاعتماد على بياناتها في عمل التحليلات والاختبارات الإحصائية اللاحقة.

2/4/4 اختبارات الفروض الإحصائية:

في هذا الجزء من الدراسة سوف يتم عرض نتائج الإحصاءات الوصفية والإحصاءات التحليلية لكل فرض من فروض الدراسة وذلك على النحو التالي:

- الإحصاء الوصفي: تم إجراء الإحصاء الوصفي لعبارات قائمة الاستقصاء عن طريق حساب الوسط الحسابي Mean لقياس متوسط آراء المستقصي منهم، والانحراف المعياري Standard Deviation لقياس التشتت والاهمية النسبية والترتيب، ومن ثم مقارنة قيمة المتوسط الحسابي بقيمة المتوسط المرجح لإجابات عينة البحث في شكل مماثل لمقياس ليكرت الخماسي كما هو موضح بالجدول التالي رقم (10) لمعرفة اتجاه آراء عينة الدراسة، أي معرفة هل النمط السائد للمستقصي منهم يميل نحو الموافقة أم عدم الموافقة.

جدول (10): معايير مقياس ليكرت الخماسي

الفئة	الاتجاه
1.79-1.00	**تميل الإجابات إلى (غير موافق جداً)**
2.59-1.80	**تميل الإجابات إلى (عدم الموافقة)**
3.39-2.60	**تميل الإجابات إلى (محايد)**
4.19-3.40	**تميل الإجابات إلى (الموافقة)**
5.00-4.20	**تميل الإجابات إلى (موافق جداً)**

المصدر: (Pimentel, 2010)

- **الإحصاء التحليلي:** وتشمل قيام الباحث بالتحقق من مدي تتبع البيانات للتوزيع الطبيعي وفي ضوء نتيجة الاختبار تبين للباحث أن بيانات الدراسة لا تتبع التوزيع الطبيعي ومن ثم اتجه الباحث إلى استخدام الاختبارات اللامعلمية لاختبار فروض البحث ومنها اختبار Mann-Whitney لاختبار مدى وجود فروق معنوية بين آراء فئات عينة الدراسة وفقاً لمتغير جهة العمل (العاملين بقطاعالبنوك، أعضاء هيئة التدريس ومعاونيهم).

1/2/4/4 اختبار صحة الفرض الأول:

سوف يتم في هذا الجزء اختبار صحة الفرض الأول كما يلي:

➢**الفرض العدم:** لا توجد فروق معنوية ذات دلالة إحصائية بين أراء عينة الدراسة حول مدي الادراك والوعي بمخاطر الأمن السيبراني وطرق مواجهتها وفقاً لمتغير جهة العمل.

➢**الفرض البديل:** توجد فروق معنوية ذات دلالة إحصائية بين أراء عينة الدراسة حول مدي الادراك والوعي بمخاطر الأمن السيبراني وطرق مواجهتها وفقاً لمتغير جهة العمل.

وسوف يتم اختبار صحة الفرض من خلال الإحصاءات الوصفية والإحصاءات التحليلية وذلك على النحو التالي:

أولاً: الإحصاءات الوصفية

جدول (11): نتائج الإحصاءات الوصفية للفرض الأول

رقم العبارة	المتوسط الحسابي	الانحراف المعياري	الأهمية النسبية	الاتجاه العام	الترتيب
1	4.04	1.05	%81	موافق	3
2	3.90	1.05	%78	موافق	10
3	3.96	0.97	%79	موافق	4
4	3.96	0.97	%79	موافق	5
5	3.64	1.20	%73	موافق	18
6	3.77	1.10	%75	موافق	15
7	3.58	0.99	%72	موافق	19
8	3.76	1.07	%75	موافق	16
9	3.66	0.99	%73	موافق	17
10	3.85	1.04	%77	موافق	12
11	3.86	1.05	%77	موافق	11
12	3.90	1.00	%78	موافق	9
13	3.92	0.93	%78	موافق	7
14	3.92	0.94	%78	موافق	8
15	3.79	1.02	%76	موافق	14
16	3.83	0.88	%77	موافق	13
17	3.96	0.89	%79	موافق	6
18	4.08	0.76	%82	موافق	1
19	4.06	0.79	%81	موافق	2
المتوسط العام لإجمالي المحور	3.87	0.98	%77	موافق	-

المصدر: إعداد الباحث في ضوء نتائج التحليل الإحصائي

تؤكد النتائج بالجدول السابق على أن اتجاهات عينة الدراسة المستقصي منهم على اختلاف فئاتهم قد أظهرت اتجاهاً عاماً نحو الموافقة على وجود وعي وإدراك كاف بمخاطر الأمن السيبراني وكيفية مواجهتها بالبنوك المصرية حيث بلغ المتوسط الحسابي الإجمالي (3.87) بإنحراف معياري يساوى (0.98) وهذا يشير إلى وجود اتفاق بين آراء أفراد العينة على اتجاههم الإيجابي نحو مدى أهمية المحور الأول بأهمية نسبية بلغت (77%).

مما يشير إلى وجود اتفاق كبير حول مخاطر الأمن السيبرانيوطرق مواجهتها والتي يأتي في مقدمتها وجود آليات لتقديم حوافز حكومية من أجل تشجيع بناء القدرات في مجال الأمن السيبرانيبنسبة موافقة بلغت 4.08 وبأهمية نسبية 82% ثم يلي ذلك عدم وجود شراكة بين بنوك القطاع العام وبنوك القطاع الخاص أو تدابير تعاونية سواء اتفاقات ثنائية أو متعددة الأطراف أو دولية بشأن التعاون في مجال الأمن السيبرانيبنسبة موافقة بلغت 4.06 وبأهمية نسبية 81% وفي المرتبة الأخيرة عدم وجود تشريعات أو لوائح كافية تتناول بالتفصيل حماية الخصوصية والتوقيعات الرقمية والمعاملات الإلكترونية بنسبة موافقة بلغت 3.58 وبأهمية نسبية 72%.

ثانياً: الإحصاءات التحليلية

جدول (12): نتائج تطبيق اختبار Mann-Whitneyلاختبار الفرض الأول

رقم العبارة	Mann-Whitney	Z	Sig.	الدلالة الاحصائية
1	11462.0	6.839-	0.0	فروق معنوية
2	11490.0	6.789-	0.0	فروق معنوية
3	10995.0	7.366-	0.0	فروق معنوية
4	12022.5	6.288-	0.0	فروق معنوية
5	13309.5	4.922-	0.0	فروق معنوية
6	14426.5	3.879-	0.0	فروق معنوية
7	17590.5	826.-	0.4	فروق غير معنوية
8	12160.5	6.105-	0.0	فروق معنوية
9	15332.5	3.024-	0.0	فروق معنوية
10	10553.5	7.634-	0.0	فروق معنوية
11	12714.5	5.524-	0.0	فروق معنوية
12	12043.0	6.175-	0.0	فروق معنوية
13	12015.5	6.393-	0.0	فروق معنوية
14	13174.0	5.149-	0.0	فروق معنوية
15	14818.0	3.494-	0.0	فروق معنوية
16	14621.0	3.708-	0.0	فروق معنوية
17	13682.0	4.679-	0.0	فروق معنوية
18	15708.0	2.716-	0.0	فروق معنوية
19	15373.0	3.029-	0.0	فروق معنوية

المصدر: إعداد الباحث في ضوء نتائج التحليل الإحصائي

تشير نتائج الجدول السابق إلى وجود فروق معنوية بين متوسطات الرتب في جميع العبارات الخاصة بمدي الادراك والوعي بمخاطر الأمن السيبراني وطرق مواجهتها لصالح العاملين بقطاع البنوك حيث تقل الدلالة الإحصائية عن نسبة (0.05) باستثناء العبارة رقم (7) والخاصة بـعدم وجود تشريعات أو لوائح كافية تتناول بالتفصيل حماية الخصوصية والتوقيعات الرقمية والمعاملات الإلكترونية حيث يوجد اتفاق عليها حيث تزيد الدلالة الإحصائية عن نسبة (0.05).

وبناءً على ما سبق فإن النتائج السابقة ترجح قبول الفرض البديل القائل بأنهتوجد فروق معنوية ذات دلالة إحصائية بين أراء عينة الدراسة حول مدي الادراك والوعي بمخاطر الأمن السيبراني وطرق مواجهتها وفقاً لمتغير جهة العمل.

2/2/4/4 اختبار صحة الفرض الثاني:

سوف يتم في هذا الجزء اختبار صحة الفرض الثاني كما يلي:

- **الفرض العدم:** لا توجد فروق معنوية ذات دلالة إحصائية في أراء عينة الدراسة حول دور خصائص تشكيل لجان المراجعة في تعزيز قدرة البنوك المصرية على مواجهة مخاطر الأمن السيبراني وفقاً لمتغير جهة العمل.

- **الفرض البديل:** توجد فروق معنوية ذات دلالة إحصائية في أراء عينة الدراسة حول دور خصائص تشكيل لجان المراجعة في تعزيز قدرة البنوك المصرية على مواجهة مخاطر الأمن السيبراني وفقاً لمتغير جهة العمل.

وسوف يتم اختبار صحة الفرض من خلال الإحصاءات الوصفية والإحصاءات التحليلية وذلك على النحو التالي:

أولاً: الإحصاءات الوصفية

جدول (13): نتائج المقاييس الوصفية للفرض الثاني

رقم العبارة	المتوسط الحسابي	الانحراف المعياري	الأهمية النسبية	الاتجاه العام	الترتيب
20	3.9639	0.97	%79	موافق	1
21	3.9613	0.97	%79	موافق	2
22	3.6418	1.20	%73	موافق	5
23	3.7680	1.10	%75	موافق	3
24	3.5799	0.99	%72	موافق	6
25	3.7552	1.07	%75	موافق	4
المتوسط العام لإجمالي المحور	3.78	1.05	%76	موافق	-

المصدر: إعداد الباحث في ضوء نتائج التحليل الإحصائي

ومن الجدول السابق يتضح الاتي:

قام الباحث بحساب المؤشر العام المعبر عن كافة عبارات المحور الثاني، وتبين أن متوسط آراء أفراد العينة بلغ (3.78) بإنحراف معياري يساوى (1.05) وهذا يشير إلى وجود اتفاق بين آراء أفراد العينة على اتجاههم الإيجابي نحو مدى أهمية المحور الثاني بأهمية نسبية بلغت (76%).

مما يشير إلى وجود اتفاق كبير حول دور خصائص تشكيل لجان المراجعة في تعزيز قدرة البنوك المصرية على مواجهة مخاطر الأمن السيبراني والتي يأتي في مقدمتها تشكيل لجان المراجعة من عدد مناسب من الأعضاء غير التنفيذيين بمجلس الإدارة يساعد البنك على الحد من مخاطر الأمن السيبراني بنسبة موافقة بلغت 3.96 وبأهمية نسبية 79% ثم يلي ذلك اناستقلالية أعضاء لجان المراجعة تؤثر بشكل إيجابي في قدرة لجنة المراجعة على التقرير عن مخاطر الأمن السيبراني التي تواجه البنك والافصاح عن أوجه القصور في أداء إدارة البنك بنسبة موافقة بلغت 3.96 وبأهمية نسبية 79% وفي المرتبة الأخيرة يأتي دور بذل العناية المهنية الواجبة من قبل لجان المراجعة يؤدي إلى تحسين أدائها في مواجهة مخاطر الأمن السيبراني بالبنوك المصرية بنسبة موافقة بلغت 3.58 وبأهمية نسبية 72%.

ثانياً: الإحصاءات التحليلية

جدول (14): نتائج تطبيق اختبار Mann-Whitney لاختبار الفرض الثاني

رقم العبارة	Mann-Whitney	Z	Sig.	الدلالة الاحصائية
20	10995.0	7.4-	0.0	فروق معنوية
21	12022.5	6.3-	0.0	فروق معنوية
22	13309.5	4.9-	0.0	فروق معنوية
23	14426.5	3.9-	0.0	فروق معنوية
24	17590.5	0.8-	0.0	فروق معنوية
25	12160.5	6.1-	0.0	فروق معنوية

المصدر: إعداد الباحث في ضوء نتائج التحليل الإحصائي

تشير نتائج الجدول السابق إلى وجود فروق معنوية بين متوسطات الرتب في جميع العبارات الخاصة بدور خصائص تشكيل لجان المراجعة في تعزيز قدرة البنوك المصرية على مواجهة مخاطر الأمن السيبراني لصالح العاملين بقطاع البنوك حيث تقل الدلالة الإحصائية عن نسبة (0.05).

وبناءً على ما سبق فإن النتائج السابقة ترجح قبول الفرض البديل القائل بأنه توجد فروق معنوية ذات دلالة إحصائية في أراء عينة الدراسة حول دور خصائص تشكيل لجان المراجعة في تعزيز قدرة البنوك المصرية على مواجهة مخاطر الأمن السيبراني وفقاً لمتغير جهة العمل.

3/2/4/4 اختبار صحة الفرض الثالث:

سوف يتم في هذا الجزء اختبار صحة الفرض الثالث كما يلي:

- **الفرض العدم:** لا توجد فروق معنوية ذات دلالة إحصائية في أراء عينة الدراسة حول دور آليات عمل لجان المراجعة في تعزيز قدرة البنوك المصرية على مواجهة مخاطر الأمن السيبراني وفقاً لمتغير جهة العمل.
- **الفرض البديل:** توجد فروق معنوية ذات دلالة إحصائية في أراء عينة الدراسة حول دور آليات عمل لجان المراجعة في تعزيز قدرة البنوك المصرية على مواجهة مخاطر الأمن السيبراني وفقاً لمتغير جهة العمل.

وسوف يتم اختبار صحة الفرض من خلال الإحصاءات الوصفية والإحصاءات التحليلية وذلك على النحو التالي:

أولاً: الإحصاءات الوصفية

جدول (15): نتائج المقاييس الوصفية للفرض الثالث

العبارة	المتوسط الحسابي	الانحراف المعياري	الأهمية النسبية	الاتجاه العام	الترتيب
26	3.6572	0.99	%73	موافق	5
27	3.8454	1.04	%77	موافق	4
28	3.8582	1.05	%77	موافق	3
29	3.9046	1.00	%78	موافق جدا	2
30	3.9227	0.93	%78	موافق	1
المتوسط العام لإجمالي المحور	3.8376	1.00	%77	موافق	-

المصدر: إعداد الباحث في ضوء نتائج التحليل الإحصائي

ومن الجدول السابق يتضح الاتي:

قام الباحث بحساب المؤشر العام المعبر عن كافة عبارات المحور الثالث، وتبين أن متوسط آراء أفراد العينة بلغ (3.84) بإنحراف معياري يساوى (1) وهذا يشير إلى وجود اتفاق بين آراء أفراد العينة على اتجاههم الإيجابي نحو مدى أهمية المحور الثالث بأهمية نسبية بلغت (77%).

ومما يشير إلى وجود اتفاق كبير حول دور آليات عمل لجان المراجعة في تعزيز قدرة البنوك المصرية على مواجهة مخاطر الأمن السيبراني، وقد كان من أكثر العبارات موافقة في الإجابة على الترتيب: عبارة رقم (30)، عبارة رقم (29) وذلك بأهمية نسبية مقدارها (78%) لكل منهما، كما يتضح من الجدول أيضاً أن أقل العبارات التي حازت على أقل موافقة في الإجابة على الترتيب: عبارة رقم (27) وعبارة رقم (26) وذلك بأهمية نسبية مقدارها (77%) و(73%)، وفقاً لردود مفردات عينة الدراسة.

ثانياً: الإحصاءات التحليلية

جدول (16): نتائج تطبيق اختبار Mann-Whitney لاختبار الفرض الثالث

رقم العبارة	Mann-Whitney	Z	Sig.	الدلالة الاحصائية
26	15332.50	3.02-	0.0	فروق معنوية
27	10553.50	7.63-	0.0	فروق معنوية
28	12714.50	5.52-	0.0	فروق معنوية
29	12043.00	6.17-	0.0	فروق معنوية
30	12015.50	6.39-	0.0	فروق معنوية

المصدر: إعداد الباحث في ضوء نتائج التحليل الإحصائي

تشير نتائج الجدول السابق إلى وجود فروق معنوية بين متوسطات الرتب في جميع العبارات الخاصة بدور آليات عمل لجان المراجعة في تعزيز قدرة البنوك المصرية على مواجهة مخاطر الأمن السيبراني لصالح العاملين بقطاع البنوك حيث تقل الدلالة الإحصائية عن نسبة (0.05).

وبناءً على ما سبق فإن النتائج السابقة ترجح قبول الفرض البديل القائل بأنهتوجد فروق معنوية ذات دلالة إحصائية في أراء عينة الدراسة حول دور آليات عمل لجان المراجعة في تعزيز قدرة البنوك المصرية على مواجهة مخاطر الأمن السيبراني وفقاً لمتغير جهة العمل.

5/ نتائج الدراسة:

هدفت هذه الدراسة إلى تعزيزدورلجان المراجعة لمواجهة مخاطر الأمن السيبراني في قطاع البنوك المصرية، وذلك عن طريق تحديد مخاطر الأمن السيبراني وتأثيراتها، ودور لجان المراجعة في هذا المجال. واستخدمت الدراسة أسلوب التحليل النظري للتعرف على مخاطر الأمن السيبراني وما يترتب عليها من خسائر على مستوى البنوك المصرية وعلى المستوى القومي، وتحديد أهم الجهود الدولية والمحلية في مجال مواجهة مخاطر الأمن السيبراني، بالإضافة إلى دور لجان المراجعة في مواجهة مخاطر الأمن السيبراني.

وتوصلت الدراسة في جانبها النظري إلى ما يلي:

أ. أثبتت الدراسات السابقة وجود زيادة مستمرة في مخاطر الأمن السيبراني، وتسبب الهجمات السيبرانية في أضرار وخسائر كبيرة لمنظمات الأعمال والاقتصاد القومي؛ كما تناولت دور لجان المراجعة كخط دفاع في مواجهة مخاطر الأمن السيبراني، وطرحت مجموعة من العوامل اللازمة للقيام بهذا الدور بشكل فعال.

ب. يهدف الأمن السيبراني إلى المساعدة على حماية أصول المنظمات ومواردها من النواحي التنظيمية والبشرية والمالية والتقنية والمعلوماتية، ويسمح لها بمواصلة مهماتها. وهدفه الأسمى هو أن يضمن عدم تضررها ضرراً دائماً، ويتمثل ذلك في تقليل احتمالات سوء الأداء أو ظهور أي تهديد والحد من الأضرار الناجمة عنها، وضمان رجوع العمليات العادية إلى حالتها السابقة خلال إطار زمني مقبول وبتكلفة مقبولة في أعقاب وقوع حادث أمني.

ج. لإنشاء منظومة متكاملة للأمن السيبراني، من المهم التحديد الدقيق للأصول والموارد اللازمة للوقاية الفعالة؛ الأمر الذي يتطلب نهجاً عالمياً للأمن، نهجاً متعدد التخصصات وشاملاً على مجموعة من الإجراءات والقواعد التي يجب أن تكون متوافقة مع التوجيهات والمعايير الدولية القياسية.

د. كان للبنك المركزي المصري رؤية استراتيجية شاملة ونهج مرن وفعال من أجل التعامل مع تحديات الأمن السيبراني المعقدة الناشئة عن التوصيل البيني واسع النطاق للأنظمة والشبكات، وتزايد الارتباط بين البُنى التحتية والاعتماد على التكنولوجيات الرقمية والتهديدات والمخاطر.

وتوصلت الدراسة في جانبها الميداني إلى ما يلي:

أ. توجد فروق معنوية ذات دلالة إحصائية بين أراء عينة الدراسة ولصالح العاملين بقطاع البنوك حول مدي الادراك والوعي بمخاطر الأمن السيبراني وطرق مواجهتها وفقاً لمتغير جهة العمل.

ب. توجد فروق معنوية ذات دلالة إحصائية في أراء عينة الدراسةولصالح العاملين بقطاع البنوك حول دور خصائص تشكيل لجان المراجعة في تعزيز قدرة البنوك المصرية على مواجهة مخاطر الأمن السيبراني وفقاً لمتغير جهة العمل

ج. توجد فروق معنوية ذات دلالة إحصائية في أراء عينة الدراسةولصالح العاملين بقطاع البنوك حول دور آليات عمل لجان المراجعة في تعزيز قدرة البنوك المصرية على مواجهة مخاطر الأمن السيبراني وفقاً لمتغير جهة العمل.

6. التوصيات:

في ضوء نتائج البحث يوصي الباحث بما يلي:

أ. زيادة الاهتمام بتوعية العاملين بقطاع البنوك بأهمية الأمن السيبراني حتى يتسنى لهم مواجهة التحديات والمخاطر الناتجة عن بيئة تكنولوجيا المعلومات.

ب. إعداد برامج توعية مجتمعية للمواطنين للتعرف على أهمية الأمن السيبراني حتى يتسنى لهم مواجهة التحديات والمخاطر الناتجة عن الهجمات الالكترونية.

ج. تطوير البنية التحتية السيبرانية داخل المؤسسات المصرفية للحد من الاختراق والتجسس والقرصنة الإلكترونية.

د. ضرورة إنشاء إدارة للتطبيقات الإلكترونية لمراجعة كل جديد واختباره قبل إطلاقه بالسوق

ه. ضرورة تقييم المؤسساتالمصرفية بشكل دوري ووضع خطط لعلاج الثغرات الموجودة بها ومتابعة تنفيذها

و. ضرورة إطلاق مبادرة التدريب على أمن المعلومات بالتعاون مع المؤسسات المصرفية.

ز. ضرورة إنشاء مركز متخصص لمواجهة التهديدات ومخاطر الأمن السيبراني في مصر

ح. ضرورة تجهيز معامل في مجال الهندسة العكسية للبرامج الضارة وللتصدي للهجمات المحتملة

ط. ضرورة تجهيز فريق لاكتشاف الثغرات الموجودة في المؤسسات المصرفية

7/ مقترحات الدراسات المستقبلية:

أ. أثر الأمن السيبراني على سمعة البنوك المصرية.

ب. أثر تطبيق إطار عمل COBIT5 في الحد من تهديدات أمن نظم المعلومات المحاسبية الآلية في البنوك المصرية

ج. أثر حوكمة الأمن السيبراني على فعالية المعاملات الإلكترونية في البنوك المصرية.

المراجع

8/ 1 المراجع العربية

1. أبو الخير، محمد حارس محمد طه (2023)، "أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الاستقرار المالي في البنوك الالكترونية: دراسة ميدانية"، **المجلة العلمية للدراسات والبحوث المالية والإدارية**، المجلد رقم (15)، العدد الأول، 1-65.
2. البغدادي، مروة فتحي السيد (2021)، "اقتصاديات الأمن السيبراني في القطاع المصرفي"، **مجلة البحوث القانونية والاقتصادية**، العدد رقم (76)، 1446- 1513.
3. الخرينج، نواف متعب بن يهمتعب، البسطويسي، مروة أحمد عبد الرحمن، وداود، ياسر إبراهيم محمد (2022)، "دور حوكمة تكنولوجيا المعلومات في إدارة المخاطر السيبرانية للقطاع المصرفي" ، **المجلة العلمية للدراسات والبحوث المالية والإدارية**، المجلد رقم (13)، 1715- 1743.
4. الشواربي، محمد عبدالمنعم (2018)، "دور دوران أعضاء لجان المراجعة فى تحقيق فعالية لجنة المراجعة وأثر ذلك على أتعاب المراجعة الخارجية"، **الفكر المحاسبي**، المجلد رقم (22)، العدد رقم (7)، 269-327.
5. القرموطي، شيماء محمد السعيد (2019)، "تعزيز لجان المراجعة بغرض زيادة فاعلية حوكمة الشركات"، **مجلة الاسكندرية للبحوث المحاسبية**، المجلد الرابع، العدد الثالث،1-30.
6. امانى، احمد وهبه يوسف، (2022)، "واقع الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وأثره على قرارات الاستثمار ومنح الائتمان في البورصة: دراسة تطبيقية"، **المجلة العلمية للدراسات التجارية والبيئية**، المجلد رقم (13)، العدد الثاني،28-109.
7. زيود، لطيف، نصور، ريم محمد، وعلي، حسين (2014)، "تحديد مستوى حوكمة تكنولوجيا المعلومات المطبق في المصرف التجاري السوري بالاذقية وفق إطار عمل (COBIT)"، **مجلة جامعة تشرين للبحوث والدراسات العلمية ـ سلسلة العلوم الإقتصادية والقانونية**، المجلد رقم (36)، العدد الثاني، 189-210.
8. غلام الله، جبالي عياد(2020)، "لجان التدقيق ودورها في المؤسسة في ظل التطور السريع لفضاء الجريمة الإلكترونية"، **مجلة اقتصادات شمال افريقيا**، المجلد رقم (16)، العدد رقم (23)،543-566.

9. محروس، رمضان عارف رمضان (2022)، "استخدام المنهجية الرشيقة في تطوير أداء المراجعة الداخلية لمواجهة مخاطر الأمن السيبراني"، **مجلة البحوث المالية والتجارية**، العدد الثالث، 142-491.

10. هاشم، أماني هاشم السيد حسن (2012)، "تفعيل دور لجان المراجعة في الحد من المخاطر المصرفية الإلكترونية: دراسة ميدانية"، **مجلة التجارة والتمويل**، العدد الأول، 301-367.

8/2 Bibliography:

11. Adrian, f. X., andwang, g. (2023), "Measure the level capability it governance in effectiveness internal control for cybersecurity using the cobit 2019 in organization: banking company", **Journal of theoretical and applied information technology**, Vol. 101, No. 5,1710: 1723.

12. Akintoye, R., Ogunode, O., Ajayi, M., and Joshua, A. A. (2022),"Cyber security and financial innovation of selected deposit money banks in Nigeria", **universal Journal of Accounting and Finance**, Vol. 10, No. 3, 643-652.

13. Al-Alawi, A. I., and Al-Bassam, M. S. A. (2020),"The significance of cybersecurity system in helping managing risk in banking and financial sector", **Journal of Xidian University**, Vol. 14, No. 7, 1523-1536.

14. Al-Alawi, A. I., and Al-Bassam, S. A. (2019),"Assessing the Factors of Cybersecurity Awareness in the Banking Sector", **Arab Gulf Journal of Scientific Research**, Vol. 37, No. 4, 17-32.

15. Alazab, M., RM, S. P., Parimala, M., Maddikunta, P. K. R., Gadekallu, T. R., and Pham, Q. V. (2021),"Federated learning for cybersecurity: concepts, challenges, and future directions", **IEEE Transactions on Industrial Informatics**, Vol. 18, No. 5, 3501-3509.

16. Al-Khasawneh, R. O., andRazouk, S. (2023),"Internal Control System on Using Digital Banking Applications and Services in Jordanian Banks During the Corona Virus Pandemic",**Digitalisation: Opportunities and Challenges for Business**, Vol. 1, 849-865.
17. Association of Healthcare Internal Auditors (AHIA) and Deloitte (2017), "Cyber assurance: How internal audit, compliance and information technology can fight the good fight together?", available at: https://bit.ly/4482YXY.
18. Badawy, H. A. E. S. (2020),"Audit Committee Effectiveness and Corporate Sustainable Growth: The Case of Egypt",**Alexandria Journal of Accounting Research**, Vol. 4, No. 2, 537-578.
19. Bepari, M. K. (2023),"Audit committee characteristics and Key Audit Matters (KAMs) disclosures", **Journal of Corporate Accounting and Finance**, Vol. 34, No. 1, 152-172.
20. Cerin, B. (2020),"Cyber Security Risk is a Board-Level Issue",**43rd International Convention on Information, Communication and Electronic Technology (MIPRO)**, 384-388.
21. Clinton, L. (2017),"Cyber-Risk Oversight: Directors Handbook Series", Internet Security Alliance, available at: https://bit.ly/3pzoOor.
22. Dezoort, F., Todd, H.R., Dana, A.D., Reed, A.S. (2002), "Audit committee effectiveness: Asynthesis of the empirical audit committee literature",**Journal of Accountancy Literature**, Vol. 21, 38-75.
23. Duvenhage, M. F., Smit, A., and Botha, M. (2022),"Cyber Security Disclosure inthe Banking Sector: A Case of South Africa and China",**International Business Conference,** 1485-1450.

24. El-Masry, E.E., Hansen, K.A., (2008),"Factors affecting auditors' utilization of evidential cues",**Taxonomy and future research directions, Managerial Audit**, Vol. 23, No. 1, 26–50.

25. Endsley, M. R., and Garland, D. J. (2000),"Theoretical underpinnings of situation awareness: A critical review", **Situation awareness analysis and measurement**, Vol. 1, No. 1, 3-21.

26. Fariha, R., Hossain, M. M., and Ghosh, R. (2022),"Board characteristics, audit committee attributes and firm performance: empirical evidence from emerging economy", **Asian Journal of Accounting Research**, Vol. 7, No. 1, 84-96.

27. Galligan, M. (2014),"For Audit Committees, a Growing Role in Cybersecurity", **Risk and Compliance Journal**, vol. 16, 1-4.

28. Gatzert, N., and Schubert, M. (2022), "Cyber risk management in the US banking and insurance industry: A textual and empirical analysis of determinants and value", **Journal of Risk and Insurance**, Vol. 89, No. 3, 725-763.

29. Gbenyi, G. T., Tsegba, I. N., andDuenya, M. I. (2023), "Audit Committee Attributes and Share Price Reaction of Listed Deposit Money Banks in Nigeria", **Asian Journal of Economics, Business and Accounting**, Vol. 23, No. 4, 1-16.

30. Institute of Internal Auditors (IIA) (2016), "Assessing cybersecurity risk: roles of the three lines of defense", available at: https://bit.ly/3NsUC6k.

31. Institute of Internal Auditors (IIA) (2020), "The IIA's three lines model. An update of the Three Lines of Defense", available at: https://bit.ly/3PFAP6h.

32. IT Governance Institute (2006), "IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control over Financial Reporting", available at:https://bit.ly/46v9IRv

33. IT Governance Institute (2007), "Control Objectives for Information and Related Technology". available at:https://bit.ly/3K42ESr

34. Johnson, A. L. (2016),"Cybersecurity for financial institutions: The integral role of information sharing in cyber-attack mitigation", NC Banking Inst., Vol. 20, 277.

35. Johri, A., and Kumar, S. (2023),"Exploring Customer Awareness towards Their Cyber Security in the Kingdom of Saudi Arabia: A Study in the Era of Banking Digital Transformation", Human Behavior and Emerging Technologies, 2023.

36. Kahyaoglu, S.B., Çaliyurt, K., (2018),"Cybersecurity assurance process from the internal audit perspective",**Managerial Audit**. Vol. 33, No. 4, 360–376.

37. Kartal, M. T., İbiş, C., andÇatıkkaş, Ö. (2018),"Adequacy of audit committees: A study of deposit banks in Turkey", **Borsa İstanbul Review**, Vol. 18, No. 2, 150-165.

38. Katz, D. A., and McIntosh, L. A. (2012),"Cybersecurity Risks and the Board of Directors",**New York Law Journal**.

39. KPMG. (2023), "Cyber security for audit committees", available at: https://bit.ly/3JIxPCl.

40. Krishnasamy, V., andVenkatachalam, S. (2021),"An efficient data flow material model based cloud authentication data security and reduce a cloud storage cost using Index-level Boundary Pattern Convergent Encryptionalgorithm",Materials Today: Proceedings.

41. Lemmon, M. L., andLins, K. V. (2003),"Ownership structure, corporate governance, and firm value: Evidence from the East Asian financial crisis", **The journal of finance**, Vol. 58, No. 4, 1445-1468.

42. Liu, P. Y., and Chin, C. L. (2023),"Are banking and accounting expertise on the audit committee related to bank loan terms?", **Journal of Corporate Accounting and Finance**, Vol. 34, No. 1, 191-213.

43. Mazumder, M. M. M., and Hossain, D. M. (2023),"Voluntary cybersecurity disclosure in the banking industry of Bangladesh: does board composition matter?",**Journal of Accounting in Emerging Economies**, Vol. 13, No. 2, 217-239.

44. McGrath, V., Sheedy, E. A., and Yu, F. (2022), "Governance of Cyber Security: State of Play", **SSRN Electronic Journal** Available at:**https://bit.ly/3JC1q0n.**

45. Ojeka, S. A., Ben-Caleb, E., andEkpe, E. O. I. (2017),"Cyber Security in the Nigerian Banking Sector: An Appraisal of Audit Committee Effectiveness", **International Review of Management and Marketing**, Vol. 7, No. 2, 340-346.

46. Pelletier, J. (2020), "Three tips for better audit communications", available at: https://bit.ly/43gOSmc

47. Pimentel, J. L. (2010). "A note on the usage of Likert Scaling for research data analysis", USM RandD Journal, vol. 18, No. 2, p. 109-112.

48. Putte, Vande D., andVerhelst, M. (2014),"Cybercrime: Can a standard risk analysis help in the challenges facing business continuity managers?",**Journal of business continuity and emergency planning**, Vol. 7, No. 2,126-137.

49. Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D., and Moore, A. (2005),"Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector. Pittsburgh", PA: Carnegie Mellon.

50. Shamsuddin, a., adam, m. A., adnan, s. A., andyasin, y. M. (2018), "The effectiveness of internal audit functions in managing cybersecurity in malaysia'sbanking institutions", **International Journal of Industrial Management**,
Vol. 4, 61-69.

51. Thiéry, S., andFass, D. (2020),"Cybersecurity risks and situation awareness: Audit committees' appraisal", In Advances in Human Factors in Cybersecurity: AHFE 2020 Virtual Conference on Human Factors in Cybersecurity, USA, Springer International Publishing, 83-87.

52. Vuko, T., Slapničar, S., Čular, M., andDrašček, M. (2020),"How effective is cyber security assurance by internal auditors?",**SSRN Electronic Journal**, available at: https://bit.ly/3XDYshx.

53. Yew, S., Gan, T., Leong, K., Houw, T., and Lim, D. (2015),"Cybersecurity: The changing role of audit committee and internal audit".

54. Yıldırım, İ. (2019),"Cyber Risk Management in Banks: Cyber Risk İnsurance", Global cyber security labor shortage and international business risk, 38-50.

Abstract:

The study aims to enhance the role of audit committees as one of the governance mechanisms to facecybersecurity risks in Egyptian banks. In order to achieve the objectives of the study and test its hypotheses, the researcher designed a theoretical and a field study, where the theoretical study included three axes, in which the researcher dealt with the general framework of the study, cybersecurity risks, and ways to face them in Egyptian banks, and previous studies related to the research problem.

In order to test the validity of the study hypotheses, the researcher designed a field study where the researcher dealt with the survey list, which consisted of three main axes, and the size of the study sample was (388) responses were randomly selected from the study community, and statistical tests and analyzes were conducted.

The theoretical study found that cybersecurity dangers continue to rise, and that cyber-attacks result in significant harm and financial losses for businesses and the global economy. Cybersecurity also helps organizations protect their assets and resources from the organizational, human, financial, technical, and informational aspects and allows them to continue their missions. Its primary objective is to prevent permanent damage, to minimize the likelihood of nonperformance or the emergence of any threat, and to limit the damage resulting from it, as well as to ensure that normal operations are restored within a reasonable time and at a reasonable price after a security incident.

The field study concluded that all hypotheses of the study were rejected. The results of the statistical analysis showed that there were statistically

significant differences between the mean ranks of the study sample according to the variable of the employer. These differences were in favor of workers in the banking sector, regarding their opinions about cybersecurity risks and ways to confront them. Also, their opinions about the role of the characteristics of Audit committees and its mechanisms in enhancing the ability of Egyptian banks to face cybersecurity risks.

In the end, the researcher suggested a set of recommendations, including increasing interest in educating workers in the banking sector about the importance of cybersecurity so that they can face the challenges and risks resulting from the information technology environment. He also recommended preparing community awareness programs for citizens to learn about the importance of cybersecurity. In addition to developing cyber infrastructure within banking institutions to reduce from penetration, espionage and electronic piracy, and a management of electronic applications must be established to review and test everything new before launching it in the market. The systems of banking institutions must be evaluated periodically and plans to remedy the gaps in them and follow up on their implementation.

Keywords: audit committees, cybersecurity, cybersecurity risks, ways to face cybersecurity risks.