مجلة البحوث المالية والتجارية
المجلد (23) – العدد الثالث – يوليو 2022

أثر جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني وإنعكاساته على ترشيد قرارات المستثمرين

(دراسة ميدانية)

The impact of internal audit quality in reducing cybersecurity risks and its repercussions on rationalizing investor decisions

(Empirical Study)

دكتور: جيهان عادل أميرهم

مدرس المحاسبة

كلية التجارة – جامعة بورسعيد

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

الملخص :

يهدف البحث إلى دراسة وإختبار أثر جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني وإنعكاساته على ترشيد قرارات المستثمرين ، ولتحقيق هدف البحث تم إجراء دراسة ميدانية على عينة من مسئولي المراجعة الداخلية ، مسئولي تكنولوجيا المعلومات ، مسئولي إدارة المخاطر ، المستثمرين (من خلال شركات وساطة وتداول الأوراق المالية) في شركات الإتصالات المقيدة في سوق الأوراق المصرية .

وقد توصلت الدراسة إلى مجموعة من النتائج النظرية والعملية لعل أهمها : لن يستطيع أصحاب المصالح وخاصة المستثمرين متابعة عمليات المخاطر السيبرانية إلا بمساعدة المراجعة الداخلية ، كما أثبتت نتائج الدراسة الميدانية أيضاً بناء على تحليل إستجابات مفردات المجموعات الأربعة لعينة الدراسة فيما يتعلق بإختبار الفرض الثاني حيث تشير النتائج إلى أنه لا توجد فروق معنوية بين آراء مسئولي المراجعة الداخلية ، مسئولي تكنولوجيا المعلومات ، مسئولي إدارة المخاطر ، المستثمرين (من خلال شركات وساطة وتداول الأوراق المالية) حيث كان مستوى المعنوية أكبر من 0.05 وبالتالي إتفاق المجموعات الأربعة على وجود علاقة بين الحد من مخاطر الأمن السيبراني وترشيد قرارات المستثمرين ، مما يعني قبول الفرض الثاني .

وفي النهاية أوصت الدراسة بالعديد من التوصيات كان أهمها : على المراجع الداخلي أن يُعيد تأهيل ذاته بمهارات وقدرات تؤهله لكي يكون شريكاً إستراتيجياً مضيفاً للقيمة ومرشداً لقرارات أصحاب المصالح وخاصة المستثمرين .

الكلمات المفتاحية : جودة المراجعة الداخلية – الحد من مخاطر الأمن السيبراني – ترشيد قرارات المستثمرين .

Abstract :

The research aims to study and test the impact of internal audit quality in reducing cybersecurity risks and its repercussions on rationalizing investors' decisions. Securities) in telecommunications companies listed in the Egyptian stock market.

The study reached a set of theoretical and practical results, perhaps the most important of which are: stakeholders, especially investors, will not be able to follow up on cyber risk operations without the help of the internal audit. There are no significant differences between the opinions of internal audit officials, information technology officials, risk management officials, and investors (through brokerage and stock trading companies) where the level of morale was greater than 0.05 and therefore the four groups agreed on the existence of a relationship between reducing cybersecurity risks And rationalizing investors' decisions, which means accepting the second hypothesis.

In the end, the study recommended several recommendations, the most important of which were: The internal auditor should rehabilitate himself with skills and capabilities that qualify him to be a value-adding strategic partner and a guide to the decisions of stakeholders, especially investors.

Keywords: Internal Audit Quality - Reducing Cyber Security Risks - Rationalizing Investor Decision .

المحور الأول : الإطار العام للبحث .

1/1 مقدمة :

تزامناً مع التحول الرقمي ودخول التكنولوجيا الرقمية في مجال الأعمال زادت التحديات والتهديدات وخاصة فيما يتعلق بمخاطر الأمن السيبراني Cyber Security(CS) والتي تتمثل في مجموعة المخاطر التكنولوجية والتشغيلية والتنظيمية التي تتعرض لها المنشآت المستندة على تقنيات تكنولوجيا المعلومات الحديثة ، والتي قد تنشأ نتيجة إختراق نظام الأمن السيبراني بالمنشأة بما يحد من قدرتها على تحقيق أهدافها المنشودة (Badawy, 2021, p.7) ، وكنتيجة حتمية لحاجة بيئة الأعمال إلى تكيف أدواتها والسعي الدائم نحو الحد من مخاطر الأمن السيبراني والذي هو في الأساس عملية ضمان وسلامة الفضاء السيبراني من التهديدات يمكن أن تلعب وظيفة المراجعة الداخلية دوراً هاماً في تقييم الاضطرابات السيبرانية وتوفير توكيد فيما يتعلق بأمن المعلومات ، وفي تكوين رؤي حول كيفية تحسين وحوكمة أمن معلومات المنشأة وتنسيق جهود إدارة المخاطر .

وفي سياق متصل ترتبط جودة وظيفة المراجعة الداخلية بتقديم مساهمات في القضايا الإستراتيجية داخل المنشأة وخاصة فيما يتعلق بقضايا الأمن السيبراني ، حيث أن المراجعة الداخلية تمثل أحد الدعائم الرئيسية لتلبية إحتياجات مختلف أصحاب المصالح وخاصة المستثمرين ، وذلك من خلال إعدادها لتقرير عن مدى فعالية هيكل الرقابة الداخلية ، وتوفيرها نظرة أكثر شمولية عن أداء مختلف إدارات وأقسام ومراكز المنشأة والمخاطر التي تواجهها ، فضلاً عن قدرتها على متابعة قرارات مجالس الإدارات (شحاتة ، 2020، ص ص 109 – 115 ;PWC, 2018)

ومن ثم فإن هذا البحث يستهدف إستكشاف دور جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني وإنعكاساته على ترشيد قرارات المستثمرين ، وتحقيقاً لهدف البحث سوف تعتمد الباحثة على المنهج التحليلي لأهم الإصدارات المهنية والدراسات ذات الصلة بموضوع البحث

وإختبار فروض البحث من خلال دراسة ميدانية سوف يتم إجرائها من خلال إستمارة إستبيان موزعة على مجموعة من الفئات المستهدفة مع إستخدام الأساليب الإحصائية المناسبة والإشارة إلى مجالات البحث المحاسبي .

وفي هذا الشأن فقد إهتمت العديد من الدراسات السابقة بدور المراجعة الداخلية في الحد من مخاطر الأمن السيبراني ، حيث تنوعت هذة الدراسات بين العربية والأجنبية ، ولعل أهم هذه الدراسات ما جاء بدراسة كل من (عثمان ، 2022 ، ص ص 4-13 ,.sergeja et al ., 2022 ; Pp.1-21) حيث هدفت كل منهما إلى إلقاء الضوء وإستكشاف فعالية دور المراجعة الداخلية في مراجعة الأمن السيبراني والحصول على دليل مستقل وموضوعي على الإلتزام بسياسات الأمن السيبراني ، وتوفير توكيد لمجلس الإدارة في تنفيذ مسئولياتهم المتعلقة بحوكمة الأمن السيبراني ، وقد إعتمدت الدراستان على تحليل أهم الإصدارات المهنية والدراسات السابقة ذات الصلة بفعالية الدور الاستشاري والتوكيدي لوظيفة المراجعة الداخلية في عمليات إدارة مخاطر الأمن السيبراني ومحددات فعالية هذا الدور ، وقد إنتهت الدراستان إلى أن وظيفة المراجعة الداخلية تلعب دوراً رئيسياً وفعالاً في تقييم الإضطرابات السيبرانية وتوفير توكيد فيما يتعلق بأمن المعلومات وفي تكوين رؤي حول كيفية تحسين وحوكمة أمن المعلومات وجهود إدارة المخاطر وتزويد الإدارة ولجنة المراجعة بتوكيد مستقل يفيد بأن إستراتيجية وسياسات وإجراءات وضوابط إدارة مخاطر الأمن السيبراني فعالة وأن محددات فعالية وظيفة المراجعة الداخلية تعتمد على الجوانب التشريعية ، والإلتزام بالمعايير والممارسات والخصائص التنظيمية للمنشأة وخصائص وسمات المراجع الداخلي .

وفي سياق متصل فقد هدفت دراسة (Vuko et al., 2021, Pp. 17-29) إلى تحليل العوامل التي تفسر فعالية المراجع الداخلي في توفير ضمانات وتأكيدات حول إدارة مخاطر الأمن السيبراني ، وقد قامت الدراسة بإجراء إستبيان إشتمل على 183 مراجعاً في مجال تكنولوجيا المعلومات ورئيساً تنفيذياً للمراجعة من مختلف الصناعات والمؤسسات على مستوى العالم لدراسة العلاقات بين فعالية مراجعة الأمن السيبراني Cyber Security Auditing (CSA) وبعض العوامل المؤثرة في جودة المراجعة الداخلية ، وقد إنتهت الدراسة إلى أن القوى المعيارية والتي

تتمثل في شهادات الأمن السيبراني للمراجعين الداخليين والعوامل البشرية تفسر بشكل كبير فعالية مراجعة الأمن السيبراني .

كما هدفت دراسة (صالح ، 2022 ، ص ص 5-20) إلى تحليل علاقة محددات فعالية المراجع الداخلي للأمن السيبراني ، وقد إنتهت الدراسة إلى إشتقاق مقياس لدعم فعالية توكيد المراجعة الداخلية على الأمن السيبراني بالاعتماد على معايير الممارسة المهنية للمراجعة الداخلية التي توفر إطاراً إلزامياً لوظيفة المراجعة الداخلية وهي (COBIT5) و (ISO 27001/2) حيث تم تحديد مجموعة من الإجراءات لقياس فعالية توكيد المراجعة الداخلية على الأمن السيبراني خلال مراحل أداء التكليف الثلاثة بدء بالتخطيط ثم التنفيذ وأخيرا إعداد التقرير .

وفي هذا الإطار فقد إتفقت دراسة كل من (Lois et al ., 2021, Pp.25-47; Islam et al , 2018,Pp. 379-382 ; Shamsuddn, 2018, Pp. 61-69) في الهدف حيث سعت كل منها إلى فحص المتغيرات التي تؤثر على الأمن السيبراني والمرتبطة بالمراجعة الداخلية ، وقد حددت الدراسات المتغيرات في الدور الاستشاري والتعاون بين متخصصي تكنولوجيا المعلومات والمراجع الداخلي والمعرفة التكنولوجية والسياسات والمعايير والمعلومات وتدريب الموظفين فيما يتعلق بتقنية المعلومات ، وقد إنتهت الدراسات إلى أن العلاقة الجيدة بين متخصصي تكنولوجيا المعلومات والمراجعين الداخلي محدودة للغاية بالإضافة إلى ذلك فإن مستوى المعرفة التكنولوجية المتخصصة من جانب المراجعين الداخليين منخفض للغاية فيما يتعلق بمعايير سياسات الأمن التي تم مراجعتها من قبل المراجع الداخلي ، هذا بالإضافة إلى أن الدور الاستشاري للمراجعين الداخليين وتعاونهم مع الإدارة في تشكيل السياسات يظل أمراً حيوياً لتدابير الأمن السيبراني والحد من مخاطره .

وتري الباحثة أن الدراسات السابقة التي تم تناولها فيما يتعلق بالمراجعة الداخلية وإنعكاساتها على مخاطر الأمن السيبراني قد أكدت علي اهمية العلاقة بين وظيفة المراجعة الداخلية وادارة مخاطر الامن السيبراني ، وبيان اهم التحديات و المخاطر المتعلقة بالامن

السيبراني ، وتسليط الضوء علي اهمية وجود اطر وقواعد مهنية وتنظيمية تحكم هذه العلاقة ، هذا علاوة علي التعرض لمجموعة العوامل التي تؤثر علي فعالية المراجع الداخلي في ادارة الامن السيبراني ، الا ان هذه الدراسات لم تتعرض لتوضيح العلاقة بين محددات جودة المراجعة الداخلية و دورها في الحد من مخاطر الامن السيبراني وانعكاسات هذه العلاقة علي كفاءة وترشيد قرارات المستثمرين ، وهو الأمر الذي أظهر الحاجة إلى القيام بهذا البحث .

2/1 مشكلة البحث :

أدى التطور في بيئة الأعمال بسرعة غير مسبوقة إلى إتجاه العديد من المنشآت نحو مواكبة إستخدامات التكنولوجيا الحديثة ، حيث تطبق تقنيات وأدوات تكنولوجية متطورة في مباشرة أعمالها لجعلها أكثر كفاءة ، هذا علاوة على قيام معظم المنشآت الكبرى بتخزين بياناتها الهامة والحساسة على الشبكات وفي السحابة Cloud Computing ، وفي الوقت نفسه تجبر بيئة الأعمال العالمية المنشآت على الحفاظ على بنية تحتية رقمية آمنة لإجراء معاملاتها التجارية وتسمى هذه البنية التحتية الرقمية العالمية المترابطة بالفضاء السيبراني ، والذي يشتمل على الإنترنت وأنظمة الكمبيوتر والأجهزة والبرامج والمعلومات الرقمية ، ويُعد هذا الفضاء السيبراني (الإلكتروني) هاماً لجميع المعاملات الإلكترونية (Kahyaoglu & Caliyurt, 2018, Pp.360-376) .

هذا الأمر جعل الأمن السيبراني والذي يتمثل في مجموعة من التقنيات والعمليات التي تم تصميمها لحماية أجهزة الكمبيوتر من الهجمات الإلكترونية والشبكات وقواعد البيانات بما تحتويه من بيانات وما تقدمه من خدمات يتمتع بأهمية كبيرة لكافة الأطراف الداخلية بالمنشأة ، علاوة على أهميته لجميع الأطراف ذات الصلة وخاصة المستثمرين ، وفي هذا السياق تُعد تهديدات الأمن السيبراني من أهم وأكثر التهديدات التي تواجه المنشآت ومستقبلها ، حيث أكد المديرين التنفيذيين (CEOs) لعدد من المنشآت على أن الهجوم الإلكتروني الذي يؤثر على تلف أو فقد بعض المعلومات المالية للمنشآت يكون له تأثير سلبي على ثروة الملاك وسمعة المنشأة وقرارات المستثمرين ، نتيجة التأثير السلبي على أسعار أسهم المنشآت وعلى تقييم أصحاب المصالح لقدرة المنشأة على الحفاظ على أمن المعلومات (Tuson, 2021, Pp. 4-8 ; Kamiya et

(al., 2021, Pp.722-725) . كما أنه من الممكن أن يمتد التأثير السلبي للهجمات الإلكترونية على فقد أصحاب المصالح الثقة في المنشأة التي تعرضت للهجمات الإلكترونية وكذلك في الصناعة التي تنتمي إليها هذه المنشأة ، فيما يعرف بتأثير عدوى إختراق الأمن السيبراني (Cybersecurity Breach Contagion Effect) (Kelton & Pennington, 2020,) (Pp. 139-144

وفي هذا الشأن فقد أكدت دراسة كل من (ISACA , 2019 ; IIA , 2016) على أن الهجمات السيبرانية تتطور بشكل أسرع من تطور الحلول الأمنية ، الأمر الذي يترتب عليه أن تصبح تلك الإنتهاكات الأمنية تمثل جانباً سلبياً على المنشآت وعملائها من الناحية المالية ومن حيث السمعة ، وتعتبر برامج الأمان المعمول بها مثل برامج مكافحة الفيروسات والبرامج الضارة والجدران النارية غير كافية حتى الآن للحماية من مخاطر تكنولوجيا المعلومات وتوفير ضمانات بشأن الأمن السيبراني ، لذلك يجب على المنشآت التركيز على إستراتيجيات الدفاع المتعمق لتقليل التأثير المحتمل للإنتهاكات .

ومما لاشك فيه أن اتساع نطاق المراجعة الداخلية ليشمل كافة الإجراءات اللازمة لإدارة المخاطر ، أصبح يوفر للمراجع الداخلي رؤية واضحة تمكنه من تقديم توصيات بتبني إجراءات رقابية جديدة ، الأمر الذي يترتب عليه أن تكون المراجعة الداخلية في حالة ديناميكية مستمرة حتى تستطيع أن تتماشى مع التغير الحادث في تلك المخاطر ، ولذلك يمكن أن تلعب وظيفة المراجعة الداخلية دوراً مهماً في إدارة التهديدات السيبرانية من خلال تقديم منظور موضوعي إلى لجنة المراجعة وأعضاء مجلس الإدارة ثم إستخدام هذه النتائج لتطوير خطة مراجعة داخلية واسعة تتناول مجالات المخاطر السيبرانية وبالتالي إجراء تقييم مشاكل للمخاطر السيبرانية للمنشآة .

وفي سياق متصل يقترح (ضيف ، 2016 ، ص ص 496 – 554) أن يتحمل قسم المراجعة الداخلية مهمة الفحص الدوري لبيئة المعلومات الرقمية للمنشآت وتقييم مستوى مخاطر التلاعب المحيطة بها ، ومن ثم فإن تحمل قسم المراجعة الداخلية مسئولية توفير التقارير المهنية والمستقلة عن نتيجة الفحص الدوري لبيئة المعلومات الرقمية لا يمثل فقط أحد متطلبات

مجالس إدارات المنشـــآت ولكنه يمثل أيضـــاً أحد متطلبات معايير المراجعة الداخلية ، فقد أكدت معايير المراجعة الداخلية الصـــادرة عن معهد المراجعين الداخليين IIA ضـــرورة إمتلاك المراجع الداخلي المعرفة الكافية بالمخاطر والأدوات الرقابية على تقنية المعلومات بالإضـافة إلى ضـرورة إلمامهم بأساليب المراجعة المعتمدة على تقنية المعلومات (IIA , 2013).

هذا وقد اكدت دراســة كل من (Islam et al., 2018, Pp.388-400 ; صـالح ،2022، 4-15) علي أن مراجعة الأمن الســـيبراني يتطلب معرفة متطورة بتكنولوجيا المعلومات (IT) ويجب أن يكون لدى المراجعيين الداخليين معرفة كافية بمخاطر تكنولوجيا المعلومات الرئيســـية وأن يتحكموا في تقنيات وأســـاليب المراجعة القائمة على التكنولوجيا والمتاحة لأداء عملهم (IIA , 2017) وأن يكون لديهم معرفة حول تقنيات مراجعة نظم المعلومات ومعايير أمن المعلومات , وأن المراجع الداخلي يحتاج إلى مراجعة مستمرة لتقييم ومراجعة الأمن السيبراني وأن مراجعة الأمن السيبراني تعد بعداً جديداً لممارسة الأمان يهدف إلى دعم حماية أصول المعلومات الهامة للمنشأة زيادة قيمتها والتأثير المباشر على دعم وتحسين قرارات المستثمرين من خلال المساعدة في تحديد المخاطر وإقتراح أنشطة الرقابة ومراقبة عملية إدارة المخاطر .

وفي إطار ما تقدم ترى الباحثة أنه في ظل العالم المتغير الذي نعيشـــه الآن وحاجة بيئة الأعمال إلى تكييف أدواتها في التخفيف من مخاطر الأمن الســـيبراني Cyber – security والذي هو في الأساس عملية ضمان سلامة الفضاء السيبراني من التهديدات المعروفة وغير المعروفة والاستجابة لها في مراحل مختلفة المنع والاكتشاف والتخلص والتحسين يمكن أن تلعب وظيفة المراجعة الداخلية دوراً رئيسياً وفعالاً في تقييم الاضطرابات السيبرانية وتوفير توكيد فيما يتعلق بأمن المعلومات وفي تكوين رؤي حول كيفية تحســـين وحوكمة أمن معلومات المنشـــأة وجهود إدارة المخاطر ، وهذا ما أكدت عليه دراســـة كل من (عثمان ، 2022 ، ص8 ;Alina et al ., 2017, Pp. 510 – 513 ;steinbart et al., 2018, Pp. 15- 29).

وتؤكد الباحثة على أن آليات وظيفة المراجعة الداخلية يمكن أن تقوم بالمزيد من الأنشـــطة التوكيدية المتعلقة بمخاطر تكنولوجيا المعلومات والأمن السيبراني ، الأمر الذي يترتب عليه قيام

الكثير من المنشـآت بالسـعي الدائم نحو طلب المزيد من الإرشـادات والرؤي حول برامج الأمن السيبراني ومنع واكتشاف وإدارة المخاطر ، الأمر الذي يترتب عليه ترشيد القرار الإستثماري.

وبمراجعة الأداب المحاسبي في هذا الشأن وجدت الباحثة أن هناك إهتماماً بالغاً من أطراف متعددة حول موضوع مخاطر الأمن السيبراني حيث لاحظت الباحثة إرتباطه بالعديد من القضايا المحاسبية الهامة ، كذلك رصدت الباحثة أن هناك إتجاه حديث لدراسة القضايا المتعلقة بدور جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني وإنعكاساته على قرارات المستثمرين وهذا ما دفع الباحثة نحو مسايرة الإتجاه العالمي في هذا الشأن .

وإنطلاقاً مما سبق يمكن تحديد المشكلة البحثية لهذا البحث من خلال عرض التساؤلات البحثية التالية :

1- ما المقصود بالأمن السيبراني وما هي المخاطر الناجمة عنه ؟

2- ما هي محددات جودة المراجعة الداخلية للأمن السيبراني ؟

3- إلى أي مدى يمكن أن تسـاهم جودة المراجعة الداخلية المسـتخدمة في الحد من مخاطر الأمن السيبراني؟ وما هي إنعكاسات ذلك على ترشيد قرارات المستثمرين ؟

4- هل يمكن الحصـول على دليل ميداني عن أهمية الدور الذي يمكن أن تلعبه جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني وإنعكاس ذلك على ترشيد قرارات المستثمرين؟

3/1 أهمية ودوافع البحث :

تنبع أهمية البحث الأكاديمية من أهمية الموضوع قيد الدراسة والذي يعتبر من الموضوعات الحديثة في أدبيات الفكر المحاسبي وهو دور جودة المراجعة الداخلية في الحد من مخاطر الأمن السـيبراني وإنعكاسـاته على قرارات المسـتثمرين ، علاوة على ندرة الدراسـات الأكاديمية وخاصـة باللغة العربية – في حدود علم الباحثة – التي تناولت العلاقة بين المراجعة الداخلية ومخاطر الأمن السـيبراني وإنعكاسـات هذه العلاقة على قرارات المسـتثمرين ، لذلك ظهرت الحاجة الملحة لتضييق الفجوة البحثية في ذلك الصدد .

كما تتمثل أهمية البحث العملية في أهمية الأمن السـيبراني والذي يعد أحد المواضـيع التي لاقت إهتماماً واسـعاً على الصـعيد المحلي والعالمي خلال الفترة الأخيرة ، لا سـيما مع التحول الرقمي في مجال أنشـطة الأعمال ، مما يترتب عليه زيادة التهديدات الإلكترونية حيث يتوقع كل يوم إمكانية حدوث إختراق للبيانات مما يستدعي قيام اللجان المتخصصة بالضغط على المنشآت لإظهار كيفية تخفيف المخاطر الإلكترونية بوضـوح ويعتبر ذلك محفز قوي لدخول المراجعين الداخليين إلى عالم الأمن السـيبراني ، علماً بأن مراعاة تفعيل إدارة الأمن السـيبراني والحد من مخاطره بشكل صحيح في المنشآت يساعد كثيراً في مواجهة أي كوارث تقنية وسيبرانية من خلال إقفال الثغرات ومعالجة القصـور في الأنظمة وتعزيز سـياسـات أمن المعلومات وترشـيد قرارات المستثمرين .

4/1 أهداف البحث :

يستهدف البحث دراسة دور جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني وإنعكاساته على قرارات المستثمرين ، وذلك من خلال إستعراض الأمن السيبراني وتحديد المخاطر الناجمة عنه ، توضيح محددات جودة المراجعة الداخلية للأمن السيبراني ، علاوة على تحديد جودة المستخدمة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني وتأثير ذلك على ترشيد قرارات المستثمرين ، بالإضافة إلى الحصول على دليل ميداني عن أهمية الدور الذي يمكن أن تلعبه جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني وإنعكاس ذلك على ترشيد قرارات المستثمرين .

5/1 منهج وأسلوب البحث :

سوف تستخدم الباحثة المنهج العلمي بشقيه الإستنباطي والإستقرائي ، حيث تستخدم المنهج الإستنباطي من خلال المسح المرجعي للدراسات والبحوث بغية بناء الإطار النظري للبحث وإشتقاق فروض البحث ، كما تستخدم المنهج الإستقرائي في الدراسة الميدانية عن طريق جمع البيانات اللازمة لإختبار فروض البحث .

6/1 خطة البحث :

لتحقيق هدف البحث وفي ضوء مشكلته سوف يتم تنظيم البحث على النحو التالي :

المحور الأول : الإطار العام للبحث .

المحور الثاني : الأمن السيبراني (المفهوم – المخاطر) .

المحور الثالث : محددات جودة المراجعة الداخلية للأمن السيبراني

المحور الرابع : تحليل العلاقة بين جودة المراجعة الداخلية المســـتخدمة في الحد من مخاطر الأمن السيبراني وتأثير ذلك على ترشيد قرارات المستثمرين .

المحور الخامس : دراسة ميدانية .

النتائج والتوصيات والتوجهات المستقبلية .

قائمة المراجع .

المحور الثاني : الأمن السيبراني (المفهوم – المخاطر) .

2/1 مفهوم الأمن السيبراني :

يعد الأمن السيبراني من المفاهيم التي لاقت إهتماماً كبيراً في الآونة الأخيرة نظراً لظهور تقنيات وأدوات تكنولوجية جديدة وإستخدامها بشكل واسع في كافة أنشطة معظم المنشآت ، وقد عرفت دراسة (NIST, 2018) الأمن السيبراني بأنه حماية الأصول المعلوماتية من خلال معالجة التهديدات التي تتعرض لها المعلومات التي تتم معالجتها وتخزينها ونقلها بواسطة أنظمة المعلومات المتداخلة بين الشبكات ، كما عرفته دراسة (ISACA, 2017) بأنه عملية حماية مواقع تخزين البيانات والتقنيات المستخدمة لتأمينها كما يتضمن حماية تكنولوجيا المعلومات والإتصالات والأجهزة والبرمجيات .

وطبقا لما ورد في التقرير الصادر عن الاتحاد الدولي للاتصالات بشأن الامن السيبراني حول اتجاهات الإصلاح في الإتصالات للعام 2014 – 2015 حيث يمثل مجموعة من المهمات مثل

تجميع وسائل وسياسات وإجراءات أمنية ومبادىء توجيهية ومقاربات لإدارة المخاطر وتدريبات وممارسات فضلي وتقنيات يمكن إستخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين ، هذا وقد أكدت دراسة (البغدادي , 2021 ، ص ص 1513 – 1446) أن السيبراني يمثل النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات ويضمن إمكانات الحد من الخسائر والإضرار التي تترتب في حال تحقق المخاطر والتهديدات كما يتيح إعادة الوضع إلى ما كان عليه بأسرع ما يمكن بحيث لا تتوقف عجلة الإنتاج وبحيث لا تتحول الإضرار إلى خسائر دائمة .

وبناءً على ما سبق ترى الباحثة أن الامن السيبراني يمثل عملية حماية المعلومات من خلال معالجة التهديدات التي تتعرض لها هذه المعلومات التي تتم معالجتها و تخزينها ونقلها بواسطة انظمة المعلومات المتداخلة بين الشبكات ، كما تؤكد الباحثة على أن الأمن السيبراني يمتد ليشمل جميع المجالات الاقتصادية والاجتماعية والسياسية والقانونية لكافة المجتمعات المعاصرة ، كما أنه يرتبط إرتباطاً وثيقاً بسلامة مصادر الثروة والتقدم في الوقت الراهن والتي تشمل القدرة على الاتصال والتواصل والبيانات والمعلومات التي يستند عليها الإنتاج والإبداع والقدرة على المنافسة .

2/2 طبيعة وأنواع المخاطر السيبرانية :

في عالم يشوبه الكثير من التعرض للمخاطر على جميع المستويات وتزايد حدة اشكال الحرب السيبرانية تحتاج بيئة الأعمال إلى تكييف أدواتها في الحد من مخاطر الأمن السيبراني والإستجابة لها في مراحل مختلفة وأصبحت التغييرات والتحسينات التي تأتي مع التكنولوجيا الجديدة والإبتكار وإعتمادها من قبل المنشآت أكثر تعقيداً عما سبق .

وفي سياق ذلك يتطلب الأمر بداية التعرف على طبيعة الجريمة السيبرانية التي تشكل الخطر الأساسي الواجب مكافحته وإستناداً إلى مبدأ لا جريمة ولا عقاب دون نص عمدت العديد من الدول إلى وضع نصوص قانونية خاص بهذه الجرائم التي يمكنها أن تشمل قطاع واسع من الأعمال غير الشرعية كتلك التي تستخدم أجهزة الكمبيوتر والشبكات كوسيلة لتنفيذ الجريمة أو

كهدف لها بدءا من عمليات اختراق الأنظمة المعلوماتية وأنظمة الاتصالات وصولاً إلى الهجمات التي تعطل الخدمات ، وقد عمدت الاتفاقية الأوروبية لمكافحة الجريمة السيبرانية إلى تقسيم الجرائم السيبرانية إلى مجموعتين :

المجموعة الأولي والتي صنفت الجريمة السيبرانية على أساس أنها كل تصرف غير شرعي موجه بالوسائل الإلكترونية نحو أمن أنظمة المعلومات والبيانات التي تحويها , بينما جاءت المجموعة الثانية لتعرف الجريمة السيبرانية على أساس أنها كل تصرف غير شرعي يرتكب بواسطة الأنظمة المعلوماتية أو بطريقة متصلة بها ويشمل جرائم كالحيازة غير المشروعة أو عرض الخدمات وتوزيع المعلومات بواسطة أنظمة معلومات أو شبكات معلومات ، وهذا ما أكدت عليه دراسة (Eling & Wirfs, 2016, Pp. 23-57) .

1/2/2 طبيعة المخاطر السيبرانية

وبناء على ما سبق فقد أكدت دراسة كل من (Hartmann& Carmenate, 2021, Pp.9-23; Florakis et al., 2020, Pp.7-68) بأن المخاطر السيبرانية يقصد بها المخاطر التشغيلية على أصول المعلومات والتكنولوجيا التي لها عواقب تؤثر على سرية وسلامة ونظم المعلومات ومقارنة بفئات المخاطر التي يغطيها التأمين فإن المخاطر السيبرانية تتفق من حيث الخصائص والمسئولية مع مخاطر كل من الممتلكات والخصوم وكذلك المخاطر الكارثية والتشغيلية ، ومما لاشك فيه أن تكنولوجيا المعلومات والإتصالات تتيح إمكانات هائلة وغير مسبوقة لإنتاجية أفضل في جميع القطاعات وللتواصل عبر القارات إلا أن البنية التحتية لهذه التقنيات تمثل إرتباطاً بين مصالح متعددة وخدمات مختلفة ودول عديدة الأمر الذي يجعل من الأخطار في المجال السيبراني أخطاراً عالمية فلا يمكن لأي جهة أن تضمن بقاءها في منأى عن الأخطار ما دامت سلامة الأخرين معرضة للخطر .

2/2/2 أنواع المخاطر السيبرانية

أكدت دراسة كل من (Li & ; Shahimi & Mahzan,2018, Pp. 1257 – 1283 Wang, 2018, Pp.49-51) على أن الهجمات السيبرانية تضم ثلاث أنواع يمكن سردها في الآتي :

أ- مخاطر سيبرانية تتعلق بالسرية : حيث تنشأ عندما يتم الكشف عن المعلومات الخاصة داخل المنشأة إلى أطراف ثالثة كما في حالة حدوث إختراق البيانات .

ب- مخاطر سيبرانية تتعلق بالنزاهة : والتي تتعلق بإساءة استخدام الأنظمة كما هو الحال بالنسبة للاحتيال .

ج- مخاطر سيبرانية تتعلق باستمرارية الأداء : والتي تتلخص في تعطل أو التوقف عن ممارسة الأعمال .

وترى الباحثة أن هذه الأنواع الثلاثة من المخاطر السيبرانية لها تأثيرات مباشرة ومختلفة على الأهداف حيث يؤدي تعطل الأعمال إلى المنع من العمل مما ينتج عنه خسارة في الإيرادات (بالنسبة للمنشآت) أو تعطل في تحقيق الأهداف بالنسبة للأفراد كما يؤدي الاحتيال إلى خسائر مالية مباشرة في الوقت الذي يستغرق التحقيق في تأثيرات اختراق البيانات وقتاً أطول الأمر الذي ينتج عنه أضرار معنوية تمس السمعة وفضلاً عن تكاليف التقاضي وبصفة عامة فإن خطر فقدان الثقة في أعقاب الهجمات الإلكترونية قد يكون عالياً بالنسبة للقطاع المالي بالنظر إلى إعتماد المؤسسات المالية على ثقة عملائها مما يؤثر على قرارات المستثمرين .

المحور الثالث : محددات جودة المراجعة الداخلية للأمن السيبراني .

مما لاشك فيه أن إتساع نطاق المراجعة الداخلية ليشمل مراجعة ، وتقييم جميع الأنشطة والعمليات المؤسسية ، بهدف تقييم وتحسين فاعلية إدارة المخاطر ، وأنظمة الرقابة ، وتطبيق الحوكمة ، كل ذلك جعل وظيفة المراجعة الداخلية الفعالة مصدراً ذا قيمة عالية للمعلومات التي تحتاجها الأطراف ذات الصلة ، وهو ما يبرر الإهتمام المتزايد في الفترة الأخيرة بأهمية المراجعة

الداخلية وما يمكن أن تحققه من قيمة مضـــافة لجميع المنشـــآت ، وذلك من خلال ما يوفره المراجع الداخلي من معلومات ، وتوصـيات وإسـتشـارات تسـاعد الوحدة الحكومية على التخطيط الإســتراتيجي لأدائها ومتابعة هذا الأداء وتوجيهه ليحقق الأهداف المخططة ، وإتخاذ ما يلزم من قرارات لتسيير الأعمال والأنشطة ، ودعم عمليات إدارة المخاطر ، وهذا ما أكدت عليه دراسة كل من (Yang et al., 2020, pp. 167-183 ; Betti et al., 2021, Pp. 872 – 888) .

وفي ســـياق متصـــل أوصـــت لجنة مبادئ الإدارة الســـليمة للمخاطر الصـــادرة عن (COSO,2019 ; IIA, 2020) بأن إدارة مخاطر الأمن الســـيبراني يمكن أن تدار من خلال ثلاث خطوط دفاعية ، حيث يتمثل الخط الدفاعي الأول في مديرو وحدات الأعمال جنباً إلى جنب مع وظيفة تكنولوجيا المعلومات IT حيث أنهم بحاجة إلى اعتبار مخاطر الأمن السيبراني جزءاً لا يتجزأ من عملهم وإنشاء الهياكل والضوابط المناسبة لإدارة العمليات والمخاطر ، كما يتمثل الخط الدفاعي الثاني في إدارة مخاطر أمن المعلومات حيث توفر الخبرة لتنفيذ ومتابعة فعالية ضـــوابط الأمن السيبراني CS ، بينما يتمثل الخط الدفاعي الثالث في وظيفة المراجعة الداخلية حيث تزود مجلس الإدارة ولجنة المراجعة التابعة لها بتوكيد مســـتقل عن فعالية إســـتراتيجية وســـياســـات وإجراءات وضوابط إدارة مخاطر الأمن السيبراني وهذا ينطوي على مراجعة مدى كفاية العمل الذي قامت به أدوار الخطين الأول والثاني (Vuko et al., 2021, Pp. 37-40).

تعتبر وظيفة المراجعة الداخلية احد الركائز الأساسية لتلبية احتياجات مختلف أصحاب المصالح ، خاصة المساهمين والإدارة حيث تعمل المراجعة الداخلية على إعداد تقرير عن مدى فعالية هيكل الرقابة الداخلية ، كما أنها تساهم بشكل كبير في توفير نظرة عامة وشاملة عن أداء مختلف الإدارات والأقسام داخل المنشأة والمخاطر التي تواجهها ، هذا علاوة على متابعة قرارات مجلس الإدارة بشكل مستمر (pwc ,2018; شحاتة، 2020 ، ص ص 120 – 128).

وفي هذا الصدد يمكن القول ان جودة وظيفة المراجعة الداخلية فيما يتعلق بإدارة مخاطر الأمن السيبراني والحد من تلك المخاطر يرتكز على قيام مدير إدارة المراجعة الداخلية بتقديم النصح والإرشاد لمجلس الإدارة بصدد تحديد وتوصيف وقياس مخاطر الأمن السيبراني المحيطة ببيئة أعمال المنشاة التكنولوجية وكيفية مواجهتها والحد من آثارها بما يدعم تحقيق أهداف المنشاة (Florakis et al.,2020, P.46 ; Li & Wang .,2018, Pp. 53-55) وفي سياق متصل تعمل جودة المراجعة الداخلية على تمكين إدارات المنشآت من تصميم خطوط دفاع قوية لمواجهة مخاطر الأمن السيبراني طبقاً لطبيعة واحتياج البيئة التكنولوجية ونوعية وكثافة المخاطر التي تواجه المنشأة والتي تتمثل في (صالح ، 2022، ص ص 7-8) :

(أ) تقييم النضج السيبراني : والذي يتمثل في تحديد الفجوات في الوضع الحالي للأمن السيبراني هذا علاوة على فهم محددات وأبعاد نقاط الضعف المطلوب التركيز عليها .

(ب) مراجعة التكنولوجيا الجديدة : حيث تقدم منصات التكنولوجيا الناشئة والتي تضم (السحابة والشبكات الاجتماعية والجوال والبيانات الضخمة وأنظمة الذكاء الاصطناعي وغيرها) مخاطر الكترونية جديدة تستدعي القيام بعمليات مراجعة خاصة تشتمل على مراجعة عنصر الأمان قبل وبعد تنفيذ التكنولوجيا الجديدة.

(ج) مراجعة التكنولوجيا العميقة : من الأهمية قيام المراجعة الداخلية بتقييم المخاطر الأمنية المتعلقة بأنظمة التكنولوجيا المتطورة مع التأكيد على الفهم الشامل للمخاطر الأمنية.

ومما لاشك فيه أن هناك العديد من العوامل التي تحدد فعالية المراجعة الداخلية بشأن الأمن السيبراني ولعل أهمها ما جاء بدراسة كل من (Islam et al., 2018, Pp. 394-398 ; IIA, 2017; Deloitte, 2017) :

1/3 التأهيل العلمي والعملي لفريق المراجعة الداخلية بالمنشأة : أشارت منظمة المراجعة الداخلية (IAF, 2021) إلى ضرورة أن يتفهم المراجعون الداخليون ومعاهد ومنظمات المراجعة الداخلية أهمية الإستفادة من التكنولوجيا ، حيث تتطلب مراجعة الأمن السيبراني بجودة عالية تأهيل فريق المراجعة الدخلية بالمنشأة بمعرفة متطورة بتكنولوجيا المعلومات (IT) ومخاطرها ، وأن يكون لديهم القدرة على التحكم في تقنيات المراجعة القائمة على التكنولوجيا الحديثة والمتاحة لأداء أنشطة المراجعة الداخلية بجودة عالية ، الأمر الذي يترتب عليه القدرة على تطوير علاقات أعمق مع

وظائف أمن نظم المعلومات ومن ثم المساهمة في بناء برنامج إدارة أمن سيبراني أكثر فعالية وجودة وبالتالي من المتوقع أن تؤدي المراجعة الداخلية التي تضم رؤساء مراجعة داخلية حاصلين على شهادات الأمن المناسبة مثل (الشهادات الأمنية CISM و CSP) وكذلك شهادات مراجعة أمن أنظمة المعلومات مثل : (شهادة CISA و QICA) [1] إلى زيادة جودة مراجعة الأمن السيبراني .

2/3 مشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية Enterprise Risk Management (ERM) : نظراً لتطور دور المراجعة الداخلية حيث أصبح تركيزها الطبيعي على الحوكمة وإدارة المخاطر والإلتزام ، فأصبحت ذات أهمية بالغة في الإشراف على جميع مكونات أطر عمل إدارة المخاطر المؤسسية ومن ثم فإن إدارة المخاطر المؤسسية لها تأثير كبير على أنشطة المراجعة الداخلية ، الأمر الذي يترتب عليه تمتع المراجعة الداخلية بفعالية عالية في أداء أنشطتها ، علاوة على قدرة الرؤساء التنفيذيون للمراجعة على تشغيل أقسامهم بشكل أكثر كفاءة من خلال الاستفادة من موارد إدارة المخاطر للمنشأة ، هذا بالإضافة إلى أنه عند مشاركة المراجعة الداخلية في إدارة المخاطر ينهج المراجعون نهج التفكير الإبتكاري الإستراتيجي مثل المديرين والتركيز على أهداف العمل بدلاً من أهداف المراجعة فقط وبالتالي يمكن للمراجعة الداخلية من خلال إجراء تقييم شامل للمخاطر السيبرانية تقديم وجهات نظر ونتائج موضوعية إلى لجنة المراجعة وأعضاء مجلس الإدارة واستخدام هذه النتائج لتطوير خطة المراجعة الداخلية بشكل موسع تضم مجالات المخاطر السيبرانية التي تواجهها المنشأة خلال فترة مراجعة واحدة أو فترة مراجعة متعددة السنوات .

3/3 جودة وظيفة المراجعة الداخلية : أكدت دراسة كل من صالح ، 2022 ، ص 9 ; (Islam et al., 2018, Pp. 385- 390 ; Christ et al., 2015, Pp. 37 – 59 ;Ege, 2015, Pp. 495 – 497) على أن وظيفة المراجعة الداخلية المصـــحوبة بالجودة العالية يترتب عليها مجموعة من المنافع للمنشـــآت لعل أهمها : تحســـين حوكمة المنشـــآت ، جودة

[1] تتمثل الشهادات المناسبة في الشهادات الأمنية مثل CISM – CISSP – CSP – CDP – CISRCP شهادة مراجعة أنظمة المعلومات مثل CISA – CRISC – QICA

التقارير المالية ، فعالية هيكل الرقابة الداخلية ، القدرة على تقديم تقييمات أفضـــل للمخاطر ، الحد من سوء السلوك الإداري وزيادة كفاءة المراجعة الخارجية ، وفيما يتعلق بالأمن السـيبراني يمكن أن تلعب المراجعة الداخلية دوراً هاماً وبارزاً في إدارة المخاطر الســـيبرانية من خلال إجراء تقييم شـــامل للمخاطر الإلكترونية ويمثل برنامج توكيد الجودة والتحســـين The Quality assurance and Improvement Program (QAIP) الخاص بالمراجعة الداخلية معياراً لتقييم جودة المراجعة الداخلية وبالتالي من المتوقع أن ترتبط المراجعة الداخلية عالية الجودة بشكل كبير وإيجابي بمراجعة الأمن السيبراني والحد من مخاطره .

4/3 حجم قســـم المراجعة الداخلية ومشـــاركته في تطوير بيئة الأعمال : من المهم أن تدرك منشآت الأعمال أن الإستثمار التكنولوجي في المراجعة الداخلية له عائد ومردود إيجابي وبالتالي يكون لإدارة المراجعة الداخلية حجم يتناسـب مع مكانتها وأهميتها لكل منشـأة ، ويزيد من فعالية إدارة المراجعة الداخلية تواصـــلها الدائم مع كافة الإدارات وخاصـــة مع إدارة المخاطر ولجنة المراجعة ، فمن المعروف أن لجنة المراجعة تتمتع بتأثير هائل على المراجعة الداخلية حيث يقوم المديرون التنفيذيون للمراجعة بتقديم تقرير إلى لجنة المراجعة كما تخضع مجالات عمل المراجع الداخلي لمسـؤوليات اللجنة ولذلك يجب أن يلعب المراجع الداخلي دوراً مركزياً في مسـاعدة لجنة المراجعة على الإشراف على الأمن السيبراني ، والجدير بالذكر أن اجتماعات المراجعين الداخليين المتكررة مع لجنة المراجعة يقلل من إحتمالية حدوث مشـــاكل تتعلق بمراجعة الأمن الســـيبراني ، نظراً لتقارب المسـافات بين لجنة المراجعة وإدارة المراجعة الداخلية ورفع التقارير إلى الإدارة العليا ، هذا علاوة على دعم مشـــاركة المراجعين الداخليين في طرح وتطوير الرؤى حول مخاطر الأمن السيبراني .

وترى الباحثة أن المراجع الداخلي مطالب بتوفير تأكيدات معقولة عن مدى توافر متطلبات أمن الأنظمة والمعلومات وتأكيد كفاءتها وفعاليتها ، لتحقيق متطلبات الأمن الســـيبراني ، ومما لاشـــك فيه أن قيامه بهذا العمل يتطلب منه تطوير ذاته ليمتلك المهارات اللازمة لتقييم إدارة مخاطر الأمن السـيبراني بشـكل فعال ، وفهم وتقييم إجراءات التعامل مع المخاطر المتوقعة نظراً

لأن فرق المراجعة الداخلية التي تمتلك مهارات رقمية ولديها إدراك بأهمية الإمكانيات الرقمية ، وكيفية الإستفادة منها سوف تمثل قيمة مضافة للمنشأة مما ينعكس بشكل قوي على جذب العديد من الإستثمارات ودعم كفاءة القرار الإستثماري ، وهذا ما سوف تتناوله الباحثة في المحور التالي من البحث .

المحور الرابع : تحليل العلاقة بين جودة المراجعة الداخلية المستخدمة في الحد من مخاطر الأمن السيبراني وتأثير ذلك على ترشيد قرارات المستثمرين .

نال موضوع إدارة مخاطر الأمن السيبراني والحوادث المتعلقة به إهتماماً بالغاً من جانب الباحثين والجهات المهنية والأكاديمية ، نظراً لتأثيره الكبير على قرارات بعض أصحاب المصالح مثل المحللين الماليين وكذلك على الأداء المالي للمنشآت وسمعتها ، وتعتبر مخاطر الأمن السيبراني من أكبر المخاطر التي تواجهها المنشآت حيث على غرار المخاطر المالية ومخاطر السمعة التي تتعرض لها المنشآت يمكن لمخاطر الأمن السيبراني أن تؤدي إلى إرتفاع التكاليف والتأثير السلبي على عوائد المنشآت والإضرار بقدرة المنشآت على الابتكار وإكتساب العملاء والحفاظ عليهم حيث أن الهجمات الإلكترونية مكلفة ولها تأثير واضح على المركز المالي للمنشآت ، مما يؤثر على القرارات الإستثمارية بشكل كبير، وهذا ما أكدت عليه دراسة كل من (Kelton&Pennington, 2020, Pp. 152-155; Tuson, 2021,Pp.9-15 ;Frank et al.,2019, Pp.183-200; Kamiya et al., 2021, Pp. 735-738 ؛علي وعلي،2022، ص ص 17-32) .

وفي سياق متصل فقد أكدت دراسة (AL- Moshaigeh et al., 2019, Pp. 36-41; Badawy, 2021,p.6) على أن تعتبر الهجمات الإلكترونية مكلفة وقد يكون لها تأثير شديد على الوضع المالي للمنشأة وقد تتسبب في تحريف جوهري في سجلات المنشأة والحد من قدرة المنشأة على الإستمرار ، ولهذا السبب تعتبر مخاطر الأمن السيبراني ذات أهمية كبيرة للمستثمرين أثناء عملية اتخاذ القرار الاستثماري ، واستنادًا إلى استطلاع تم إجرائه (بمركز جودة

التدقيق) في الولايات المتحدة عام 2017 ، وإتضح أن رأى 43% من المستثمرين غير المحترفين تؤكد على أن الهجمات السيبرانية سوف تؤثر على قراراتهم وخططهم الاستثمارية .

هذا وقد أكدت بعض الدراسات (Hilary el al., 2016, Pp. 1-59; Heroux & Anne, 2020, Pp. 73-100; Kelton & Pennington, 2020, Pp.147-153) على أن المنشآت يمكنها استخدام نظرية الإشارة Theory Signaling للحد من عدم تماثل المعلومات بين الإدارة وأصحاب المصالح من خلال إفصاح المنشآت عن تقرير إدارة مخاطر الأمن السيبراني لإرسال إشارات إيجابية لأصحاب المصالح حول الجهود المبذولة من المنشأة في مجال الأمن السيبراني والحماية من الهجمات الإلكترونية حيث أن الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني يمكن أصحاب المصالح من تقييم مدى قدرة المنشأة على الحفاظ على أمن المعلومات وتقليل احتمالات حدوث اختراقات وأحداث سلبية في المستقبل مما يدعم قرارات المستثمرين .

كما أكدت دراسة (Kamiya et al., 2021, Pp. 720-738) التي تمت على عينة مكونة من 244 شركة مدرجة في البورصة الصينية خلال الفترة من 2005 إلى 2017 على أن الهجوم الإلكتروني الذي يؤثر على تلف أو فقد بعض المعلومات المالية للمنشآت يكون له تأثير سلبي على ثروة الملاك وسمعة المنشأة نتيجة التأثير السلبي على اسعار أسهم المنشآت وعلى تقييم أصحاب المصالح لمقدرة المنشأة على الحفاظ على أمن المعلومات .

والجدير بالذكر أن المستثمرين يمثلون أكثر الشرائح قلقاً فيما يتعلق بمخاوف مخاطر وجرائم الأمن السيبراني ، حيث يسعى المديرون إلى تخصيص المزيد من الموارد لمواجهة المخاطر السيبرانية وذلك نظراً لأن بعض المستثمرين يهتمون بالأبعاد والرؤى التالية فيما يتعلق بمخاطر الأمن السيبراني (Kelton & Pennington, 2020, Pp.138-150) :

أ- يهتم المستثمرون بإستراتيجية إدارة المخاطر التي تتبناها المنشأة .

ب- يهتم المستثمرون بكيفية قيام المنشأة بإكتشاف مخاطر الأمن السيبراني .

ج- يهتم المستثمرون بقيام المنشأة بمواجهة مخاطر الأمن السيبراني والحد منها .

د- يريد المستثمرون الحصول على تقييم مستقل للإنترنت الإلكتروني للمنشأة موضع إستثماراتهم.

وليس بغريب ان يسعي اصحاب المصالح وخاصة المستثمرين علي الحصول علي معلومات وتقارير حول كيفية حماية المنشات لانفسها من مخاطر حوادث الامن السيبراني ، حيث يعتمد المستثمرون بشكل كبير علي افصاحات وتقارير الامن السيبراني لاتخاذ قراراتهم الاستثمارية .

وفي ضوء ما سبق نجد أن المستثمرون يعتمدون بشكل كبير علي تقارير الامن السيبراني الصادرة من ادارة المراجعة الداخلية للجنة المراجعة و الادارة العليا لاتخاذ قراراتهم الاستثمارية ، وبالتالي تلعب جودة المراجعة ذات الصلة بالأمن السيبراني ومخاطره دوراً كبيراً في ترشيد القرارات الإستثمارية .

وترى الباحثة أن أصحاب المصالح وخاصة المستثمرين يهتمون بالمعلومات المالية وغير المالية المؤكدة من أجل إتخاذ قراراتهم المختلفة ، ومن المهم أن يتم إعلام المستثمرين بمخاطر وهجمات الأمن السيبراني الجوهرية التي تؤثر على المنشآت التي يستثمرون فيها من خلال تقارير واضحة تعمل على إضافة القيمة لهم ، حيث يمثل ذلك محور تعزيز للثقة في قدرة المنشأة على إدارة مخاطرها الإلكترونية .

وبناء على ما سبق وفي ظل مشكلة البحث وأهميته وتحقيقاً لأهدافة يمكن صياغة فروض البحث على النحو التالي :

فروض البحث :

(1) الفرض الأول : توجد علاقة تأثير إيجابية ذات دلالة إحصائية بين محددات جودة المراجعة الداخلية والحد من مخاطر الأمن السيبراني

وينبثق من هذا الفرض الفروض الفرعية التالية :

1/1 الفرض الفرعي الأول : توجد علاقة تأثير إيجابية ذات دلالة إحصائية بين المقدرة المهنية لفريق المراجعة الداخلية والحد من مخاطر الأمن السيبراني .

2/1 الفرض الفرعي الثاني : توجد علاقة تأثير إيجابية ذات دلالة إحصائية بين مشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية والحد من مخاطر الأمن السيبراني .

3/1 الفرض الفرعي الثالث : توجد علاقة تأثير إيجابية ذات دلالة إحصـــائية بين جودة تنفيذ المهام والحد من مخاطر الأمن السيبراني .

4/1 الفرض الفرعي الرابع : توجد علاقة تأثير إيجابية ذات دلالة إحصـــائية بين حجم قســـم المراجعة الداخلية ودعم الإدارة والحد من مخاطر الأمن السيبراني .

(2) الفرض الثاني : توجد علاقة تأثير إيجابية ذات دلالة إحصـــائية بين الحد من مخاطر الأمن السيبراني وترشيد قرارات المستثمرين .

المحور الخامس : دراسة ميدانية .

1/5 إجراءات ومنهجية الدراسة الميدانية

هدف الدراسة الميدانية

يتمثل الهدف الرئيسي للدراسة الميدانية في الحصول على دليل ميداني عن أهمية إختبار فروض البحث المتعلقة بأثر جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني وإنعكاساته على ترشيد قرارات المستثمرين ، وذلك للوقوف على العلاقة بين أهم المتغيرات المستقلة المتعلقة بمحددات جودة المراجعة الداخلية والتي يمكن أن تؤثر بشكل معنوي على الحد من مخاطر الأمن السيبراني كمتغير تابع والتوصل إلى إنعكاسات هذه العلاقة على ترشيد قرارات المستثمرين ، عن طريق إستقصاء الواقع التطبيقي والمتمثل في مجموعة من الفئات المستقصى منهم والتي تتمثل في :

1/1/5 مسئولي المراجعة الداخلية .

2/1/5 مسئولي تكنولوجيا المعلومات .

3/1/5 مسئولي إدارة المخاطر .

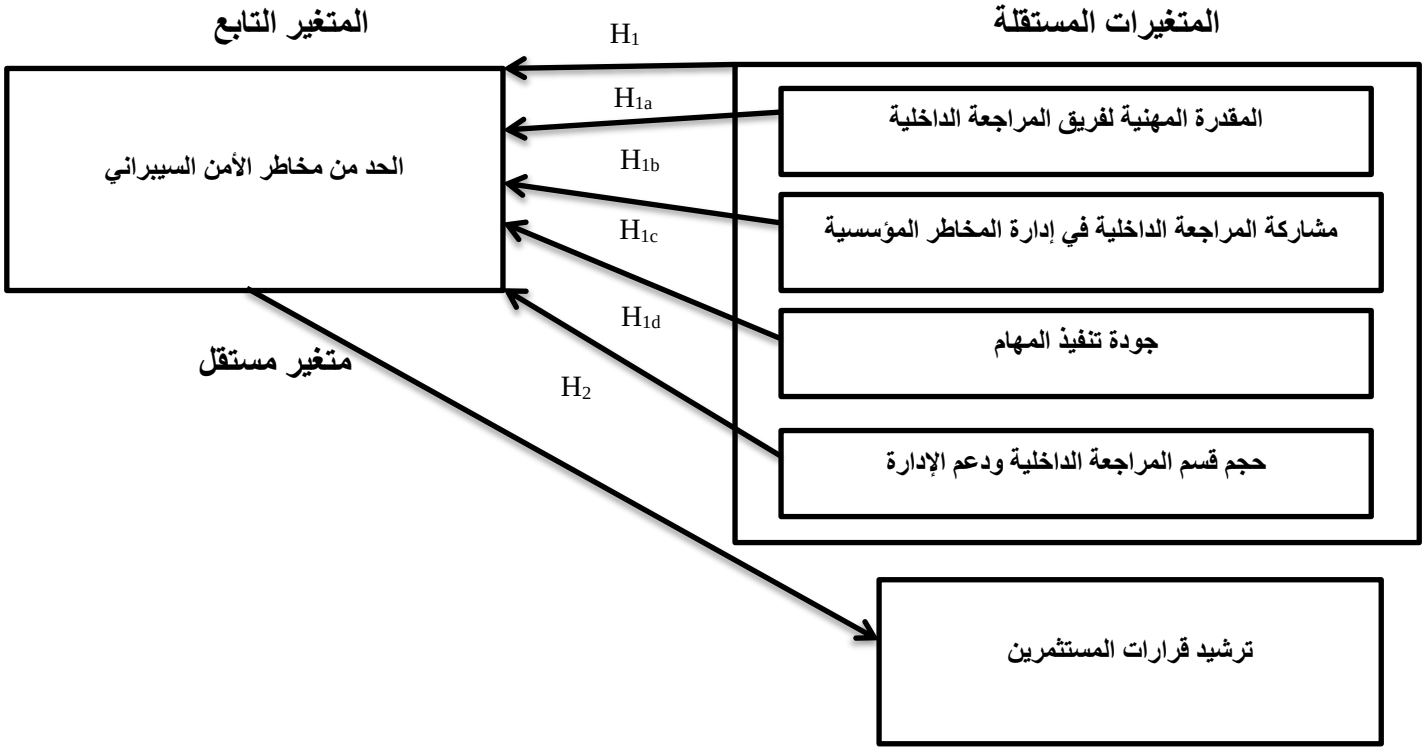
4/1/5 المستثمرين (من خلال شركات وساطة وتداول الأوراق المالية)

متغيرات ونموذج البحث :

يمكن للباحثة إستعراض متغيرات ونموذج البحث وذلك تمهيداً لإختبار فرض البحث الأول الرئيسي والفروض الفرعية المنبثقة منه ، علاوة على إختبار فرض البحث الثاني ، وذلك من خلال الشكل رقم (1) التالي :

شكل رقم (1)

متغيرات ونموذج البحث



المصدر : من إعداد الباحثة .

وبناء على الشكل السابق وطبقاً لصياغة الفرض الأول الرئيسي فإن المتغير المستقل لهذا الفرض يتمثل في محددات جودة المراجعة الداخلية والتي أفردتها الباحثة في المقدرة المهنية لفريق المراجعة الداخلية ، مشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية ، جودة تنفيذ المهام ، حجم قسم المراجعة الداخلية ودعم الإدارة ، بينما يتمثل المتغير التابع في الحد من مخاطر الأمن السيبراني ، أما طبقاً لصياغة الفرض الثاني فإن المتغير المستقل يتمثل في الحد من مخاطر الأمن السيبراني ، بينما يتمثل المتغير التابع في ترشيد قرارات المستثمرين .

مجتمع وعينة البحث:

ويتمثل مجتمع الدراسة في مجموعة من شركات الإتصالات المقيدة في سوق الأوراق المالية المصرية والتي تضم الشركات التالية :

1- شركة أورانج مصر .

2- شركة فودافون مصر .

3- شركة إتصالات مصر .

4- الشركة المصرية للإتصالات .

ويوضح الجدول التالي توزيع المجتمع على فئات الدراسة :

جدول رقم (1)

توزيع المجتمع على فئات الدراسة

فئات الدراسة	العدد
مسئولي المراجعة الداخلية	136
مسئولي تكنولوجيا المعلومات	48
مسئولي إدارة المخاطر	32
المستثمرين (من خلال شركات وساطة وتداول الأوراق المالية)	44
الإجمالي	260

- عينة الدراسة:

بإستخدام أسلوب العينة الطبقية المتناسبة، وبإفتراض توافر الظاهرة محل الدراسة بنسبة (50%) اى أن (L=0.5) وبتطبيق معادلة حجم العينة (Weijters et al., 2021,Pp85-103)

$$n = \frac{L(1-L)}{\frac{d^2}{Z^2} + \frac{L(1-L)}{N}}$$

حيث أن:

N حجم العينة عندما يكون السحب عشوائى طبقى.

Z القيمة الجدولية تحت المنحنى الطبيعى، عند معامل الثقة 95%، وتساوى 1.96

D الخطأ المسموح به ويساوى 05. عند معامل ثقة 95%

L نسبة العينة من حجم المجتمع

وبتطبيق القانون السابق توصلت الباحثة إلى أن حجم عينة الدراسة فى الحدود العليا لها = 155 مفردة تقريباً كما يلى :

$$n = \frac{0.5\,(1-0.5)}{\frac{0.5}{\frac{(1-0.5}{260} + \frac{(0.05)^2}{(1.96)}}}$$

مفردة 155 =

وبإستخدام العينة الطبقية المتناسبة تم توزيع مفردات عينة الدراسة على فئات المستقصى منهم تبعاً للمعادلة التالية:

$$n_j^* = n^* \frac{N_j}{}$$

حيث أن

Nj حجم المجتمع من كل فئة من فئات الدراسة.

nj هي حجم العينة الطبقية المتناسبة من كل فئة.

وقد قامت الباحثة بإتباع أسلوب المقابلة الشخصية لبعض مفردات العينة وإعتمدت الباحثة في توزيع إستمارات الإستقصاء على البريد الإلكتروني ، حيث قامت الباحثة بتوزيع (155)

إستمارة كما حاولت الباحثة من خلال هذا الإستمارة إستقصاء كافة المشاكل والأسئلة التي ظهرت خلال الإطار النظري للبحث.

وقد بلغت عدد الإستمارات التي لم يتم الرد عليها 9 استمارة استبيان، و بالتالي بلغت عدد الاستمارات المستلمة (146 استمارة) تشكل ما نسبته 94.19% من الإستمارات الموزعة وهي نسبة مرتفعة، وقد تم إستبعاد (7) إستمارات لوجود أكثر من إجابة على السؤال الواحد، وكذلك (4) إستمارة لوجود كثير من الأسئلة الهامة غير المجاب عليها، وبالتالي أصبح عدد الاستمارات الصالحة للتحليل 135 إستمارة تشكل نسبة 92.46% من الإستمارات المستلمة ونسبة 87.09% من نسبة الإستمارات الموزعة وهى نسبة عالية يمكن الإعتماد عليها في التحليل الإحصائى.

وقد إعتمد الإستقصاء على مقياس ليكرت الخماسي طبقاً لأوزانه النسبية والموضح في الشكل رقم (2) التالي :

شكل رقم (2)

الأوزان النسبية لمقياس ليكرت الخماسي

التصنيف	موافق تماما	موافق	محايد	غير موافق	غير موافق تماما
الوزن النسبي	5	4	3	2	1

الخصائص الديموجرافية لعينة الدراسة:

جدول رقم (2)

توصيف عينة الدراسة وفقا للوظيفة :

الوظيفة	العدد	النسبة المئوية %
مراجع داخلي	74	%55
مسئول تكنولوجيا المعلومات	26	%19

مسئول إدارة المخاطر	14	%10
مستثمر (من خلال شركات وساطة وتداول الأوراق المالية)	21	%16
المجموع الكلي	135	%100

جدول رقم (3)

توصيف عينة الدراسة وفقا للعمر :

العمر	العدد	النسبة المئوية %
أقل من 30	20	%15
30 وأقل من 40 عام	65	%48
40 وأقل من 50 عام	36	%27
من 50 وما بعدها	14	%10
المجموع الكلي	135	%100

جدول رقم (4)

توصيف عينة الدراسة وفقا للمؤهل العلمي :

المؤهل	العدد	النسبة المئوية %
دبلوم	10	%7
تعليم جامعي	50	%37
ماجستير	27	%20
دكتوراه	48	%36
المجموع الكلي	135	%100

جدول رقم (5)

توصيف عينة الدراسة وفقاً لمستوى الخبرة :

عدد سنوات الخبرة	العدد	النسبة المئوية %
أقل من 5 سنوات	17	%13
5 سنوات وأقل من 10 سنوات	60	%44
من 10 سنوات وأقل من 20 سنة	40	%30
من 20 سنة فأكثر	18	%13
المجموع الكلي	135	%100

جدول رقم (6)

توصيف عينة الدراسة وفقاً للتخصص

التخصص	العدد	النسبة المئوية %
محاسبة ومراجعة	77	%57
برمجة ونظم معلومات	28	%21
إدارة أعمال	15	%11
متنوعة	15	%11
المجموع الكلي	135	%100

الأساليب الإحصائية المستخدمة :

لغرض اختبار فروض البحث تم تحليل البيانات بإستخدام بعض الأساليب الإحصائية الملائمة لطبيعة هذه البيانات وهي :

1- اختبار ألفا كرونباخ لقيس درجة الصدق والثبات والتأكد من إمكانية الاعتماد على نتائج الدراسة الميدانية في تعميم النتائج .

2- اختبار كروسكال واليس (Kruskal-Wallis) ويتم استخدامه بغرض دراسة مدى الاتفاق بين استجابات مفردات المجموعات الأربعة لعينة الدراسة من مسئولي المراجعة الداخلية ، مسئولي تكنولوجيا المعلومات ، مسئولي إدارة المخاطر ، المستثمرين (من خلال شركات وساطة وتداول الأوراق المالية)

3- استخدام أساليب التحليل الإحصائي الوصفي مثل الوسط الحسابي المرجح للوقوف على مدى الأهمية النسبية لإجراءات التحقق المستخدمة في تقييم الدراسة والانحراف المعياري لقياس درجة التشتت في أراء المستقصي منهم بقائمة الاستقصاء .

4- أسلوب تحليل الانحدار المتعدد حيث تم استخدام هذا الأسلوب لقياس مدى تأثير العلاقة بين محددات جودة المراجعة الداخلية والتي تضم (المقدرة المهنية لفريق المراجعة الداخلية – مشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية – جودة تنفيذ المهام – حجم قسم المراجعة الداخلية ودعم الإدارة) والحد من مخاطر الأمن السيبراني ، وقد استخدم هذا الأسلوب لقياس مدى العلاقة بين محددات جودة المراجعة الداخلية كمتغير مستقل والحد من مخاطر الأمن السيبراني كمتغير تابع في الفرض الأول الأساسي .

5- أسلوب تحليل الانحدار البسيط : تم استخدام هذا الأسلوب لقياس مدى تأثير العلاقة بين كل خاصية من خصائص جودة المراجعة الداخلية والمقدرة المهنية لفريق المراجعة الداخلية ، خصائص جودة المراجعة الداخلية ومشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية ، خصائص جودة المراجعة الداخلية وجودة تنفيذ المهام ، خصائص جودة المراجعة الداخلية وحجم قسم المراجعة الداخلية ودعم الإدارة كمتغيرات مستقلة للفرض الفرعي الأول والثاني والثالث والرابع على التوالي والحد من مخاطر الأمن السيبراني كمتغير تابع ، كما تم قياس اثر الحد من مخاطر الأمن السيبراني كمتغير مستقل على ترشيد قرارات المستثمرين كمتغير تابع في الفرض الثاني .

5/2 النتائج الإحصائية للدراسة الميدانية

5/2/1 اختبار الصدق والثبات

تم اختبار الثبات والصـــدق من خلال مقياس ألفا كرونباخ لتغيرات البحث فإذا زاد هذا المقياس عن 0.60 (Reddy, 2020, Pp.178-188) أمكن الاعتماد على نتائج الدراســة وتعميمها على المجتمع وذلك طبقاً لما جاء في الجدول رقم (7) التالي :

جدول رقم (7)

إختبار الصدق والثبات لمحاور الإستبيان

محاور الاستبيان	العبارات	معامل الصدق	معامل الثبات
1- العوامل التي تؤثر على المقدرة المهنية لفريق المراجعة الداخلية.	5	0.772	0.878
2- العوامل التي تؤثر على مشـــاركة المراجعة الداخلية في إدارة المخاطر المؤسسية .	5	0.717	0.846
3- العوامل التي تؤثر على جودة تنفيذ المهام.	5	0.709	0.842
4- العوامل التي تؤثر على حجم قسم المراجعة الداخلية ودعم الإدارة .	6	0.714	0.844
5- آلية الحد من مخاطر الأمن السيبراني .	6	0.732	0.855
6- الحد من مخاطر الأمن السـيبراني وترشـيد قرارات المستثمرين	6	0.728	0.853
الاستمارة ككل	33	0.907	0.952

وتم اســتخدام معامل الثبات(Alpha Cronbach) ومعامل الصــدق الذاتي لقياس ثبات المحتوى للدراســة ككل وقد ظهرت النتائج من برنامج SPSS أن معامل الثبات بلغ (0.952) كما بلغ معامل الصـــدق (0.907) وهي قيمة معقولة تعبر عن إرتفاع درجة التناســق بين المتغيرات داخل القائمة وكذلك عن إرتفاع درجة التجانس بين الإجابات الواردة في مفردات العينة .

النتائج الإحصائية لاختبار الفرض الأول :

الفرض الأول الرئيســـي : توجد علاقة تأثير إيجابية ذات دلالة إحصـــائية بين محددات جودة المراجعة الداخلية والحد من مخاطر الأمن السيبراني .

وهناك فروض فرعية كما هي :

الفرض الفرعي الأول : توجد علاقة تأثير إيجابية ذات دلالة إحصائية بين المقدرة المهنية لفريق المراجعة الداخلية والحد من مخاطر الأمن السيبراني.

الفرض الفرعي الثاني : توجد علاقة تأثير إيجابية ذات دلالة إحصـــائية بين مشـــاركة المراجعة الداخلية في إدارة المخاطر المؤسسية والحد من مخاطر الأمن السيبراني.

الفرض الفرعي الثالث : توجد علاقة تأثير إيجابية ذات دلالة إحصـــائية بين جودة تنفيذ المهام والحد من مخاطر الأمن السيبراني .

الفرض الفرعي الرابع : توجد علاقة تأثير إيجابية ذات دلالة إحصـــائية بين حجم قســـم المراجعة الداخلية ودعم الإدارة والحد من مخاطر الأمن السيبراني .

تم حساب المتوسط الحسابي والإنحراف المعياري لعبارات الفرض الأول الرئيسي والتي تظهر في الجدول رقم (8) التالي :

جدول رقم (8)

المتوسط الحسابي والإنحراف المعياري لعبارات الفرض الأول

العبارة	المتوسط	الانحراف المعياري	معامل الاختلاف	الترتيب
(1) المحور الأول : محددات جودة المراجعة الداخلية (يتفرع منه المحاور التالية) :				
1/1 المحور الفرعي الأول : المقدرة المهنية لفريق المراجعة الداخلية .				
1/1/1 توافر المؤهلات العلمية اللازمة لإنجاز المهام .	**4.424**	**0.611**	**0.371**	**1**

2/1/1 توافر الشهادات المهنية المناسبة لإنجاز المهام .	4.322	0.731	0.532	3
3/1/1 توافر الخبرة والمعرفة اللازمة لعمليات المنشأة .	4.211	0.762	0.579	5
4/1/1 توافر المعرفة التكنولوجية لإنجاز المهام .	4.382	0.677	0.456	2
5/1/1 توافر عدد ساعات تدريب وتعليم مستمر لإنجاز المهام .	4.299	0.733	0.534	4
1/2 المحور الفرعي الثاني : مشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية .				
1/1/2 القيام بالتحديث والمتابعة الدورية لمختلف أُطر المخاطر التي تتعرض لها المنشأة .	3.991	0.904	0.814	4
2/1/2 المساهمة في تقديم توصيات ومقترحات للإدارة بشأن الحد المقبول من المخاطر .	4.216	0.813	0.658	3
3/1/2 تقديم المشورة لإدارة المنشأة بشأن تحديد أفضل الطرق لتحقيق الأهداف في ظل المخاطر التي تمر بها المنشأة .	3.961	0.993	0.982	5
4/1/2 تطوير وتنمية الإستراتيجيات المتبعة لإدارة المخاطر .	4.507	0.595	0.352	1
5/1/2 تقديم التقارير المتعلقة بمدى صدق إدارة المخاطر بالمنشأة في إعداد تقاريرها .	4.274	0.800	0.637	2

1/3 المحور الفرعي الثالث : جودة تنفيذ المهام .				
1/1/3 وجود نظام لرقابة جودة الأداء .	3.974	0.966	0.931	5
2/1/3 بذل العناية المهنية الواجبة تجاه أداء المهام .	4.319	0.631	0.396	2
3/1/3 تحديد الإجراءات التي يجب إتباعها في عمليات التخطيط والتوثيق والمشورة .	4.074	0.891	0.792	4
4/1/3 الإلتزام بالمعايير المهنية المتعارف عليها .	4.341	0.602	0.360	1
5/1/3السعي نحو المحافظة على الجودة وإستمرارية تحسينها .	4.216	0.748	0.557	3
1/4 المحور الفرعي الرابع : حجم قسم المراجعة الداخلية ودعم الإدارة .				
1/1/4 عدد مرات الإجتماعات مع لجان المراجعة .	4.241	0.699	0.486	3
2/1/4 المساهمة في تفعيل عمليات الحوكمة وتحقيق أهدافها.	4.286	0.703	0.492	2
3/1/4 العمل على إدارة وإكتشاف المخاطر .	4.319	0.730	0.531	1
4/1/4 تقديم تأكيد موضوعي إلى مجلس الإدارة عن مدى فعالية أنشطة الإدارة الشاملة للمخاطر .	4.124	0.806	0.647	4
5/1/4 التأكد من أن نظام الرقابة يعمل بفعالية .	4.056	0.734	0.537	5

6/1/4 توافر الدعم والتمويل والتعاون الكافي من الإدارة العليا .	4.106	0.633	0.398	6
(2) المحور الثاني : آلية الحد من مخاطر الأمن السيبراني .				
1/2 تحديد المخاطر السيبرانية وكيفية قياسها .	4.230	0.585	0.341	3
2/2 تصميم وإختبار نظام مراقبة الأمن السيبراني .	4.026	0.855	0.713	5
3/2 إختبار الفعالية التشغيلية لرقابة الأمن السيبراني .	4.243	0.788	0.621	2
4/2 الإفصاح عن ممارسات إدارة مخاطر الأمن السيبراني .	3.816	0.936	0.875	6
5/2 تقديم خدمة التوكيد على تقارير الإفصاح عن إدارة مخاطر الأمن السيبراني .	4.432	0.659	0.431	1
6/2 توفير محتوى مرتبط بالمفاهيم الأساسية لتقنيات إدارة المخاطر السيبرانية .	4.172	0.795	0.631	4

ومن الجدول رقم (8) نجد أن متوسط جميع العبارات أكبر من (3) وهذا يدل على أن هناك علاقة بين محددات جودة المراجعة الداخلية والحد من مخاطر الأمن السيبراني وذلك من وجهة نظر عينة الدراسة كما نلاحظ أيضاً أن الإنحراف المعياري العام لجميع العبارات أقل من الواحد وذلك يدل على إنخفاض التشتت في إستجابات العينة لهذه العبارات وأن إتجاهات مفردات عينة البحث قد أظهرت إتجاهاً عاماً نحو الموافقة على أهمية وجود علاقة بين محددات جودة المراجعة الداخلية والحد من مخاطر الأمن السيبراني وقد كانت من أكثر العبارات أهمية بالنسبة للعوامل التي تؤثر على المقدرة المهنية لفريق المراجعة الداخلية في الفرض الفرعي الأول العبارة رقم

(1/1/1) والمتعلقة بتوافر المؤهلات العلمية اللازمة لإنجاز المهام حيث ظهرت في المرتبة الأولى وحصلت على معامل اختلاف معياري قدره 0.371 وإنحراف معياري قدرة 0.611 ومتوسط قيمته 4.424 ، ثم جاء في الفرض الفرعي الثاني مشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية العبارة رقم (4/1/2) والمتعلقة بتطوير وتنمية الإستراتيجيات المتبعة لإدارة المخاطر في المرتبة الأولى حيث حصلت على معامل اختلاف معياري قدره 0.352 وإنحراف معياري قدرة 0.595 ومتوسط قيمته 4.507 ، وجاء في الفرض الفرعي الثالث جودة تنفيذ المهام العبارة رقم (4/1/3) والمتعلقة بالإلتزام بالمعايير المهنية المتعارف عليها في المرتبة الأولى حيث حصلت على معامل اختلاف معياري قدره 0.360 وإنحراف معياري قدرة 0.602 ومتوسط قيمته 4.341 ، ثم جاء في الفرض الفرعي الرابع حجم قسم المراجعة الداخلية ودعم الإدارة العبارة رقم (3/1/4) والمتعلقة بالعمل على إدارة وإكتشاف المخاطر وخاصةً السيبرانية في المرتبة الأولى حيث حصلت على معامل اختلاف معياري قدره 0.531 وإنحراف معياري قدرة 0.730 ومتوسط قيمته 4.319 ، ثم جاء في المحور الثاني آلية الحد من مخاطر الأمن السيبراني العبارة رقم (5/2) والمتعلقة بتقديم خدمة التوكيد على تقارير الإفصاح عن إدارة مخاطر الأمن السيبراني حيث حصلت على معامل اختلاف معياري قدره 0.431 وإنحراف معياري قدرة 0.659 ومتوسط قيمته 4.432 .

باستخدام نموذج تحليل الإنحدار للفرض الأول الموضح في الجدول رقم (9) والذي يشير إلى أن هناك علاقة إيجابية ذات دلالة إحصائية بين محددات جودة المراجعة الداخلية والتي تضم (المقدرة المهنية لفريق المراجعة الداخلية – مشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية – جودة تنفيذ المهام – حجم قسم المراجعة الداخلية ودعم الإدارة) والحد من مخاطر الأمن السيبراني بمستوى معنوية 0.000 كما أن معامل الارتباط يشير إلى قوة العلاقة بين محددات جودة المراجعة الداخلية والتي تضم (المقدرة المهنية لفريق المراجعة الداخلية – مشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية – جودة تنفيذ المهام – حجم قسم المراجعة الداخلية ودعم الإدارة) والحد من مخاطر الأمن السيبراني بقيمة 0.804 كما أن معامل التحديد يعني محددات جودة المراجعة الداخلية الأربعة تفسر وحدها بمقدار 64.3% تقريباً من إجمالي

التغير في الحد من مخاطر الأمن السـيبراني من وجهة نظر أفراد العينة الأربعة من مسـئولي المراجعة الداخلية ، مسئولي تكنولوجيا المعلومات ، مسئولي إدارة المخاطر ، المستثمرين (من خلال شركات وساطة وتداول الأوراق المالية) .

جدول رقم (9)

نتائج إختبار الفرض الرئيسي الأول بإستخدام نموذج تحليل الإنحدار

المتغيرات	R	R Square	F	Sig
(Constant)	.804	0.643	52.019	(0.000)

تشـير نتائج اسـتخدام نموذج تحليل الانحدار للفرض الفرعي الأول من الفرض الرئيسـي الأول الموضحة (بالجدول رقم 10) إلى وجود علاقة إيجابية بين المقدرة المهنية لفريق المراجعة الداخلية والحد من مخاطر الأمن السيبراني بمستوى معنوية 0.000 ومعامل الارتباط الذي يشير إلى قوة العلاقة بقيمه قدرها 0.733 كما أن معامل التحديد فسـر 53.9% من إجمالي التغير للحد من مخاطر الأمن السـيبراني وذلك من وجهة نظر مفردات المجموعات الأربعة لعينة الدراسة .

جدول رقم (10)

نتائج إختبار الفرض الفرعي الأول بإستخدام نموذج تحليل الإنحدار

	R	R Square	F	Sig
الفرض الفرعي الأول	.733	0.539	137.525	.000

كما تشير نتائج استخدام نموذج تحليل الانحدار للفرض الفرعي الثاني من الفرض الرئيسي الأول موضحة في الجدول رقم (11) إلى وجود علاقة إيجابية بين مشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية والحد من مخاطر الأمن السيبراني بمستوى معنوية 0.000 ومعامل الارتباط الذي يشير إلى قوة العلاقة بقيمة قدرها 0.656 كما أن معامل التحديد يفسر 43.4%

من إجمالي التغير للحد من مخاطر الأمن الســـيبراني وذلك من وجهة نظر مفردات المجموعات الأربعة لعينة الدراسة .

جدول رقم (11)

نتائج إختبار الفرض الفرعي الثاني بإستخدام نموذج تحليل الإنحدار

	R	R Square	F	Sig
الفرض الفرعي الثاني	.656	0.434	90.064	.000

كما تشير نتائج استخدام نموذج تحليل الانحدار للفرض الفرعي الثالث من الفرض الرئيسي الأول موضــحة في الجدول رقم (12) إلى وجود علاقة إيجابية بين جودة تنفيذ المهام والحد من مخاطر الأمن الســيبراني بمســتوى معنوية 0.000 ومعامل الارتباط الذي يشــير إلى قوة العلاقة 0.725 كما أن معامل التحديد يفســـر 52.2% من إجمالي التغير للحد من مخاطر الأمن السيبراني وذلك من وجهة نظر مفردات المجموعات الأربعة عينة الدراسة .

جدول رقم (12)

نتائج إختبار الفرض الفرعي الثالث بإستخدام نموذج تحليل الإنحدار

	R	R Square	F	Sig
الفرض الفرعي الثالث	.725	0.522	129.500	.000

كما تشـــير نتائج اســـتخدام نموذج تحليل الانحدار للفرض الفرعي الرابع من الفرض الأول موضــحة في الجدول رقم (13) إلى وجود علاقة إيجابية بين حجم قسـم المراجعة الداخلية ودعم الإدارة والحد من مخاطر الأمن السيبراني بمستوى معنوية 000.ومعامل الارتباط الذي يشير إلى قوة العلاقة بقيمة قدرها 0.699 كما أن معامل التحديد يفســر 48.9% من إجمالي التغير للحد من مخاطر الأمن السيبراني وذلك من وجهة نظر مفردات المجموعات الأربعة لعينة الدراسة .

جدول رقم (13)

نتائج إختبار الفرض الفرعي الرابع بإستخدام نموذج تحليل الإنحدار

	R	R Square	F	Sig
الفرض الفرعي الرابع	.699	0.489	112.262	.000

وتشير نتائج اختبار Kruskal Wallis Test إلى عدم وجود فروق معنوية بين آراء مسئولي المراجعة الداخلية ، مسئولي تكنولوجيا المعلومات ، مسئولي إدارة المخاطر ، وذلك بمستوى معنوية أكبر من 0.05 وبالتالي اتفاق المجموعات الأربعة على وجود علاقة إيجابية بين جودة المراجعة الداخلية (المقدرة المهنية لفريق المراجعة الداخلية – مشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية – جودة تنفيذ المهام – حجم قسم المراجعة الداخلية ودعم الإدارة) والحد من مخاطر الأمن السيبراني ويمثل المستثمرين (من خلال شركات وساطة وتداول الأوراق المالية) أعلى نسبة موافقة بين أفراد العينة بالنسبة لحجم قسم المراجعة الداخلية ودعم الإدارة بقيمة قدرها 71.54% ويأتي مسئولي المراجعة الداخلية أعلى نسبة موافقة بين أفراد العينة بالنسبة لمشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية بقيمة قدرها 69.82% بينما مسئولي إدارة المخاطر أعلى نسبة موافقة بين أفراد العينة بالنسبة لجودة تنفيذ المهام بقيمة قدرها 67.71% وأخيراً يكون مسئولي تكنولوجيا المعلومات أعلى نسبة موافقة بين أفراد العينة بالنسبة للمقدرة المهنية لفريق المراجعة الداخلية بقيمة قدرها 65.88% كما تظهر في الجدول التالي :

جدول رقم (14)

نتائج إختبار Kruskal Wallis حول الفروق المعنوية بين آراء الفئات المستقصى منهم فيما يتعلق بالفرض الأول

الفرض الأول	مسئولي المراجعة الداخلية	مسئولي تكنولوجيا المعلومات	مسئولي إدارة المخاطر	المستثمرين (من خلال شركات وساطة	Asyma Sig

				وتداول الأوراق المالية	
المقدرة المهنية لفريق المراجعة الداخلية	56.90	65.88	64.21	60.87	0.627
مشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية	69.82	43.91	60.21	61.22	0.100
جودة تنفيذ المهام	60.16	58.75	67.71	55.74	0.518
حجم قسم المراجعة الداخلية ودعم الإدارة	55.61	66.71	60.92	71.54	0.403

الفرض الثاني : توجد علاقة تأثير إيجابية ذات دلالة إحصائية بين الحد من مخاطر الأمن السيبراني وترشيد قرارات المستثمرين .

تم حساب المتوسط الحسابي والإنحراف المعياري لعبارات الفرض الثاني والتي تظهر في الجدول رقم (15) التالي :

جدول رقم (15)

المتوسط الحسابي والإنحراف المعياري لعبارات الفرض الثاني

العبارة	المتوسط	الانحراف المعياري	معامل الاختلاف	الترتيب
(3) المحور الثالث : العلاقة بين الحد من مخاطر الأمن السيبراني وترشيد القرار الإستثماري .				
1/3 يهتم المستثمرون بالإفصاح عن المخاطر لتحديد الغرض والتحديات التي تواجههم .	4.224	0.836	0.696	3

2/3 إهتمام الإدارة العليا بالإفصاح عن المخاطر يدعم جذب المزيد من المستثمرين ويمثل قيمة مضافة للمنشأة .	4.057	0.962	0.923	6
3/3 الإفصاح عن المخاطر يساعد في تحقيق عدم تماثل المعلومات بين المستثمرين والإدارة .	4.241	0.595	0.352	2
4/3 نشر المعلومات عن المخاطر في التوقيت المناسب يمكن المستثمرين من إتخاذ القرارات الإستثمارية الرشيدة .	4.174	0.865	0.750	5
5/3 قيام المنشأة بتوفير قاعدة بيانات حالية ومستقبلية عن المخاطر يساهم في مساعدة المستثمرين في إتخاذ قراراتهم .	4.299	0.666	0.540	1
6/3 زيادة الهجمات السيبرانية على المنشأة بدون رقابة تحد من رغبة المستثمرين في الإستثمار .	4.182	0.851	0.723	4

ومن الجدول رقم (15) نجد أن متوسط جميع العبارات أكبر من (3) وهذا يدل على أن هناك علاقة بين الحد من مخاطر الأمن السيبراني وترشيد القرار الإستثماري ، وذلك من وجهة نظر عينة الدراسة كما نلاحظ أيضاً أن الإنحراف المعياري العام لجميع العبارات أقل من الواحد وذلك يدل على إنخفاض التشتت في إستجابات العينة لهذه العبارات وأن إتجاهات مفردات عينة البحث قد أظهرت إتجاهاً عاماً نحو الموافقة على البنود وقد كانت من أكثر العبارات أهمية في الإجابة هي العبارة رقم (5/3) والمتعلقة بقيام المنشأة بتوفير قاعدة بيانات حالية ومستقبلية عن المخاطر يساهم في مساعدة المستثمرين في إتخاذ قراراتهم حيث حصلت على معامل اختلاف معياري قدره 0.540 وإنحراف معياري قدرة 0.666 ومتوسط قيمته 4.299 ، وجاء في المرتبة الثانية العبارة رقم

(3/3) والمتعلقة بالإفصاح عن المخاطر يساعد في تحقيق عدم تماثل المعلومات بين المستثمرين والإدارة حيث حصلت على معامل اختلاف معياري قدره 0.352 وإنحراف معياري قدرة 0.595 ومتوسط قيمته 4.241 ، وجاء في المرتبة الثالثة العبارة رقم (1/3) والمتعلقة بإهتمام المستثمرون بالإفصاح عن المخاطر لتحديد الغرض والتحديات التي تواجههم حيث حصلت على معامل اختلاف معياري قدره 0.696 وإنحراف معياري قدرة 0.836 ومتوسط قيمته 4.224 ، وجاء في المرتبة الرابعة العبارة رقم (6/3) والمتعلقة بزيادة الهجمات السيبرانية على المنشأة بدون رقابة تحد من رغبة المستثمرين في الإستثمار حيث حصلت على معامل اختلاف معياري قدره 0.723 وإنحراف معياري قدرة 0.851 ومتوسط قيمته 4.182 ، وجاء في المرتبة الخامسة العبارة رقم (4/3) والمتعلقة بنشر المعلومات عن المخاطر في التوقيت المناسب يمكن المستثمرين من إتخاذ القرارات الإستثمارية الرشيدة حيث حصلت على معامل اختلاف معياري قدره 0.750 وإنحراف معياري قدرة 0.865 ومتوسط قيمته 4.174 ، ثم جاء في المرتبة السادسة العبارة رقم (2/3) إهتمام الإدارة العليا بالإفصاح عن المخاطر يدعم جذب المزيد من المستثمرين ويمثل قيمة مضافة للمنشأة حيث حصلت على معامل اختلاف معياري قدره 0.923 وإنحراف معياري قدرة 0.962 ومتوسط قيمته 4.057.

باستخدام نموذج تحليل الانحدار للفرض الثاني موضحة في الجدول رقم (16) إلى أن هناك علاقة إيجابية ذات دلالة إحصائية بين الحد من مخاطر الأمن السيبراني وترشيد قرارات المستثمرين بمستوى معنوية 000. ومعامل الارتباط الذي يشير إلى قوة العلاقة بين الحد من مخاطر الأمن السيبراني وترشيد قرارات المستثمرين بقيمة قدرها 0.785 كما أن معامل التحديد يعني الحد من مخاطر الأمن السيبراني تفسر وحدها بمقدار 61.4% تقريباً من إجمالي التغير في ترشيد قرارات المستثمرين من وجهة نظر أفراد العينة الأربعة من مسئولي المراجعة الداخلية ، مسئولي تكنولوجيا المعلومات ، مسئولي إدارة المخاطر ، المستثمرين (من خلال شركات وساطة وتداول الأوراق المالية) .

جدول رقم (16)

نتائج إختبار الفرض الثاني بإستخدام نموذج تحليل الإنحدار

	R	R Square	F	Sig
الفرض الثاني	0.785	0.614	188.69	0.000

كما أثبتت نتائج اختبار Kruskal Wallis بناء على تحليل إستجابات مفردات المجموعات الأربعة لعينة الدراسة فيما يتعلق بإختبار الفرض الثاني حيث تشير النتائج إلى أنه لا توجد فروق معنوية بين آراء مسئولي المراجعة الداخلية ، مسئولي تكنولوجيا المعلومات ، مسئولي إدارة المخاطر ، المستثمرين (من خلال شركات وساطة وتداول الأوراق المالية) حيث كان مستوى المعنوية أكبر من 0.05 وبالتالي إتفاق المجموعات الأربعة على وجود علاقة بين الحد من مخاطر الأمن السيبراني وترشيد قرارات المستثمرين ويمثل المستثمرين (من خلال شركات وساطة وتداول الأوراق المالية) أعلى نسبة موافقة بين أفراد العينة 68% ويليه مسئولي المراجعة الداخلية بنسبة 64.42% ثم مسئولي إدارة المخاطر بنسبة 62.05% ثم مسئولي تكنولوجيا المعلومات بنسبة 56.18% كما تظهر في الجدول التالي :

جدول رقم (17)

نتائج إختبار Kruskal Wallis حول الفروق المعنوية بين آراء الفئات المستقصى منهم فيما يتعلق بالفرض الثاني

الفرض الثاني	مسئولي المراجعة الداخلية	مسئولي تكنولوجيا المعلومات	مسئولي إدارة المخاطر	المستثمرين (من خلال شركات وساطة وتداول الأوراق المالية)	Asymp Sig
	64.42	56.18	62.05	68.00	0.304

النتائج والتوصيات والتوجهات المستقبلية .

يتناول هذا الجزء من البحث عرضا لنتائج البحث ، وتوصياته ، ومجالات البحث المقترحة ، وذلك علي النحو التالي :

أولاً – النتائج :

تناول البحث دراسة واختبار أثر جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني وإنعكاساته على ترشيد قرارات المستثمرين (دراسة ميدانية) ، ويمكن عرض اهم نتائج البحث ، بشقيه النظري والميداني علي النحو التالي :

1- التطور الحادث في المخاطر السيبرانية يحفز المنشات على البحث المستمر والمكثف نحو إتخاذ إجراءات وقائية ضد تلك المخاطر من خلال لوائح تجعل تلك الإجراءات أكثر وضوحاً أمام مجالس إدارات تلك المنشات الأمر الذي يؤدي إلى خلق حافز أكبر على العمل بشكل مستمر في تحسين الأمن السيبراني .

2- تحتاج المراجعة الداخلية في معظم المنشآت الي توسيع قاعدة مهاراتها و اجتذاب مهارات فنية مؤهلة بكافة وسائل التعامل مع تقنيات التكنولوجيا .

3- لن يستطيع أصحاب المصالح وخاصة المستثمرين متابعة عمليات المخاطر السيبرانية إلا بمساعدة المراجعة الداخلية ، نظراً لأنه بناء على ما يوفره المراجع الداخلي من إمكانيات بشكل رشيد سوف يحقق أقصى عائد ومنفعة تتوافق مع طلبات وإحتياجات المستثمرين .

4- كما أثبتت نتائج الدراسة الميدانية أن نتائج اختبار **Kruskal Wallis Test** تشير إلى عدم وجود فروق معنوية بين آراء مسئولي المراجعة الداخلية ، مسئولي تكنولوجيا المعلومات ، مسئولي إدارة المخاطر ، وذلك بمستوى معنوية أكبر من **0.05** وبالتالي اتفاق المجموعات الأربعة على وجود علاقة إيجابية بين جودة المراجعة الداخلية (المقدرة المهنية لفريق المراجعة الداخلية – مشاركة المراجعة الداخلية في إدارة المخاطر المؤسسية – جودة تنفيذ المهام – حجم قسم المراجعة الداخلية ودعم الإدارة) والحد من مخاطر الأمن السيبراني ، مما يؤكد على قبول الفرض الأول الرئيسي .

5- كما أثبتت نتائج اختبار Kruskal Wallis بناء على تحليل إستجابات مفردات المجموعات الأربعة لعينة الدراسة فيما يتعلق بإختبار الفرض الثاني حيث تشير النتائج إلى أنه لا توجد فروق معنوية بين آراء مسئولي المراجعة الداخلية ، مسئولي تكنولوجيا المعلومات ، مسئولي إدارة المخاطر ، المستثمرين (من خلال شركات وساطة وتداول الأوراق المالية) حيث كان مستوى المعنوية أكبر من 0.05 وبالتالي إتفاق المجموعات الأربعة على وجود علاقة بين الحد من مخاطر الأمن السيبراني وترشيد قرارات المستثمرين ، مما يعني قبول الفرض الثاني .

ثانياً – التوصيات :

وفي ضوء النتائج السابقة توصى الباحثة بالآتي :

1- على المراجع الداخلي أن يُعيد تأهيل ذاته بمهارات وقدرات تؤهله لكي يكون شريكاً إستراتيجياً مضيفاً للقيمة ومرشداً لقرارات أصحاب المصالح وخاصة المستثمرين .

2- ضرورة قيام ادارة المراجعة الداخلية بتقديم تقارير مستقلة الي مجلس الادارة ولجنة المراجعة تركز علي مجموعة واسعة من المخاطر و القضايا الرئيسية للمنشأة وخاصة فيما يتعلق بمخاطر الامن السيبراني ، الأمر الذي يترتب عليه تشجيع القرار الإستثماري .

3- دعم وتعزيز المهارات الرقمية للموارد البشرية العاملة بالمنشآت بشكل عام وللمراجعين الداخليين بصفة خاصة ، لضمان كفاءة وفعالية التعامل مع المخاطر السيبرانية والحد منها ، من خلال توفير دورات تدريبية ومنح دراسية وورش العمل .

4- ضرورة قيام المستثمرين بالإطلاع بشكل جيد على تقارير مخاطر الأمن السيبراني في المنشآت موضع إستثماراتهم نظراً لأهميتها القصوى في توضيح الرؤى المستقبلية حول الموقف المالي والتشغيلي وإستمرارية تلك المنشآت ، بما يدعم قراراتهم الإستثمارية .

5- ضرورة اهتمام الهيئة العامة للرقابة المالية بتوجيه وزيادة وعي المنشآت باهمية الافصاح عن تقرير ادارة مخاطر الامن السيبراني ، من خلال نشر ثقافة الافصاح الاختياري عن هذه المعلومات في التقارير السنوية للمنشآت ، عن طريق اصدار المعايير الارشادية التي تنظم عملية اعداد و عرض تقرير مخاطر الامن السيبراني و الاستفادة من تجارب الدول الاخري في هذا الشأن .

ثالثاً – التوجهات المستقبلية :

بناء على ما ســـبق ترى الباحثة أن هناك أهمية نحو إتجاه البحوث المســـتقبلية للمجالات التالية :

1- التكامل بين المراجعة الداخلية والخارجية لتحقيق التميز المؤسسي بالوحدات الحكومية .

2- التكامل بين المراجعة الداخلية والخارجية لدعم إدارة المخاطر الرقمية .

3- أثر جودة المراجعة الداخلية للأمن السيبراني على جودة إعداد التقارير المالية .

4- أثر فعالية المراجعة الداخلية للأمن السيبراني على الحد من الجرائم المالية .

قائمة المراجع :

أولاً – قائمة المراجع العربية :

البغدادي ، مروة فتحي السيد ، (2021) ، اقتصاديات الأمن السيبراني في القطاع المصرفي ، مجلة البحوث القانونية والاقتصادية كلية الحقوق – جامعة المنصورة ، ع76 ، ص ص 1513 – 1446.

شحاتة ، السيد شحاتة ، (2020) ، إطار مقترح لإسناد وظيفة المراجعة الداخلية بدوريها الاستشاري والتوكيد في مجال إدارة المخاطر في الوحدات الصغيرة ومتوسطة الحجم ،المجلة العلمية التجارة والتمويل ، كلية التجارة – جامعة طنطا ، 40 ، ص ص 109 – 128 .

صالح ، نرمين محمد شاكر إبراهيم ،(2022) ، محددات فعالية المراجع الداخلي للأمن السيبراني ، المؤتمر العلمي الخامس لقسم المحاسبة والمراجعة بعنوان تحديات وآفاق مهنة المحاسبة والمراجعة في القرن الحادي والعشرين ، كلية التجارة – جامعة الإسكندرية ، ص ص 1–24 .

ضيف ، علاء الدين توفيق إبراهيم ، (2016) ، دور المراجعة القضائية في الحد من التلاعب في بيئة المعلومات الرقمية للشركات دراسة ميدانية في بيئة الأعمال السعودية مجلة البحوث المحاسبية قسم المحاسبة – كلية التجارة – جامعة طنطا المجلد الثالث العدد الأول ، ص ص 496 – 554 .

عثمان ، محمد أحمد ، (2022) ، محددات فعالية وظيفة المراجعة الداخلية في إدارة مخاطر الأمن السيبراني ، المؤتمر العلمي الخامس لقسم المحاسبة والمراجعة بعنوان تحديات وآفاق مهنة المحاسبة والمراجعة في القرن الحادي والعشرين ، كلية التجارة – جامعة الإسكندرية ، ص ص 1–21 .

على ، محمود أحمد أحمد ، وعلي ، صالح علي صالح ، (2022) ، أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية (دراسة تجريبية) ، المؤتمر العلمي الخامس لقسم المحاسبة والمراجعة

بعنوان تحديات وآفاق مهنة المحاسبة والمراجعة في القرن الحادي والعشرين ، كلية التجارة – جامعة الإسكندرية ، ص ص 17-32 .

ثانياً – قائمة المراجع الأجنبية :

Alina , C. M., Cerasela S.E., and Gabriela G, (2017) ,Internal audit role in cybersecurity ovidius university Annals Economic Sciences Series 17 (2) Pp. 510 – 513 .

Al-Moshaigeh, A., Dickins, D. and Higgs, J. (2019) , Cybersecurity Risks and Con-trols: Is the AICPA's SOC for Cybersecurity a Solution?, The CPA Journal, Vol. 89, Issue 6, Pp. 36-41.

Badawy, H., (2021) , The Impact of Assurance Quality and Level on Cybersecurity Risk Management Program on Non-Professional Egyptian Investors' Decisions: An Experimental Study, Alexandria Journal of Accounting Research, 3 (5) P.6-7.

Betti N., Sarens G., and Poncin, (2021) ,Effects of digitalisation of organisations on internal audit activities and practices Managerial auditing Journal Vol 36, No 6, Pp. 872 – 888

Christ M., Masli N., Sharip N., and Wood D., (2015) ,Rotational internal audit programs and financial reporting quality Do compensating controls help ? accounting Organizations and society Vol., 44 , Pp. 37 – 59.

Committee of sponsoring organizations of the treadway commission (COSO), (2019) ,Enterprise wide management (ERM) for Cybersecurity available at http://www.coso.org/documents/COSO-Deloitte-Managing-Cyber-Risk-in-a-Digital-Age.pdf

Deloitte, Development LLC, (2017), Cyber security and role of internal audit an urgent call to action, available at www2.deloitte.com .

Ege M., (2015) ,Does internal audit function quality deter management misconduct ? the accounting review Vol., 90 No., 2, Pp. 495 – 497.

Eling M. and J.H. wirfs , (2016), Cyber Risk : too big toinsure ? Risk transfer options for a mercurial risk class institute of Insurance Economics Univesity of St. Gallen , Pp. 23-57 .

Florakis C.C. Louca R. Michaely and M Weber, (2020) ,Cybersecurity Risk, Pp. 1-73, Available at http://ssrn.com

Frank, M., Grenier, J. and Pyzoha, J., (2019) , How Disclosing a Prior Cyberattack Influences the Efficacy of Cybersecurity Risk Management Reporting and Independent Assurance, Journal of Information Systems, 33 (3) , Pp. 183-200 .

Hartmann C.C. and J. Carmenate, (2021) ,Academic Research on the Role of Corporate Governance and IT Expertise in Addressing Cybersecurity Breaches Implications for Practice Policy and Research, American Accounting Association, 15 (2) Pp. 9 - 23 .

Heroux, S. and Anne, F., (2020) , Cybersecurity Disclosure by the Companies on the S&PTSX 60 Index, Accounting Perspectives/Perspectives Compatibles, 19 (2), Pp. 73-100 .

Hilary, G., Segal, B., and Zhang, M., (2016) , Cyber-risk disclosure: Who cares? Research paper, Pp. 1-59, https://papers.ssrn.com.

Information Systems Audit and Control Association (ISACA), (2017), Available at: https://www.isaca.org/en/resources/isaca-journal/issues/2017/volume-3 .

Institute of internal auditors (IIA), (2013) ,international standards for the professional practice of internal auditing .

Institute of internal auditors (IIA), (2016) ,assessing cybersecurity Risk Roles of the three lines of Defense available at : guidance@theiia.org

Institute of internal auditors (IIA), (2017) ,international standards for the professional practice of internal auditing institute of internal auditors (IIA) report available at : guidance@theiia.org

Institute of internal auditors (IIA), (2020) ,North american pulse of internal audit available at http://theiia.mkt5790.com/2020-pulse-of-internal-audit .

International Accreditation Forum (IAF), (2021) , Available at: https://iaf.nu/en/home/ .

ISACA, (2019) ,auditors have a role in cyber resilience ISACA JOURNAL VOL 6 available at www.isaca.org

Islam M.S, Nusrat Farah, Thomas F. Stafford., (2018) ,Factors associated with security / cyber security audit by internal audit function an international study Managerial auditing journal , Pp. 377- 409, available at :10.1108/MAJ-07/2017-1595

Kahyaoglu S.B and K. Caliyurt, (2018) ,Cyber security assurance process from the internal audit perspective managerial audit J. 33 (4) Pp. 360 – 376 available at http://doi.org/10.1108/MAJ-02-2018-1804

Kamiya, S., Kang, J., Kim, J., and Stulz, R., (2021), Risk management, firm reputation, and the impact of successful

cyberattacks on target firms, Journal of Financial Economics, Pp. 719–749 .

Kelton, A. and Pennington, R., (2020) , Do Voluntary Disclosures Mitigate the Cybersecurity Breach Contagion Effect?, Journal of Information Systems, 34 (3), Pp. 133-157.

Li H. W.G.No and T. Wang , (2018) ,SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors International Journal of Accounting Information Systems, 30, Pp.40 – 55

Lois petros, George Drogalas, Alkiviadis Karagiorgos, Alkis Thrassou and Demetris Vrontis (2021) ,internal auditing and cyber security audit role and procedural contribution, international Journal of managerial and financial accounting, Vol. 13, No1 , Pp.25-47 ,available at : http://www.researchgate.net/publication/353255386 DOI 10.1504/IJMFA2021.116207

National institute of standards and technology (NIST) (2018) , a Glossary of key information security terms National institute of standards and technology interagency or internal report available at http://csrc.nist.gov/publications

PricewaterhouseCoopers (PWC), (2018) ,Internal Audit Available at www.pwc.org .

Reddy, C. D. (2020) , "Teaching Research Methodology: Everything'sa Case." Electronic Journal of Business Research Methods, Vol.18, No.2, Pp. 178-188.

sergeja slapni car, Sergeja Slapničar, Marko Čular, Matej Drašček (2022) ,Effectiveness of cyber security audit, international

Journal of accounting information systems, Pp.1-21, available at : http://doi.org/10.1016/j.accinf.2021.100548

Shahimi S. and N. Mahzan, (2018) ,Building a research model and hypotheses development and findings of Exploratory Interviews International Journal of Management Excellence 10 (2) Pp. 1257 – 1283.

Shamsuddn , amanuddinn, (2018) ,the EFFECTIVENESS of internal audit functions in managing cybersecurity in malaysia's Banking institutions international Journal of industrial management IJIM ISSN print 2289 – 9286 Volume 4, Pp. 61-69 .

Steinbart P.J., Raschke R. L. Gal G and Dilla W.N. (2018) the influence of a good relationship between the internal audt and information security functions on information security outcomes accounting organizations and society Vol., 71 Pp. 15-29 .

Tuson, O., (2021), Cyber-attacks and stock market activity, International Review of Financial Analysis,Pp.1-15.

Vuko Tina, Sergeja Slapničar, Marko Čular, Matej Drašček, (2021) ,key drivers of cyber security audit effectiveness the neo-institutional perspective, Pp.1-43 available at http://ssrn.com/abstract=3932177 .

Weijters, Bert, Kobe Millet, and Elke Cabooter. (2021) ,"Extremity in Horizontal and Vertical Likert Scale Format Responses. Some Evidence on How Visual Distance Between Response Categories Influences Extreme Responding" . International Journal of Research in Marketing, Vol.38, No.1, Pp .85-103.

Yang, L., Lau, L. and Jan, H. (2020) . Investors' perceptions of the cybersecurity risk management reporting framework. International Journal of Accounting & Information Management, Vol. 28 No. 1, Pp. 167-183.