القيمة المضافة من توكيد المراجع الداخلي على مزاعم الإدارة عن إدارة مخاطر الأمن السيبراني – الدور المُعدّل لطبيعة إسناد وظيفة المراجعة الداخلية ونوع وخبرة أصحاب المصالح: دراسة تجريبية

دكتور/ محمد إبراهيم عبده الفار

مدرس بقسم المحاسبة والمراجعة – كلية التجارة – جامعة دمنهور.

mohmedelfar@hotmail.com

دكتور/ ياسر محمد عبدالله

مدرس بقسم المحاسبة والمراجعة – كلية التجارة – جامعة دمنهور. ysa@gulf.edu.sa

الملخص:

استهدف البحث دراسة واختبار أثر توكيد المراجع الداخلي على مزاعم إدارة المخاطر بشأن إدارة مخاطر الأمن السيبراني على القيمة المضافة من وظيفة المراجعة الداخلية؛ كما تم اختبار أثر الإسناد الخارجي لوظيفة المراجعة الداخلية، ونوع وخبرة الأطراف أصحاب المصلحة كمتغيرات معدلة للعلاقة محل الدراسة (Moderators)؛ وتحقيقاً لهدف البحث تم إجراء دراسة تجريبية على عينة من الأطراف أصحاب المصلحة والتي بلغت (76) مفردة.

وقد تم ذلك من خلال إجراء تصميم تجريبي (2×3×2)؛ وعمل محاكاة لشركة افتراضية تعمل في مجال الاتصالات وتكنولوجيا المعلومات لديها تقرير من قبّل إدارة المخاطر بشأن إدارة مخاطر الأمن السيبراني؛ في ظل حالتين رئيستين؛ أحداهما تتضمن توكيد من قبّل القائم بوظيفة المراجعة الداخلية على مزاعم إدارة المخاطر بشأن إدارة مخاطر الأمن السيبراني، والأخرى لا تتضمن ذلك.؛ مع وجود مجموعة من المعالجات التي تعكس ضمن الحالتين السابقتين المتغيرات المعدلة للعلاقة محل الدراسة وهي؛ طبيعة إسناد وظيفة المراجعة الداخلية (إسناد داخلي/إسناد خارجي)،

ونوع الأطراف أصحاب المصلحة (ذكر/أنثي)، ومستوي خبرة الأطراف أصحاب المصلحة (مرتفعة/منخفضة).

وقد أظهرت النتائج في ظل التحليل الأساسي وجود تأثير إيجابي معنوي لتوكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني على القيمة المضافة من وظيفة المراجعة الداخلية (مقاسة بمدى التحسن في الأداء التشغيلي للمنشأة، ومدي صدق التقارير والقوائم المالية، ومدي الالتزام بالقوانين واللوائح، مدي تحسن سمعة الشركة مقاسة بحصتها السوقية) مقارنةً بعدم التوكيد؛ ويزداد هذا التأثير الإيجابي المعنوي في حال الإسناد الخارجي لوظيفة المراجعة الداخلية مقارنةً بالإسناد الداخلي لها. كما توصلت النتائج إلى عدم وجود تأثير معنوي لكل من نوع وخبرة الأطراف أصحاب المصالح سواء كانوا داخليين أو خارجيين على العلاقة الرئيسية محل الدراسة. وقد جاءت نتائج التحليل الإضافي والحساسية داعمة لنتائج التحليل الأساسي.

الكلمات المفتاحية: القيمة المضافة لوظيفة المراجعة الداخلية، الأمن السيبراني، إدارة مخاطر الأمن السيبراني، الإسناد الخارجي لوظيفة المراجعة الداخلية، نوع أصحاب المصالح، وخبرة أصحاب المصالح.

The Added Value of Internal Auditor Assurance on Management's Cybersecurity Risk Management Assertions – The Moderating Role of Internal Audit Sourcing, and Stakeholders' Type and Experience: An Empirical Study

Abstract:

This study aims to examine the impact of internal auditor assurance on management's assertions regarding cybersecurity risk management on the added value of the internal audit function. It also investigates the moderating effects of internal

audit sourcing and stakeholders' type and experience on this relationship. To achieve the research objective, an empirical study was conducted on a sample of 76 stakeholders.

The study adopted a 2×3×2 empirical design, using a simulation of a virtual company in the telecommunications and information technology sector. The company issued a report from its risk management department pertaining to cybersecurity risk management under two main conditions: the first was for the internal auditor to provide assurance regarding management's assertions relating to risk management's claims about cybersecurity risk management, and the second was for the internal auditor to provide no such assurance. Within these two conditions, the moderating variables were introduced: internal audit sourcing (internal vs. external), stakeholders' gender (male/female), and stakeholders' experience level (high/low).

The results indicated a significant and positive effect of internal auditor assurance on management's cybersecurity risk management assertions in terms of the added value of the internal audit function. This value was measured by improvements in operational performance, reliability of financial reports and statements, compliance with laws and regulations, and enhanced corporate reputation as reflected in market share. Moreover, the positive effect was more pronounced when the internal audit function was outsourced compared to when it was in-ward. However, no significant moderating effect was found for

stakeholders' type (gender) or experience level, from both internal and external. whether internal or external.

Keywords: Added value of the internal audit function, cybersecurity, cybersecurity risk management, internal audit outsourcing, stakeholders' type, stakeholders' experience.

١- مقدمة البحث:

لقد مهدت الثورة الرقمية العالمية التي تجتاح مختلف القطاعات في الآونة الأخيرة الطريق لإحداث ثورة في الممارسات التقليدية؛ مما أدى إلى رقمنة العمليات المؤسسية[١]، وإحداث تغيرات جذرية في بيئة الأعمال[٢]، وزيادة اعتماد الشركات[٣] على نظم تكنولوجيا المعلومات في إدارة أعمالها وما صاحبها من ظهور تقنيات جديدة تمثل تحدياً كبيراً أمام الشركات مثل الذكاء الاصطناعي، والبيانات الضخمة، والحوسبة السحابية، وانترنت الأشياء (IOT)، وسلاسل الكتل، والروبوتات؛ ورغم أن هذه المفاهيم الرنانة تقدم مجموعة واسعة من الفوائد متمثلة في زيادة كفاءة وفعالية وجودة العمليات، وزيادة رضا العملاء، وتخفيض الوقت اللازم لإنجاز المهام والعمليات، والاستجابة الفورية للتغيرات البيئية، والتحليل الفوري والمنتظم للبيانات المحاسبية،

[١] رقمنة العمليات المؤسسية أو ما يعرف بالتحول الرقمي (Digital Transformation) هو "عملية تغيير جذري وتطوير للبنية التحتية لنماذج الأعمال عن طريق الاعتماد على التقنيات والتطورات التكنولوجية المستحدثة سواء كان ذلك بصورة جزئية أو بصورة كلية لاكتساب ميزة تنافسية وتحقيق قيمة مضافة والسعي نحو تحقيق الأهداف المرجوة من استراتيجيات الأعمال بصفة عامة" (شحاته، ٢٠٢٢).

[٢] في ظل المشهد الرقمي سريع التطور والاعتماد على تقنيات التحول الرقمي فقد تم إحداث تغيرات جذرية في مهنة المحاسبة والمراجعة من خلال إضافة تفاصيل حديثة في دورة حياة نظام المعلومات المحاسبي وتصميمه، وإضافة عناصر حديثة إلى النظام المحاسبي مثل مهارات علوم الحاسب وسلاسل الكتل (Block chain)، وتقليص الوقت والتكلفة، وتقليص المهام التقليدية اليدوية للمحاسب والمراجع واستبدالها بمهام تحليلية وتقييمية واستشارية، وتبادل الأدوار بين الانسان والروبوتات في إجراء العديد من المعالجات المحاسبية وإجراءات الرقابة الداخلية (نافع، ٢٠٢٢ & Vitali and Giuliani, 2024 & Johari et al., 2023).

[٣] يستخدم الباحث لفظ مشروع، منشأة، شركة، مؤسسة، وحدة اقتصادية، وكيان اقتصادي كمترادفات لهم نفس المعنى للإشارة إلى شكل من أشكال منظمات الأعمال التجارية أو الخدمية أو الصناعية؛ والذي يهدف بشكل أساسي إلي تحقيق ربح. وسيتم استخدام لفظ منشأة وشركة كمترادفات لغرض الاتساق.

وبالتالي تحسين عملية اتخاذ القرارات؛ إلا إنها تحمل في طياتها مجموعة من المخاطر والتحديات التي لا تحصى والتي تتعلق بضمان أمن وسلامة نظم المعلومات مما يفرض على المنشآت ضغوطاً كبيرة لحماية نفسها من تلك المخاطر؛ ورداً على تلك المخاطر والتحديات فقد ظهر مفهوم الأمن السيبراني (Johari et al., 2023 & Calvin et al., 2025 & Vitali and Giuliani, 2024 & Abu-Musa, 2006 & Babiker, 2025 & Elqadi et al., 2024 & شحاته، ٢٠٢٢).

وفي السنوات الأخيرة أصبح مفهوم الأمن السيبراني ذو أهمية متزايدة بالنسبة للشركات، وإداراتها، ولجان المراجعة، والمستثمرين؛ إلا أن المخاطر التكنولوجية والتشغيلية والتنظيمية المصاحبة للأمن السيبراني قد أدت إلى زيادة التهديدات الأمنية التي تواجه الشركات، وارتفاع وتيرة الهجمات السيبرانية[١] وهو ما يعرف بمخاطر الأمن السيبراني[٢] (Calvin et al., 2025 & Hossain et al., 2025). وأصبحت مخاطر الأمن السيبراني من بين أكثر فئات مخاطر الأعمال هيمنة على الشركات؛ فوفقا لنتائج دراسة استقصائية تمت بواسطة الاتحاد الأوروبي لمعهد المراجعين الداخليين (ECIIA) على عدد (٥٧٩) من كبار مسئولي المراجعة الداخلية تم تصنيف مخاطر الأمن السيبراني كأحد أهم خمسة مخاطر تجارية تواجه الشركات بمختلف أحجامها وأنواعها (Islam et al., 2018 & Alina et al., 2017 & Loeb and

[١] زادت الهجمات السيبرانية على الشركات المقيدة بالبورصات العالمية بشكل ملحوظ في الفترة الأخيرة بمتوسط ١٦٠ هجوماً إلكترونيا ناجحاً أسبوعيا في عام ٢٠١٤ وهو ما يزيد عن ثلاثة أضعاف متوسط عام ٢٠١٠، فضلاً عن زيادة تلك الهجمات الناجحة في عام ٢٠١٩ لتمثل ٤٠٠% مقارنةً بالأرقام المسجلة في عام ٢٠١٠ح ومن المتوقع أن تصل إلى ٣٤٩٤ هجوما إلكترونيا ناجحا بحلول عام ٢٠٢٥ (Islam et al., 2018 & Johari et al., 2013 & Elqadi et al., 2024). كما أنه وفقا لتقرير (COSO, 2019) فإن (٩٠%) من الشركات الأمريكية التي قامت بالتحول الرقمي قد تعرضت بالفعل لمخاطر الهجمات السيبرانية (Elmaasrawy and Tawfik, 2025)؛ كما انه وفقاً لمركز الأمن السيبراني التابع للمنتدى الاقتصادي العالمي فإن (٧٤%) من الشركات تعرضت للاختراق في عام ٢٠٢٢ (Babiker, 2025).

[٢] أدى ظهور جائحة كورونا إلى زيادة الاتجاه نحو التحول الرقمي بشكل غير محسوب؛ حيث اضطرت العديد من الشركات التي كانت تدير أنشطتها رقمياً بشكل جزئي وتدريجي إلى التحول الرقمي بشكل كلي ومفاجئ في ظل عدم استعداد بيئة معظم الشركات لتلك التحول وهو ما ساهم بشكل كبير في زيادة مخاطر الأمن السيبراني من خلال العمل عن بعد وتوسيع بيئات العمل باستخدام برامج الاجتماعات الافتراضية (فيديو كونفرانس) وإضافة الأجهزة الشخصية إلى أنظمة الشركات (Metwally et al., 2022 & Slapnicar et al., 2022).

Zhou, 2016 & Slapnicar et al., 2022 & Elqadi et al., 2024 & Dikokoe, 2021 & Hossain et al., 2025).

وكنتيجة لمخاطر الأمن السيبراني تتعرض الشركات لأضرار وخسائر اقتصادية بالغة قد تضر بقدرتها على الابتكار واكتساب العملاء والحفاظ عليهم؛ بالإضافة إلى تسببها في حدوث أخطاء جوهرية في السجلات والتقارير المالية، واختراق البيانات، وتعطيل الخدمات التي تقدمها المنشآت، وسرقة الهوية للشركات؛ وكذلك التأثير السلبي على علامتها التجارية وسمعتها، وفقد حصتها السوقية، وانخفاض صافي أرباحها نظراً لارتفاع تكلفة الهجمات السيبرانية[1] وبالتالي التأثير السلبي على المركز والأداء المالي للشركة، والحد من قدرتها على تحقيق أهدافها المنشودة (Elmaasrawy et Tawfik, 2025 & Haapamaki and &Sihvonen, 2019& Vitali and Giuliani, 2024 & Elqadi et al., 2024 & Badawy, 2021& محروس، وصالح، ٢٠٢٢)

ونظراً للمعدل المتصاعد لحوادث الأمن السيبراني وحجم التأثير المالي الكبير المرتبط بها فقد قامت الشركات بإعطاء أولوية كبيرة لإدارة مخاطر الأمن السيبراني، واعتبارها بنداً رئيسياً في جدول أعمال المحاسبين والمراجعين والمديرين؛ بل أصبح جانباً أساسياً من جوانب الأمن الوطني على مستوى العالم (Steinbart et al., 2018 & Haapamaki and Sihvonen, 2019 & Babiker, 2025). وأصبح من الضروري على الشركات القيام بتكييف أدواتها للحد من مخاطر الأمن السيبراني، وإدارتها والاستجابة لها؛ حيث تلك المخاطر لا يمكن تجنبها ولكن يمكن إداراتها (Alina et al., 2017 & Babiker, 2025 & Dikokoe, 2021).

[1] في عام ٢٠١٠ بلغ متوسط تكلفة الهجمات السيبرانية لشركة تعمل في الولايات المتحدة الأمريكية (١٥.٤) مليون دولار سنوياً؛ وقد تضاعف هذا الرقم سنوياً منذ عام ٢٠١٠؛ حيث أشارت التقارير إلى أن الهجمات السيبرانية قد كلفت الشركات أكثر من (٢) تريليون دولار في عام ٢٠١٩ وهو ما يقارب من (٤) أضعاف التكاليف الخاصة بعام ٢٠١٥؛ ومن المتوقع أن تصل إلى (٦) تريليون دولار بحلول عام ٢٠٢٥ (Islam et al., 2018 & Johari et al., 2013 & Elqadi et al., 2024).

وتلعب وظيفة المراجعة الداخلية باعتبارها إحدى آليات حوكمة الشركات وأحد دعائم القيمة المضافة للشركات دوراً هاماً وفعالاً في إدارة المخاطر المرتبطة بالأمن السيبراني لكونها بمثابة خط دفاع أساسي للمنشأة وذلك من خلال توفير الضمانات فيما يتعلق بأمن وسلامة نظم المعلومات عن طريق التوكيد على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني، وتوليد رؤى جديدة حول كيفية تحسين وحوكمة أمن المعلومات في المنشأة، وتنسيق جهود إدارة المخاطر؛ وبالتالي فقد تطور دور المراجع الداخلي بشكل تدريجي من مجرد التحقق من الالتزام إلى تقييم الفعالية والكفاءة، وتقديم قيمة مضافة للمنشأة، وتطوير الأساليب والآليات القادرة على اكتشاف المخاطر وتجنبها وإداراتها، والعمل على أخذ خطوات استباقية وفعالة للتعامل مع المخاطر السيبرانية، والقيام بوظائف استشارية من شأنها تحسين إدارة مخاطر الأمن السيبراني (Steinbart et al., 2018 & Hepworth et al., 2022 & Inyang et a., 2021 & Johari et al., 2023 & Elmaasrawy and Tawfik, 2025 && Babiker, 2025 & Steinbart et al., 2018 أبو الخير، ٢٠٢٣).

ولكي تكون وظيفة المراجعة الداخلية قادرة على الوفاء بالمسئوليات السابق ذكرها ؛ فيجب أن تكون تلك الوظيفة في حالة ديناميكية مستمرة تمكنها من مواكبة التغيرات في بيئة الأعمال والمخاطر المحيطة بها ولا سيماً وأن الهجمات السيبرانية تتطور بشكل أسرع من تطوير آليات اكتشافها والحد منها وإدارتها؛ وهو ما أدى إلى زيادة المتطلبات الملقاة على عاتق المراجعين الداخليين وضرورة قيامهم باكتساب مهارات وخبرات جديدة متعلقة بمخاطر نظم تكنولوجيا المعلومات وأدوات الرقابة عليها، وتوسيع نطاق عملهم، والإلمام بأساليب مراجعة نظم تكنولوجيا المعلومات وطرق تقييم نتائج إجراءات المراجعة الآلية، وإعطاء أولوية للضوابط المرتبطة بالوقاية من مخاطر الأمن السيبراني والكشف عنها والاستجابة لها وإداراتها وتقييم كفاءتها وفعاليتها وتحسينها باستمرار، وتعزيز العلاقات مع الإدارات الأخرى[١] (Steinbart

[١] أوصي معهد المراجعين الداخليين بتحسين العلاقة بين وظيفتي المراجعة الداخلية وأمن وتكنولوجيا المعلومات والعمل معاً بشكل متوازي؛ حيث يقوم موظفو أمن المعلومات بتصميم وتنفيذ وتشغيل إجراءات وتقنيات لحماية الموارد

et al., 2018 & Hepworth et al., 2022 & Babiker, 2025 & Steinbart et al., 2018 & Suleiman and Dandago, 2014 & Abu-Musa, 2006 & Alina et al., 2017).

وفي ظل قلة خبرة المراجعين الداخليين في مجال حوكمة نظم تكنولوجيا المعلومات ومخاطر الأمن السيبراني، والرغبة في تحسن الأداء وزيادة الجودة؛ فقد اتجهت معظم الشركات في الآونة الأخيرة إلى إسناد وظيفة المراجعة الداخلية لطرف خارجي كوسيلة للوصول إلى أفضل الخبرات والمهارات والممارسات المحاسبية في مجال المراجعة الداخلية وعلاقتها بإدارة مخاطر الأمن السيبراني، فضلاً عن مساعدة الإدارة بالتركيز على المزايا التنافسية والأنشطة الرئيسية المضيفة للقيمة للمنظمة بما يساعد على تحسين جودة الخدمات المقدمة وتحقيق مزيد من الوفر في التكلفة نظراً لتمتع الموفر الخارجي للخدمة باقتصاديات الحجم الكبير (Rittenberg and Covaleski, 2001 & Rittenberg et al., 1999 & Vuko et al., 2025).

وبناءاً على ما سبق؛ يتضح أن وظيفة المراجعة الداخلية قد تكون بمثابة أحد الركائز الأساسية التي يعتمد عليها أصحاب المصلحة في توفير توكيد بشأن مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني. وهو ما دعي الباحثان للسعي نحو إيجاد دليل تجريبي في البيئة المصرية حول القيمة المضافة لتوكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني؛ وهل سيختلف هذا الأمر باختلاف طبيعة إسناد وظيفة المراجعة الداخلية لطرف خارجي من عدمه؛ وأيضاً باختلاف نوع وخبرة أصحاب المصالح أم لا؟.

المعلوماتية للمنشأة؛ وفي نفس الوقت تقوم وظيفة المراجعة الداخلية بتقديم ملاحظات دورية بشأن فعالية هذه الأنشطة جنباً إلى جنب مع تقديم اقتراحات لتحسين الفعالية الاجمالية لأمن المعلومات في الشركة وهو ما يؤدي في النهاية إلى تعظيم فعالية برنامج أمن أنظمة المعلومات بالمنشأة (Steinbart et al., 2012 & Haapamaki and Sihvonen, 2019).

٢- مشكلة البحث:

تزامناً مع انتشار جائحة كورونا وما صاحبها من تحوًل متسارع نحو الرقمنة والاعتماد الكثيف من قبل الشركات على تقنيات تكنولوجيا المعلومات في إدارة عملياتها؛ فقد ازدادت المخاطر السيبرانية التي تواجه الشركات بشكل كبير، وجعلتها أكثر عرضة للهجمات السيبرانية والتي لم تعد بمثابة اختراقات تقنية عابرة فحسب بل أصبحت ًتشكًل تهديدات أمنية استراتيجية قد تعصف بسمعة الشركة وتؤثر جوهريا على قدرتها في البقاء والنمو والاستمرار. وفي ظل هذا الواقع الجديد؛ أصبح لزاماً على الشركات أن تعزز من قدراتها في إدارة مخاطر الأمن السيبراني، وإعداد تقارير دورية دقيقة وشاملة حول تلك المخاطر وإداراتها بما يساعد على تدعيم عملية اتخاذ القرارات من قبل أصحاب المصلحة.

وقد تواجه عملية إعداد التقارير بشأن إدارة مخاطر الأمن السيبراني من قبل إدارة المخاطر بالشركة العديد من التحديات ومن أبرزها؛ التعقيد الفني لمعظم المخاطر السيبرانية مما قد يؤدي إلى قصور في وصفها أو تقييمها بصورة دقيقة داخل التقارير، وصعوبة قياس بعض أنواع المخاطر السيبرانية بدقة مما يؤدي إلى انخفاض جودة المعلومات المقدمة، فضلاً عن احتمال وجود تحيزات داخلية من قبًل مُعدي التقارير أو إدارة المخاطر.

وفي ظل التحديات السابقة؛ فقد زادت أهمية وظيفة المراجعة الداخلية لكونها طرف مستقل يضفي مزيد من الثقة حول مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني، ويساهم في طمأنة الإدارة العليا وأصحاب المصالح بموثوقية ودقة تقارير إدارة المخاطر السيبرانية. وعلى الرغم من الدور الحيوي المتوقع من وظيفة المراجعة الداخلية في هذا الشأن؛ إلا أن هناك العديد من التساؤلات المتعلقة بمدى قدرة المراجعين الداخليين على فهم الجوانب الفنية المعقدة للأمن السيبراني بشكل كافي يمكنه من التوكيد بشأن إداراتها من قبًل إدارة المخاطر السيبرانية، وبمدى توافر الكفاءة الفنية لدى المراجعين الداخليين لفحص تقارير إدارة المخاطر السيبرانية بعمق،

وبمدى قدرة المراجع الداخلي على إضافة قيمة للشركة عند القيام بالتوكيد على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني (Johari et al., 2023 & Usman et al., 2024).

وبالتالي تتمحور مشكلة البحث الحالي في محاولة الإجابة نظرياً وتجريبياً على الأسئلة التالية: ما هي القيمة المضافة من توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة المخاطر السيبرانية؟؛ وإلى أي مدى يؤثر إسناد وظيفة المراجعة الداخلي لطرف خارجي على طبيعة العلاقة السابقة؟؛ وهل نوع وخبرة الأطراف أصحاب المصالح من شأنهما تعديل العلاقة السابقة؟.

٣- هدف البحث:

يستهدف البحث دراسة وتحليل واختبار القيمة المضافة من توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني؛ وأثر كل من طبيعة إسناد وظيفة المراجعة الداخلية ونوع وخبرة ممثلي جانب الطلب للمراجعة الداخلية على هذه القيمة المضافة؛ وذلك من خلال دراسة وتحليل وتقييم لأهم الإصدارات المهنية والدراسات الأكاديمية السابقة ذات الصلة بموضوع البحث. واختبار فروض البحث من خلال إجراء دراسة تجريبية على عينة من المهتمين بوظيفة المراجعة الداخلية متمثلة في أعضاء مجلس الإدارة، ولجنة المراجعة، وشركات السمسرة، وإدارة منح الائتمان بالبنوك، وإدارة أمناء الاستثمار بالبنوك، والمحللين الماليين، ومراقبي الحسابات.

٤- أهمية ودوافع البحث:

تنبع أهمية البحث من الناحية العلمية؛ من مساهمته في سد فجوة بحثية قائمة بين وظيفة المراجعة الداخلية وإدارة مخاطر الأمن السيبراني داخل بيئة الممارسة المهنية المصرية؛ حيث لم تحظ العلاقة بين المجالين بالاهتمام الكافي في الدراسات السابقة وخصوصاً فيما يتعلق بدور المراجعة الداخلية كجهة توكيد مستقلة على مزاعم إدارة المخاطر بشأن إدارة مخاطر الأمن السيبراني بما قد يساهم في توسيع الإطار النظري للمراجعة الداخلية ليشمل

تقييم المخاطر السيبرانية بجانب المخاطر التشغيلية والمالية التقليدية، وإعادة تشكيل مهارات وخبرات المراجع الداخلي بما يتناسب مع تحديات البيئة الرقمية.

كما تنبع أهمية البحث من الناحية العملية؛ من كون نتائج هذا البحث قد تساهم في تحسين قدرة المنشآت على مواجهة التهديدات السيبرانية وتقليل الخسائر الناجمة عنها من خلال العمل على زيادة دور وظيفة المراجعة الداخلية في اكتشاف المخاطر السيبرانية والحد منها والاستجابة لها. فضلاً عن مساعدة الأطراف أصحاب المصلحة في تحسين عملية اتخاذ القرارات من خلال القيمة المضافة من توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني.

ورغم كثرة الدوافع إلا أن من أهمها؛ التحول الرقمي السريع في بيئة الأعمال وما يصاحبه من خلق تحديات جديدة في مجال الأمن السيبراني والتي تفرض بدورها تحديات جديدة أمام المراجع الداخلي. بالإضافة إلى الرغبة في زيادة وعي وإدراك لجان المراجعة ومجلس الإدارة بأهمية وظيفة المراجعة الداخلية في فهم وتقييم قدرات المنشآت بشأن إدارة مخاطر الأمن السيبراني؛ والعمل على رفع المستويات المعرفية والمهارية والتدريبية لدى المراجعين الداخليين بما يمكنهم من إضافة قيمة للمنشأة. فضلاً عن التعرف على القيمة المضافة من توكيد المراجع الداخلي – إسناد داخلي أو إسناد خارجي - على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني في بيئة الأعمال المصرية من خلال إتباع منهجية بحثية متكاملة متطورة تتلافي عيوب الاعتماد على قوائم الاستقصاء باعتبارها أدارة بحثية يتم استخدامها في معظم البحوث المحاسبية ذات الصلة. وأخيراً مسايرة اتجاه الدراسات السابقة الأجنبية ذات الصلة بإجراء تحليل أساسي وتحليل الحساسية بهدف التغلب على نقص يكاد يكون متكرراً في كثير من الدراسات المصرية ذات الصلة إن وجدت.

٥- حدود البحث:

يقتصر البحث الحالي على دراسة واختبار القيمة المضافة من توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني؛ **وبذلك يخرج عن نطاق البحث** القيمة المضافة من أداء وظيفة المراجعة الداخلية لدورها الاستشاري في مجال إدارة مخاطر الأمن السيبراني؛ **كما يخرج عن نطاق البحث** أثر القيمة المضافة من توكيد المراجع الداخلي على مزاعم الإدارة بشأن مخاطر الأعمال التشغيلية والمالية والاستراتيجية والأخلاقية[١] الأخرى بخلاف مخاطر الأمن السيبراني. **كما يخرج عن نطاق البحث** القيمة المضافة من توكيد المراجع الخارجي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني.

كما يركز البحث الحالي على اختبار أثر بعض المتغيرات المعدلة للعلاقة محل الدراسة وهي طبيعة الإسناد - سواء كان داخلي أو خارجي- ونوع جنس وخبرة الأطراف أصحاب المصالح. **وبالتالي يخرج عن نطاق البحث** بدائل الإسناد الأخرى مثل الإسناد المحلي والإسناد الدولي والإسناد التعاوني. **كما يخرج عن نطاق البحث** المتغيرات الأخرى المتعلقة بأصحاب المصالح مثل عمره، والمؤهلات العلمية الحاصل عليها، فضلاً عن خروج حجم وسمعة والتخصص الصناعي لموفر خدمة المراجعة الداخلية في حالة الإسناد الخارجي لها.

وأخيراً؛ فإن قابلية نتائج البحث للتعميم ستكون مشروطة بضوابط اختيار عينة البحث والمتغيرات البحثية والمقاييس ذات الصلة والتصميم التجريبي المستخدم في هذا البحث.

[١] **المخاطر التشغيلية** هي تلك المخاطر التي تؤثر سلباً على إيرادات الشركة ورأس مالها، وتنشأ نتيجة اتخاذ قرارات خاطئة لا تواكب التغيرات الحديثة وتشمل مخاطر الاحتيال ومخاطر عدم التوافق في تنفيذ السياسات والإجراءات الإدارية والمخاطر الفنية. أما **المخاطر المالية** فهي المخاطر المتعلقة بالاستثمار والائتمان وعدم القدرة على سداد الالتزامات وتشمل مخاطر السيولة ومخاطر تغيرات أسعار الفائدة وأسعار الصرف ومخاطر عدم كفاية رأس المال. في حين أن **المخاطر الأخلاقية** هي تلك المخاطر التي تنشأ نتيجة تضارب في المصالح بين أطراف متعددة وما يصاحبه من عدم تماثل في المعلومات بين الأطراف الداخلية والأطراف الخارجية. أما **المخاطر الاستراتيجية** فهي تلك المخاطر المتعلقة بالتغيرات في البيئة التنافسية والصناعة التي تعمل بها المنشأة والتي قد تخرج عن نطاق سيطرة المنشأة مثل القوانين والتشريعات الجديدة والقيود السياسية والاقتصادية (Babiker, 2025).

٦- خطة البحث:

انطلاقاً من مشكلة البحث، وتحقيقاً لأهدافه، وفي إطار الحدود الموضوعة، سوف يستكمل البحث على النحو التالي:

٦-١- إدارة مخاطر الأمن السيبراني من منظور محاسبي: مهنياً وأكاديمياً.
٦-٢- وظيفة المراجعة الداخلية: المفهوم، التطور، الأدوار، ومتطلبات الدعم.
٦-٣- تحليل الدراسات السابقة؛ واشتقاق فروض البحث.
٦-٤- منهجية البحث.
٦-٥- نتائج البحث، والتوصيات، ومجالات البحث المستقبلية.

٦-١- إدارة مخاطر الأمن السيبراني من منظور محاسبي: مهنياً وأكاديمياً

في ظل التحول السريع نحو الرقمنة والتوسع في استخدام نظم تكنولوجيا المعلومات أصبح هناك زيادة كبيرة في التحديات والمخاطر التي تواجه الشركات؛ وأصبح لزاماً على الشركات القيام بالدفاع عن نفسها وعملائها ضد تلك المخاطر والتحديات من خلال تنفيذ خطة أمنية سيبرانية متقنة تهدف إلى التخفيف من حدة التهديدات السيبرانية؛ ويطلق على الاستجابة لهذه المخاطر الرقمية الجديدة مفهوم **"الأمن السيبراني"** (Hepworth et al., 2022). ويُنظر للأمن السيبراني على إنه استراتيجية بالغة الأهمية بالنسبة للشركات تهدف إلى حماية أجهزة الكمبيوتر والشبكات والبرامج والبيانات من الهجمات الالكترونية أو التلف أو الوصول غير المصرح به من أجل الحفاظ على سرية وسلامة وتوافر البيانات والمعلومات في ظل العمل في بيئة معقدة قائمة على التفاعل بين الأشخاص والتطبيقات التكنولوجية (Hossain et al., 2025 & Durst et al., 2024 & Elqadi et al., 2024).

وبناءاً على ما سبق؛ فقد اهتمت المنظمات المهنية ذات الصلة بوضع **تعريف لمفهوم الأمن السيبراني**. وفي هذا الشأن؛ عرف معهد الوطني للمعايير وتكنولوجيا

المعلومات في الولايات المتحدة الأمريكية[١] (NIST) الأمن السيبراني على إنه "عملية حماية المعلومات من خلال منع واكتشاف والاستجابة لمواجهة الهجمات الالكترونية لضمان توافر وسلامة ومصداقية وسرية البيانات" (NIST, 2013). ووفقاً للمعهد الأمريكي للمحاسبين القانونيين[٢] (AICPA) فقد تم تعريف الأمن السيبراني على إنه "حماية أصول نظام المعلومات بما في ذلك الأجهزة أو البرامج أو المكونات التكنولوجية الأخرى المسئولة عن تخزين المعلومات ومعالجتها ونقلها" (Elqadi et al., 2024 & Kahyaoglu and Caliyurt, 2018).

وبالنظر إلى الدراسات الأكاديمية ؛ فقد تم تعريف مفهوم الأمن السيبراني على إنه "تنظيم وتجميع الموارد والعمليات والهياكل المستخدمة لحماية الفضاء الالكتروني[٣] والأنظمة التي تدعمه من الممارسات التي تتعارض بحكم القانون مع حقوق الملكية الفكرية" (Badawy, 2021). كما تم تعريفه على إنه "عملية حماية المعلومات من خلال معالجة التهديدات التي تتعرض لها هذه المعلومات والتي يتم معالجتها وتخزينها ونقلها بواسطة أنظمة المعلومات المتداخلة بين الشبكات" (أميرهم، ٢٠٢٢).

وفي هذا الصدد؛ تم تعريف الأمن السيبراني على إنه "كل الأنشطة أو العمليات أو الإجراءات التنظيمية اللازمة لضمان حماية المعلومات ونظم الاتصالات بجميع أشكالها من مختلف الانتهاكات؛ فضلاً عن منع أو تقليل الآثار المالية المرتبطة بها" (عطية، ٢٠٢١). كما تم تعريفه على إنه "التقنيات والعمليات والممارسات والإجراءات المصممة لحماية أصول المعلومات الخاصة بالشركة من الهجمات والتهديدات السيبرانية" (Elmaasrawy and Tawfik, 2025).

---

[١] The National Institute of Standards and Technology.

[٢] The American Institute of Certified Public Accountants.

[٣] يمكن تعريف الفضاء الالكتروني على إنه البنية التحتية الرقمية المترابطة والتي تستهدف تسهيل المعاملات الآمنة والتي تشمل على الانترنت، أنظمة الكمبيوتر، الشبكات، الأجهزة والمعدات، البرامج، المعلومات الرقمية، والمستخدمين (Elmaasrawy and Tawfik, 2025 & Badawy, 2021 & Kahyaoglu and Caliyurt, 2018 & Elqadi et al., 2024).

وبتحليل التعريفات السابقة؛ نجد أن **مثلث الأمن السيبراني** يتكون من ثلاثة عناصر وهي (Hossain et al., 2005 & Kahyaoglu and Caliyurt, 2018 & & Dikokoe, 2021 Elqadi et al., 2024 يوسف، ٢٠٢٤)؛ (ا) **السرية** (Confidentiality): وتعني أن تكون المعلومات متاحة فقط للأشخاص المصرح لهم بالوصول إليها؛ (٢) **السلامة** (Integrity): وتعني الحفاظ على دقة وصحة واكتمال البيانات طوال دورة حياتها دون تعديلها أو تغيرها من قبّل الأشخاص غير المصر لهم؛ (٣) **التوافر** (Availability): وتعني ضمان وصول المستخدمين المصرح لهم إلى البيانات والموارد في الوقت المناسب وبصورة موثوقة عند الحاجة إليها. وبالتالي تتمثل **أهداف الأمن السيبراني** في ثلاثة فئات وهي؛ حماية سرية المعلومات الخاصة، وحماية دقة المعلومات وموثوقيتها وصحتها، وضمان وصول المستخدمين المصرح لهم إلى المعلومات في الوقت المناسب (Haapamaki and Sihvonen, 2019). ويتوقف تحقيق تلك الأهداف على مدى توافر ضوابط فعالة لتحقيق الأمن السيبراني وعادة ما يتم تنفيذ تلك الضوابط بعد إجراء تقييم شامل للمخاطر السيبرانية التي تواجه الشركة (Hepworth et al., 2022).

وفي هذا الشأن؛ تتكون **ضوابط الأمن السيبراني**[١] من ثلاثة فئات وهي (Steinbart et al., 2012 & Hepworth et al., 2022 & Steinbart et al., 2012):

[١] يتكون الأمن السيبراني من ستة أنواع (محمود، وآخرون، ٢٠٢٥) وهي: (١) تأمين الشبكات: وهي تأمين شبكة الحاسب الآلي من المتطفلين سواء كانوا مهاجمين مستهدفين أو برامج ضارة انتهازية؛ (٢) تأمين التطبيقات: وتعني التصميم السليم للتطبيقات قبل استخدامها؛ (٣) أمن المعلومات: وتعني الحفاظ على سرية البيانات وسلامتها سواء في عملية التخزين أو نقلها؛ (٤) الأمن التشغيلي: وهي القرارات والعمليات المتعلقة بمعالجة البيانات وحمايتها والأذونات التي يمتلكها المستخدمون عند الوصول إلى الشبكة، وكذلك الإجراءات التي تحدد كيف واين يمكن تخزين البيانات أو مشاركتها؛ (٥)تعزيز تعافي الشركات من الهجمات السيبرانية بأشكالها المختلفة: وتتضمن الإجراءات المتبعة للتعامل مع الهجمات السيبرانية عند حدوثها والاستجابة لها؛ (٦) تدريب المستخدم: فالمستخدم هو أكثر عوامل مخاطر هجمات الأمن السيبراني التي لا يمكن التنبؤ بها حيث يمكن لأي شخص إدخال فيروس بطريق الخطأ إلى نظام آمن من خلال عدم اتباع ممارسات الأمان الجيدة وتدريب المستخدمين على التعامل مع المرفقات المشبوهة.

- ضوابط التكوين (ضوابط وقائية): وهي تتضمن استخدام أساليب مثل عمليات فحص الثغرات الأمنية والتي تقلل من احتمالية نجاح المهاجمين في تحديد نقاط الضعف لاستغلالها.
- ضوابط الوصول (ضوابط استكشافية): تتضمن على أدوات مثل جدران الحماية وأنظمة منع التطفل وضوابط الوصول المادي وإجراءات المصادقة والتي تهدف إلى تقليل احتمالية نجاح المهاجم في الوصول غير المصرح به للنظام.
- ضوابط المراقبة (ضوابط تصحيحية): والتي تعمل على اكتشاف المشكلات وتوفير المعلومات اللازمة لحلها وإصلاحها وتجنبها في المستقبل[١].

مما سبق يرى الباحثان أن مفهوم الأمن السيبراني هو مفهوم جديد في ممارسات الأمن وسلاح استراتيجي للشركة يهدف إلى حماية الأصول المعلوماتية الحيوية والاستراتيجية للشركة من أجل الحفاظ على خصوصيتها وسريتها، ويعتبر بمثابة مقياساً ومؤشراً للمخاطر التي تشكلها أنشطة الشركة واستراتيجياتها التشغيلية والمالية؛ وبالتالي تتمثل الوظيفة الأساسية للأمن السيبراني في التعرف على مخاطر الأمن السيبراني.

وبشأن مخاطر الأمن السيبراني؛ فهي تنشأ كنتيجة لوجود جرائم وهجمات سيبرانية متعمدة أو غير متعمدة[٢] تهدف في المقام الأول إلى سرقة الأصول

[١] يمكن القول أن كلاً من ضوابط التكوين وضوابط الوصول يعملان بشكل مباشر على تقليل احتمالية تعرض أمن المعلومات للخطر من خلال منع الهجمات السيبرانية واكتشافها والحد منها؛ وعلى النقيض تعمل ضوابط المراقبة بشكل غير مباشر على تقليل مخاطر الأمن السيبراني من خلال العمل على تحسين فعالية كلاً من ضوابط التكوين وضوابط الوصول (Steinbart et al., 2012). ومن الجدير بالذكر أن التطبيق السطحي والشكل لتلك الضوابط لا يحد من الجرائم الالكترونية وبشكل فعال ولكنه قد يزيد من التكاليف (Song et al., 2024).

[٢] يمكن تقسيم **مخاطر الأمن السيبراني** إلى مخاطر طبيعية ومخاطر بشرية؛ **فالمخاطر الطبيعية** مثل العواصف والزلازل والحرائق قد تخلق ارتفاعاً هائلاً في الطاقة مما قد يقلل من فعالية أداء الشبكات وأجهزة الكمبيوتر؛ في حين أن **المخاطر البشرية** مثل الاختراقات والهجمات الالكترونية (Babiker, 2025)؛ وقد يتم تنفيذ تلك الجرائم والهجمات بواسطة أفراد من خارج الشركة أو من داخل الشركة ممن مصرح لهم بالتعامل مع النظام. وقد تكون جرائم ذات أغراض انتهازية تستهدف عمداً التلاعب بالنظام لتحقيق مكاسب شخصية أو الإضرار بالمنشأت؛ وقد تكون جرائم غير متعمدة تنشأ كنتيجة لضعف التدريب والإهمال من قبل موظفي الشركة مما قد يترتب عليه ارتكاب أفعال غير متعمدة بما يؤدي إلى حذف كميات هائلة من البيانات أو إلحاق فيروسات بالنظام (Abu-Musa, 2006 & Abu-Musa, 2001 & Usman et al., 2024).

المعلوماتية للشركة (Johari et al., 2023). ويمكن تعريف مخاطر الأمن السيبراني على إنها "مجموعة المخاطر التكنولوجية والتشغيلية والتنظيمية التي تتعرض لها الشركات المستندة على تكنولوجيا المعلومات الحديثة والتي قد تنجم عن اختراق نظام الأمن السيبراني لديها بما يحد من قدرته على تحقيق أهدافه المرجوة" (شحاته، ٢٠٢٢). كما يمكن تعريفها على إنها "أنشطة غير مشروعة تتعرض لها البنية الأساسية للشركة عن طريق استغلال الثغرات الأمنية في نظم المعلومات؛ وذلك بهدف التأثير السلبي على جميع أنشطة الشركة وإمكانياتها وإلحاق الضرر المادي بها وبسمعتها، والكشف عن معلومات الشركة وإجراء تعديلات عليها أو تدميرها" (محروس، وصالح، ٢٠٢٢). ومن الجدير بالذكر أن تلك المخاطر لا ترتبط فقط بالشركات الكبيرة فحسب؛ فعلي الرغم من أن الشركات الكبيرة تكون أكثر عرضة للجرائم السيبرانية إلا أن الشركات الصغيرة تكون ايضاً عرضة لتلك الجرائم بسبب ندرة إمكانياتها المالية وضعف أساليب الحماية بها (الصيرفي، ٢٠٢٥).

وتتمثل **أهم مخاطر الأمن السيبراني** في؛ (١) مخاطر الأداء المرتبطة بتطبيق أدوات تكنولوجيا المعلومات الحديثة والتي تعبر عن فشل تلك الأدوات في القيام بالمهام المستهدفة وتحقيق الاستفادة المرجوة منها (شحاته، ٢٠٢٢)، (٢) المخاطر المتعلقة باختراق المكونات المادية للبنية التحتية المعلوماتية للشركة وما يرتبط به من الكشف عن سرية المعلومات إلى أطراف خارجية، وإلحاق النظام بفيروسات قادرة على إحداث تغيير في البيانات أو تدميرها مما يفقدها دقتها وجودتها وإمكانية الاعتماد عليها، ورفض تقديم الخدمة والانقطاع غير المخطط لنظم تكنولوجيا المعلومات والاتصالات (Hepworth et al., 2022 & Elqadi et al., 2024 & Usman et al., 2024 & Dikokoe, 2021 & Alina et al., 2017 &شحاته، ٢٠٢٢ & أميرهم، ٢٠٢٢).

وبشأن الآثار السلبية لمخاطر الأمن السيبراني؛ فالجرائم والانتهاكات السيبرانية تتسبب في إحداث أضرار جسيمة وبالغة على مستوى قطاع الأعمال والدول؛ فهي قد

تؤدي إلى حدوث اضطرابات في عمليات الشركة وتعطيلها، سرقة المعلومات وفقد سريتها، زيادة المخاطر التشغيلية، حدوث أخطاء مادية في السجلات، ظهور تكاليف إضافية مصاحبة لمخاطر الأمن السيبراني[1]، وهو ما يؤدي إلى انخفاض في الأداء المالي للشركات، وانخفاض القيمة السوقية لها، والتأثير السلبي على سمعتها، انخفاض قيمة علامتها التجارية، وانخفاض حجم الاستثمارات الموجهة للشركات، وزيادة حجم الدعاوي القضائية (Babiker, 2025 & Shamsuddin et al., 2018 & Islam et al., 2018 & Alina et al., 2017 & Song et al., 2024 & Metwally et al., 2022 & Elmaasrawy and Tawfik, 2025 & Calvin et al., 2025).

وتحت مسمي ما يعرف بآثار عدوى الصناعة؛ فقد تنتقل الآثار الاقتصادية السلبية التي تتعرض لها الشركة المخترقة إلى الشركات الأخرى العاملة بنفس الصناعة بما قد يؤدي إلى انخفاض أسعار أسهم الشركات الأخرى التي تعمل في نفس الصناعة، وإلحاق اضرار بعملائها، وفقدان العلاقات مع العملاء، التأثير السلبي على ثروة الملاك، وفقد ثقة المستثمرين في الاعتماد على المعلومات المفصح عنها نظراً لكونها غير دقيقة وهو ما يؤثر حتمياً على عملية اتخاذ القرارات، وارتفاع تكاليف التمويل، وانخفاض الإيرادات، والتأثير السلبي على بقاء ونمو واستمرارية الشركات وهو ما يعطي مؤشرا على تهديد اقتصاديات الدول (Elqadi et al., 2024 & يوسف، ٢٠٢٤ & محمود، وآخرون، ٢٠٢٥).

[1] تعتبر الهجمات السيبرانية مكلفة للغاية؛ ويمكن تقسيم تكاليف مخاطر الأمن السيبراني إلى **مجموعتين؛ الأولى: تكاليف مؤقتة قصيرة الأجل** وهي تكاليف يتم تحملها فقط خلال الفترة التي حدثت فيها الهجمات السيبرانية وتشمل خسارة الأعمال، وانخفاض حجم الإنتاجية نتيجة عدم توافر الموارد، وتكاليف الإصلاح للأصول المخترقة واستعادة الأنظمة، وتكاليف جمع الأدلة عن القائمين بالهجمات؛ **والثانية: تكاليف دائمة طويلة الأجل** والتي تؤثر على فترات محاسبية عديدة وترتبط بعدم القدرة على جذب عملاء جدد، وانخفاض في حجم التدفقات النقدية المستقبلية، وفقد ثقة العملاء، وزيادة تكاليف التأمين على الشركات، وارتفاع تكاليف التمويل، وارتفاع تكاليف التقاضي والغرامات الناتجة عن تسوية مطالبات العملاء بشأن الأضرار التي يتعرضون لها. كما يمكن تقسيم التكاليف السابقة إلى تكاليف ملموسة وتكاليف غير ملموسة؛ فالتكاليف الملموسة تتمثل في تكاليف المبيعات أو الخدمات المفقودة وتكاليف التأمين؛ أما التكاليف غير الملموسة فتتمثل في فقد الثقة لدى أصحاب المصلحة في الشركة (فرج، ٢٠٢٢ & محمود، وآخرون، ٢٠٢٥ & أبو الخير، ٢٠٢٣).

وبناءاً على ما سبق؛ **يرى الباحثان** أنه يمكن تقسيم الآثار السلبية لمخاطر الأمن السيبراني إلى **آثار سلبية اقتصادية، واجتماعية وسياسية، وتقنية**. وتتمثل **الآثار الاقتصادية** في انخفاض أرباح الشركات، وارتفاع تكاليف استعادة الأنظمة، وانخفاض القيمة السوقية للشركات. وبينما تتمثل **الآثار الاجتماعية** تتمثل في زيادة القلق العام والخوف من التعاملات الالكترونية. بينما تتمثل **الآثار السياسية** في تهديد الأمن القومي، واستهداف المؤسسات الحكومية. في حين تتمثل **الآثار التقنية** في تعطيل البنية التحتية الحيوية كشبكات النقل، وتلف أو فقدان البيانات الحيوية للمنظمة، وإحجام الشركات عن الابتكار التقني. وهذه المخاطر بصفة عامة قد يكون لها **تأثير اقتصادي مباشر** على الشركات من خلال فقد سرية المعلومات، وتعطيل الأعمال، وحدوث أخطاء جوهرية في الدفاتر؛ وفي نفس الوقت قد يكون لها **تأثير اقتصادي غير مباشر** من خلال التأثير على زيادة قلق المستثمرين وفقد الثقة، والتأثير السلبي على قيمة الشركة، والحد من قدرتها على الاستمرار.

وبناءاً على ما سبق؛ فإن عدم وجود إجراءات فعالة لإدارة مخاطر الأمن السيبراني لا يفتح المجال فقط لإمكانية وصول مجرمي الانترنت إلى البيانات الخاصة بالشركة بل ويشمل أيضاً شل البنية التحتية لأنظمة المعلومات بالكامل وإلحاق أضرار جسيمة باقتصاديات الدول قد تهدد من بقائها ونموها؛ وهو الأمر الذي يشير لحتمية قيام الشركات بإدارة مخاطر الأمن السيبراني حتي يمكن تجنب آثارها السلبية والحد منها؛ حيث لم يعد هذا الأمر رفاهية بل أصبح قضية أمن قومي (Durst et al., 2024 & Haapamaki and Sihvonen, 2019 & عطية، ٢٠٢١).

وبشأن إدارة مخاطر الأمن السيبراني (CSRM)؛ فيمكن تعريف إدارة مخاطر الأمن السيبراني على إنه "مجموعة من السياسات والإجراءات الرقابية المصممة لحماية المعلومات والأنظمة الالكترونية من الحوادث والهجمات الأمنية التي تتعرض لها الشركات وتحول دون قدرة الشركة على تحقيق أهدافها المنشودة؛ وتهدف تلك السياسات والإجراءات إلى اكتشاف الهجمات والاستجابة لها وتخفيف آثارها والقضاء

عليها في أسرع وقت ممكن" (Elmaasrawy and Tawfik, 2025 & Babiker, 2025 & durst et al., 2024)[1].

وبشأن مردود إدارة مخاطر الأمن السيبراني؛ فإن إدارة مخاطر الأمن السيبراني تمثل قيمة مضافة على المستوى القومي ومستوى قطاع الأعمال من خلال الحد من الخسائر الناجمة عن الهجمات الالكترونية، والحفاظ على سرية وخصوصية المعلومات الحرجة الخاصة بالشركة، والعمل على تخفيض تكلفة التمويل، وزيادة معدل العائد على الاستثمار، وزيادة عدد عملائها، وتخفيض مخاطر وأتعاب المراجعة، وتحسين سمعة الشركة وخلق ميزة تنافسية لها، وبالتالي تعزيز العمليات التجارية الدولية (Islam et al., 2018 &Hossain et al., 2025 & Metwally et al., 2022 & الصيرفي، ٢٠٢٥).

ولتحقيق الاستفادة القصوى من مردود إدارة مخاطر الأمن السيبراني يجب على الشركات إتباع خمس **مراحل لإدارة مخاطر الأمن السيبراني** والتي يجب إجراؤها بشكل مستمر ومتكرر؛ وتتمثل تلك المراحل في (Badawy, 2021 & الصيرفي، ٢٠٢٥ & يوسف، ٢٠٢٤ & شحاته، ٢٠٢٢): (١) التحديد الدقيق لمخاطر الأمن السيبراني وأولوية تعرض الشركة لكل منها؛ (٢) تصميم أنظمة رقابية على الأمن السيبراني متضمنة معايير وأسس واضحة للرقابة بهدف التخفيف من المخاطر ومدى التعرض لها؛ (٣) اختبار الفعالية التشغيلية لضوابط الأمن السيبراني؛ (٤) إعداد تقارير متعلقة بالإفصاح عن مخاطر الأمن السيبراني وإدارتها؛ (٥) توفير توكيد

[1] إدارة مخاطر الأمن السيبراني ليست مسئولية مجموعة محددة داخل وظيفة تكنولوجيا المعلومات فحسب؛ بل هي مسئولية مجموعة كبيرة من الوظائف داخل الشركة بما فيها وظيفة المراجعة الداخلية (Steinbart et al., 2018). ويهدف برنامج إدارة مخاطر الأمن السيبراني إلى تحقيق عدة أهداف أساسية وهي: (١)التوافر: وتشير إلى إمكانية الوصول المستمر إلى المعلومات ووقتية الحصول عليها؛ (٢) السرية: وتشير إلى حماية المعلومات من الاختراق والهجمات الالكترونية المتكررة والوصول غير المصرح به بما يحافظ على خصوصية وسرية البيانات؛ (٣) سلامة البيانات: وتشير إلى حماية البيانات من الاختلاس أو التعديل أو التلف؛ (٤) سلامة العمليات التشغيلية: وتشير إلى حماية العمليات التشغيلية من الاستخدام غير السليم أو التعديل أو التدمير لنظام تكنولوجيا المعلومات سواء كان بشكل جزئي أو كلي (شحاته، ٢٠٢٢)

مهني مستقل على تقارير الافصاح عن مخاطر الأمن السيبراني وإدارتها. وقد تساهم وظيفة المراجعة الداخلية في نجاح برنامج إدارة مخاطر الأمن السيبراني من خلال دورها الاستشاري في مساعدة الإدارة في تنفيذ المراحل الثلاث الأولى لإدارة مخاطر الأمن السيبراني فضلاً عن مساهمتها من خلال دورها الاستشاري والتوكيدي في المرحلتين الرابعة والخامسة[١].

ومن الجدير بالذكر؛ أن تطبيق المراحل السابق ذكرها لن يكون بالأمر السهل؛ حيث أن هناك مجموعة من التحديات التي تواجه الشركات عند القيام بإدارة مخاطر الأمن السيبراني. **وبشأن تحديات إدارة مخاطر الأمن السيبراني؛** تتمثل أهم تلك التحديات في التعقد والتشابك الكبير في مجال تكنولوجيا المعلومات وما يصاحبه من تطور سريع ومستمر للبرمجيات الخبيثة يؤدي إلى صعوبة في تقدير المخاطر السيبرانية (Babiker, 2025)، وصعوبة إدارة مخاطر الأمن السيبراني في ظل الاعتماد على إجراءات الرقابة والمراجعة الداخلية التقليدية غير الفعالة (Metwally et al., 2022)، فضلاً عن ندرة الموارد المالية اللازمة للاستثمار في مجالات الأمن السيبراني والتدريب الكافي للموظفين[٢]، بالإضافة إلى عدم توافر الكوادر البشرية والفنية المؤهلة للتعامل مع مجالات الأمن السيبراني، وعدم وجود عمليات موثقة

[١] أوصت لجنة مبادئ الإدارة السليمة للمخاطر الصادرة عن (IIA, 2020 & COSO, 2019) بإدارة مخاطر الأمن السيبراني بواسطة ثلاثة خطوط دفاع؛ يتمثل **خط الدفاع الأول** في مديري الشركات وموظفي قسم تكنولوجيا المعلومات (IT) والمعنيين بوضع مخاطر الأمن السيبراني ضمن استراتيجية عملهم وتوقعها ووضع الضوابط المناسبة لتحقيق لأمن السيبراني وإدارة مخاطره؛ بينما يتمثل **خط الدفاع الثاني** في إدارة مخاطر الأمن السيبراني والمعنية بتوفير الخبرات اللازمة لتنفيذ ومتابعة ضوابط الأمن السيبراني بكفاءة وفعالية؛ في حين يتمثل **خط الدفاع الثالث** في وظيفة المراجعة الداخلية والمعنية بتوفير توكيد مستقل لكل من مجلس الإدارة ولجنة المراجعة عن فعالية استراتيجيات وسياسات وإجراءات وضوابط الأمن السيبراني وتحديد مدى كفاية العمل الذي تم إنجازه بواسطة خطي الدفاع الأول والثاني (Slapnicar et al., 2022 & Kahyaoglu and Caliyurt, 2018 & Deloitte, 2017 & Alina et al., 2017 & أبو الخير، ٢٠٢٣ & محروس، وصالح، ٢٠٢٢ & أميرهم، ٢٠٢٢).

[٢] ندرة الموارد المالية الموجهة نحو الاستثمار في مجالات الأمن السيبراني يعيق القدرة على تحسين البنية التحتية للأمن السيبراني ، ويعيق عمليات تحديث النظام، والحد من القدرة على البحث والتطوير في مجال الأمن السيبراني، ويعيق من القدرة على توظيف خبراء متخصصين في الأمن السيبراني بسبب عدم القدرة على توفير رواتب تنافسية، بالإضافة إلى الحد من مبادرات التدريب والتوعية للموظفين بمجالات الأمن السيبراني وما يتبعه من إعاقة قدرة الموظفين على التعرف المستمر بأحدث التوجهات العالمية في تلك المجال، والحد من قدرتهم في تحديد الأدوات اللازمة لمعالجة المخاطر واكتشافها والوقاية منها (Hossain et al., 2025).

للأمن السيبراني أو سياسات الحوكمة، وغياب الرؤية داخل المنشأة فيما يتعلق بالأمن السيبراني[1]، وقلة الدعم السياسي بما يعيق عمليات تنفيذ وتطوير ضوابط الأمن السيبراني الفعالة (Hossain et al., 2025).

وفي ضوء مراحل إدارة مخاطر الأمن السيبراني والتحديات المرتبطة بها؛ فقد أصبح لزاماً على الشركات القيام بتكييف أدواتها وآلياتها للحد من مخاطر الأمن السيبراني وإداراتها؛ **وبشأن آليات إدارة مخاطر الأمن السيبراني؛** تتمثل تلك الآليات في قيام الشركات بإعطاء أولوية لنظم تكنولوجيا المعلومات والأمن السيبراني والفهم الدقيق لها ودمجها ضمن الاستراتيجية الشاملة للشركة وتبني استراتيجية أكثر مرونة قادرة على الاستجابة للتهديدات السيبرانية الحديثة في ظل وجود تقييم دوري للمخاطر السيبرانية وتقييم فعالية ضوابط الأمن السيبراني والإفصاح عنها (Johari et al., 2023 & Babiker, 2025)، وزيادة حجم الاستثمارات الموجهة نحو مجالات الأمن السيبراني[2] (Usman et al., 2024 & Song et al., 2024)، وتوفير دعم وتعاون مشترك وشامل بين الإدارة التنفيذية ووظيفة تكنولوجيا المعلومات ووظيفة المراجعة الداخلية (Alina et al., 2017 & Calvin et al., 2025)، وتوفير كوادر فنية وبشرية ذات خبرات كبيرة في مجال الأمن السيبراني ولديهم القدرة على الاطلاع بصورة مستمرة بأحدث التطورات والتقنيات في مجال الأمن السيبراني وما يصاحبها من تحديثات في سياسات وإجراءات وضوابط الأمن السيبراني (Johari et al., 2023 & Badawy, 2021)، والعمل على زيادة وعي إدارة الشركة وكافة الأطراف داخل الشركة بأهمية إدارة مخاطر الأمن السيبراني لما لها من قدرة على تحسين سمعة الشركة وتدعيم فرص

[1] غياب تلك الرؤية من شأنها العمل على عدم وضع الأمن السيبراني ضمن أولويات المنشأة، وإيجاد فجوة بين صياغة السياسات والتنفيذ الفعلي لها، وعدم كفاية تخصيص الموارد، والتردد في تبني سياسات وضوابط الأمن السيبراني حتى يتم التعرض لهجوم فعلي، وعدم وضوح سياسات توزيع الأدوار والمسئوليات والمعايير المتوافقة مع مبادئ الأمن السيبراني، وغياب التعاون داخل الإدارات المختلفة بالمنشأة بما يؤدي إلى نقص التنسيق والفعالية في الاستجابة للتهديدات السيبرانية وما يتبعه من تضاعف المخاطر (Hossain et al., 2025).

[2] في ضوء محدودية الموارد الاقتصادية، ووفقاً لنموذج جوردون ولويب؛ يكون المستوى الأمثل للاستثمار في مجالات الأمن السيبراني هو النقطة التي تتعادل عندها التكاليف الحدية المتوقعة للاستثمار مع الفوائد الحدية المتوقعة من الاستثمار (Loeb and Zhou, 2016).

بقائها ونموها في المستقبل (Slapnicar et al., Kahyaoglu and Caliyurt, 2018 & 2022)، والعمل على إنشاء وثائق تأمين ضد مخاطر الأمن السيبراني بالتعاون مع شركات التأمين المختلفة والاستعانة بمصادر خارجية لتحديد المخاطر السيبرانية التي قد تتعرض لها الشركة (Usman et al., 2024 & Metwally et al., 2022)، بالإضافة إلى العمل على تطوير مهام المراجع الداخلي واكتسابه مهارات التعامل مع نظم تكنولوجيا المعلومات وتحليل البيانات والمعرفة الكافية بالمخاطر السيبرانية وتبني المنهجية الرشيقة (Agile Approach) في أداء مهامه[١] (Islam et al., 2018 & Vitali and Giuliani, 2024)[٢].

وبشأن محددات إدارة مخاطر الأمن السيبراني؛ فهناك مجموعة من العوامل التي تؤثر على الإدارة الفعالة لمخاطر الأمن السيبراني ومنها: (١) القدرات الفنية والبشرية المتوافرة لدى الشركة: فكلما زادت خبرات ومهارات القوى العاملة في الشركة بمجال تكنولوجيا المعلومات وأمنها كلما زادت قدرة الشركة على الإدارة الفعالة لمخاطر الأمن السيبراني (Elmaasrawy and Tawfik., 2025)؛ (٢) المرونة التنظيمية للشركة[٣]: فكلما زادت المرونة التنظيمية للشركة كلما زادت قدرتها على إدارة مخاطر الأمن السيبراني بكفاءة وفعالية (Durst et al., 2024)؛ (٣) دعم مجلس الإدارة وتفعيل آليات حوكمة الشركات والتي قد يلعبا دورا هاماً في التخفيف من حدة المخاطر السيبرانية (Elmaasrawy and Tawfik., 2025 & Islam et al., 2018 & Vuko et al.,

[١] المنهجية الرشيقة تعني القدرة على التحرك بسرعة وبسهولة والتفكير بطريقة ذكية للتعامل مع الاحتياجات المتغيرة لأصحاب المصالح (محروس ، وصالح، ٢٠٢٢).

[٢] لا يقتصر تطبيق آليات إدارة مخاطر الأمن السيبراني على الشركات فحسب ولكنها يجب أن تمتد إلى إلزام الشركات في سلسلة التوريد بالعمل على تطبيق تلك الآليات؛ فغالباً ما يضطر شركاء سلسلة التوريد إلى مشاركة بيانات سرية وبالتالي فإن حدوث أي انتهاك سيبراني مع أحد الشركاء سيكون بلا شك له تأثير خارجي سلبي على باقي شركاء سلسلة التوريد مما يؤدي إلى تعطيل الأعمال؛ وبالتالي فإن الشريك الاضعف في سلسلة التوريد هو الذي سيحدد قوة نظام الأمن السيبراني على طول سلسلة التوريد (Song et al., 2024 & Slapnicar et al., 2022).

[٣] المرونة التنظيمية للشركة تعني قدرة الشركة على التكيف والاستجابة السريعة للتغيرات الداخلية والخارجية، ومواصلة العمليات، والتعافي السريع من الأزمات بما يزيد من قدرتها على البقاء والنمو والاستمرار (Durst et al., 2024).

2025)؛ (٤) الموارد المالية: فكلما زادت الموارد المالية المتوافرة لدى الشركة كلما زادت قدرتها على تصور وتنفيذ استراتيجيات من شأنها العمل على تحسين كفاءة وفعالية عمليات إدارة مخاطر الأمن السيبراني (Durst et al., 2024)؛ (٥) تصميم نظام رقابة داخلي فعال وما يشمله من إدارة مراجعة داخلية فعالة يؤدي إلى توفير النهج الشامل لتحقيق الأمن السيبراني وإدارة مخاطره ويزيد من قدرة الشركة على تحديد نقاط القوة والضعف في بيئة عملها بشكل منتظم بما في ذلك المتعلقة بمجال الأمن السيبراني (Shamsuddin et al., 2024 & Metwally et al., 2022)؛ (٦) ظروف السوق والتي تؤثر بشكل كبير على مدى استعداد الشركة للاستثمار في مجالات إدارة مخاطر الأمن السيبراني (Durst et al., 2024).

وبناءاً على ما سبق؛ **يرى الباحثان** أنه يمكن تقسيم محددات إدارة مخاطر الأمن السيبراني إلى **محددات داخلية متعلقة بالشركة** مثل الكوادر البشرية والفنية، والمرونة التنظيمية، ودعم مجلس الإدارة؛ تفعيل آليات حوكمة الشركات، والموارد المالية، وجود إدارة مراجعة داخلية فعالة؛ و**محددات خارجية متعلقة ببيئة عمل الشركة** مثل ظروف السوق والاضطرابات الخارجية.

وكاستجابة لأهمية ممارسات الأمن السيبراني وإدارة المخاطر المصاحبة له؛ فقد تزايد الجهود الدولية والاقليمية والمحلية في مجال الأمن السيبراني. فبشأن الجهود الدولية في مجال الأمن السيبراني؛ هناك عدة جهات مهنية كبرى قامت بإصدار مجموعة من الأطر والمعايير التي تتعلق بالأمن السيبراني وهي (Song et al., 2024 & Hossain et al., 2024 &Yang et al., 2020 & Johari et al., 2023 & Dikokoe, 2021 & Kahyaoglu and Caliyurt, 2018 & Islam et al., 2018 & يوسف، ٢٠٢٤ & عطية، ٢٠٢١ & الصيرفي، ٢٠٢٥ & فريد، ٢٠٢٢ & محروس، وصالح، ٢٠٢٢):

■المعهد الوطني للمعايير وتكنولوجيا المعلومات (NIST): والذي قام بإصدار إطاراً لتحسين البنية التحتية للأمن السيبراني في نسخته الأولي عام ٢٠١٤ وما

تبعه من تنقيحات عامي ٢٠١٧ و ٢٠١٨؛ وتم بناء هذا الإطار على مجموعة من المعايير والممارسات والمبادئ الاسترشادية القائمة على دمج مخاطر الأمن السيبراني ضمن عمليات إدارة مخاطر الشركة بهدف مساعدة الشركات على تخفيض الآثار السلبية المحتملة للمخاطر السيبرانية.

- معهد المحاسبين القانونيين الأمريكي (AICPA): والذي قام بتطوير إطاراً للتقرير عن إدارة المخاطر السيبرانية من قبّل الشركات عام ٢٠١٧؛ ويهدف هذا الإطار إلى الإفصاح عن معلومات مفيدة لأصحاب المصلحة حول برنامج إدارة مخاطر الأمن السيبراني وفعاليته من خلال وجود طريقة موحدة لعرض المعلومات المرتبطة بمخاطر الأمن السيبراني وهو ما يساهم في خدمة أصحاب المصلحة بشكل أفضل[١].
- المنظمة الدولية للمواصفات القياسية (ISO)[٢]: والتي قامت بتطوير سلسلة (ISO 27000) وهي معايير تُمكّن الشركة من تطبيق ضوابط رقابية تدعم مبادئ أمن المعلومات بها.
- جمعية المراجعة والرقابة على نظم المعلومات (ISACA)[٣]: والتي طورت إطاراً عاماً لتنفيذ مهام إدارة ومراجعة تكنولوجيا المعلومات بهدف مساعدة الإدارة في تخفيض الفجوة بين متطلبات الرقابة والأدوات التكنولوجية ومخاطر الأعمال في وقت واحد وهو ما يطلق عليه إطار أهداف الرقابة للمعلومات والتكنولوجيا المرتبطة بها (COBIT)[٤]؛ كما قامت هذه الجمعية بتأسيس معهد تكنولوجيا

[١] هذا الإطار حتى الآن هو إطار اختياري التطبيق يتكون من ثلاثة مكونات وهي؛ (١) وصف الإدارة لبرنامج إدارة مخاطر الأمن السيبراني الخاص بالشركة؛ (٢) تأكيد الإدارة على أن وصف البرنامج يتفق مع معايير وصف (AICPA)، وأن الضوابط المطبقة من قبّل الإدارة قادرة على تحقيق الأهداف المستهدفة بفعالية؛ (٣) تقرير بشأن رأى مراقب الحسابات القائم بفحص ومراجعة تقرير إدارة مخاطر الأمن السيبراني؛ وإبداء الرأي عن مدى فعالية الضوابط المطبقة لتحقيق أهداف الأمن السيبراني (Yang et al., 2020 & Badawy, 2021).

[٢] International Organization for Standardization.

[٣] Information System Audit and Control Association.

[٤] Control Objective for Information and Related Technology.

المعلومات (ITGI) كمركز ابحاث لحوكمة تكنولوجيا المعلومات والمساعدة في تطوير إطار (COBIT) ليكون إطاراً شاملاً لإدارة تكنولوجيا المعلومات[١].

- هيئة الأوراق المالية والبورصات الأمريكية (SEC): في فبراير ٢٠٢٢ تم إصدار المقترح الأول والمعني بضرورة قيام منظمات الاستثمار وصناديق التطوير باعتماد وتنفيذ سياسات مكتوبة لمعالجة مخاطر الأمن السيبراني، والإفصاح عنها خلال تقرير يوجه إلى الهيئة. وفي مارس ٢٠٢٢ تم إصدار المقترح الثاني والمعني بتوجيه جميع الشركات المقيدة بالبورصة الأمريكية نحو توحيد وتحسين عمليات الإفصاح المتعلقة بإدارة مخاطر الأمن السيبراني[٢].

وعلى المستوى الاقليمي؛ تعتبر الدول العربية هي الأكثر تضرراً من الهجمات السيبرانية؛ وجاءت مصر في المرتبة الثالثة من بين أكثر الدول العربية تضرراً بعد الجزائر والمغرب (Elqadi et al., 2024)؛ ولذلك كان لزاما على مصر القيام ببذل مزيد من الجهود في مجال الأمن السيبراني. **وبشأن الجهود المصرية بشأن الأمن السيبراني؛** فقد قامت الإدارة المصرية بسن مجموعة من التشريعات المتعلقة بالجرائم الإلكترونية؛ وأنشأت كيانات وطنية متخصصة في الأمن السيبراني تهدف في

[١] مرت مراحل تطوير إطار (COBIT) بعدة مراحل منذ صدور نسخته الأولي عام ١٩٩٦ مروراً بصدور نسخته الثانية عام ١٩٩٨ حتي تم إنشاء (ITGI) وما صاحبه من صدور النسخة الثالثة للإطار عام ٢٠٠٠ والتي تضمنت مجموعة من الإرشادات الإدارية المتعلقة بعمليات تكنولوجيا المعلومات. وفي عام ٢٠٠٥ صدرت النسخة الرابعة من الإطار والتي هدفت إلى بناء إطار عمل يلقى القبول العام في مجال حوكمة تكنولوجيا المعلومات يوضح الأدوار والمسئوليات في سياق تكنولوجيا المعلومات. وفي عام ٢٠١٢ صدرت النسخة الخامسة من الإطار والمعتمدة على خمسة مبادئ تعمل معاً لتمكين الشركات من بناء والمعتمدة على خمسة مبادئ تعمل معاً لتمكين الشركات من بناء إطار حوكمة وإدارة فعال قادر على تحسين الاستثمار في تكنولوجيا المعلومات وتوظيفها في تحقيق تطلعات أصحاب المصلحة، وتتمثل تلك المبادئ الخمسة في تلبية احتياجات اصحاب المصلحة، تغطية الشركة من البداية إلى النهاية، وتطبيق إطار واحد متكامل، وتمكين المنهج الشمولي، وفصل الحوكمة عن الإدارة. وفي عام ٢٠١٨ صدرت النسخة السادسة من الإطار والذي هدفت إلى توفير مرونة أكبر في تنفيذ حوكمة تكنولوجيا المعلومات ويتميز هذا الإطار عن سابقيه بتقديم مجموعة من الأهداف المحدثة، وتحديد عوامل التصميم التي يجب أخذها في الاعتبار عند تصميم وتنفيذ حوكمة تكنولوجيا المعلومات، وتحديد مكونات نظام حوكمة تكنولوجيا المعلومات الفعال (محروس ، وصالح، ٢٠٢٢).

[٢] تتضمن الإفصاحات المتعلقة بإدارة مخاطر الأمن السيبراني على سياسات وإجراءات الشركة المتبعة لتحديد وإدارة مخاطر الأمن السيبراني، ودور الإدارة في تنفيذ تلك السياسات والإجراءات، خبرات مجلس الإدارة في مجال الأمن السيبراني، مناقشات الإدارة حول مخاطر الأمن السيبراني وتحليلها للأداء والمركز المالي القائم في ظل تلك المخاطر (Islam et al., 2018 & محروس، وصالح، ٢٠٢٢ & فريد، ٢٠٢٢).

المقام الأول إلى توفير بيئة رقمية آمنة وموثوقة للمجتمع المصري بمختلف أطيافه؛ فوفقا لقرار رئيس مجلس الوزراء رقم (٢٢٥٩) لعام ٢٠١٤ فقد تم إنشاء المجلس الأعلى للأمن السيبراني التابع لرئاسة مجلس الوزراء والمعني بحماية البنية التحتية المعلوماتية للدولة، وتعزيز الأمن السيبراني، ووضع الاستراتيجية وطنية لمواجهة المخاطر والهجمات السيبرانية والاشراف على تنفيذها وتحديثها تماشياً مع التطورات التقنية المتلاحقة[١]؛ بالإضافة إلى ذلك تم إنشاء المكتب التنفيذي للمجلس الأعلى للأمن السيبراني[٢]، والأمانة الفنية للمجلس الأعلى للأمن السيبراني[٣]. كما إنه وفقاً لقرار مجلس الوزراء رقم ٩٩٤ لعام ٢٠١٧ فقد تم إلزام جميع الوحدات الحكومية بكافة مستوياتها بتنفيذ قرارات وتوصيات المجلس الأعلى للأمن السيبراني فيما يتعلق بتأمين البنية التحتية الحرجة للاتصالات وتكنولوجيا المعلومات الخاصة بها، واتخاذ

[١] وفقاً لقرار رئيس مجلس الوزراء رقم (١٦٣٠) لعام ٢٠١٦؛ تتمثل اختصاصات المجلس الأعلى للأمن السيبراني في اعتماد تحديد البني التحتية للاتصالات والمعلومات الحرجة في كافة قطاعات الدولة ووضع أطر تقييم ومتابعة تأمين لها في القطاعات المختلفة، واعتماد أطر واستراتيجيات وسياسات تأمين البني التحتية للاتصالات والمعلومات الحرجة لكافة قطاعات الدولة وآليات متابعة تنفيذها، وضع خطط وبرامج تنمية صناعة الأمن السيبراني وإعداد الكوادر اللازمة لمواجهة التحديات والمخاطر السيبرانية وآليات تنفيذها، ووضع إطار للبحث العلمي والتطوير والابتكار في مجال الأمن السيبراني وآليات تنفيذه، التعاون والتنسيق إقليمياً ودولياً مع الجهات ذات الصلة في مجال الأمن السيبراني لتبادل الخبرات والمعلومات لمواجهة الهجمات السيبرانية والتصدي لها، وإعداد توصيات بأية تدخلات تشريعية لازمة لإدارة مخاطر الأمن السيبراني، إنشاء وحدة للإنذار المبكر والتدخل معنية بوضع آليات رصد للمخاطر والمتابعة الدورية للهجمات السيبرانية وتوزيع الأدوار على المستوى الوطني وإخطار الجهات المستهدفة بالاستعداد والتصدي لتلك المخاطر، وإقرار مواصفات الأمن السيبراني القياسية للأنظمة والأجهزة والتطبيقات في مختلف القطاعات وإضافة معايير الجودة السيبرانية بالتنسيق مع الجهات ذات الصلة.

[٢] وفقاً لقرار رئيس مجلس الوزراء رقم (١٦٣٠) لعام ٢٠١٦؛ تتمثل اختصاصات المكتب التنفيذي للمجلس الأعلى للأمن السيبراني في الإشراف العام على تنفيذ أعمال المجلس والخطط التي يقرها في ضوء الاستراتيجيات والسياسات المحددة، وإعداد توصيات ومقترحات وخطط تنفيذية فيما يتعلق بأعمال المجلس، ودراسة التقارير والطلبات المقدمة إلى المجلس وإعداد التوصيات الملائمة بشأنها.

[٣] وفقاً لقرار رئيس مجلس الوزراء رقم (١٦٣٠) لعام ٢٠١٦؛ تتولى الأمانة العامة للمجلس الأعلى للأمن السيبراني القيام بتنظيم وإطلاق حملات وطنية دورية للتعريف بمخاطر الاختراقات السيبرانية لنظم التحكم الصناعية في مختلف القطاعات وخاصةً في قطاع الطاقة والمرافق العامة، وتنظيم ورش عمل ودورات للتوعية بالأمن السيبراني على المستوى القطاعي، وإعداد مواصفات نظم التبادل الآمن للمعلومات المتعلقة بتأمين البني التحتية للاتصالات والمعلومات الحرجة وفقاً للمعايير العالمية ذات الصلة.

كافة الإجراءات الفنية والإدارية لمواجهة الأخطار والهجمات السيبرانية، وتنفيذ الاستراتيجية الوطنية للأمن السيبراني[١].

وفي هذا الصدد؛ قام البنك المركزي المصري بإطلاق مبادرة تعزيز الأمن السيبراني في القطاع المصرفي، وإنشاء مركز الاستجابة السريعة لطوارئ الحاسب الآلي؛ وتهدف تلك الجهود إلى زيادة أعداد الخبراء المعتمدين دولياً في مجال الأمن السيبراني في القطاع المصرفي، وتوفير الحماية اللازمة للمتعاملين مع البنوك من خلال تحديد التهديدات السيبرانية المحتملة وفحص وتقييم المخاطر المرتبطة بها والتعامل معها والإبلاغ الفوري عنها بما يساعد على توفير إنذاراً مبكراً يُمكّن من اتخاذ الإجراءات الاحترازية وتأمين البنية التحتية المعلوماتية وتعزيز الأمن السيبراني في القطاع المصرفي المصري (محروس، وصالح، ٢٠٢٢ & الصيرفي، ٢٠٢٥).

وبناءاً على ما سبق؛ **يرى الباحثان** أن هناك اهتمام دولي وإقليمي ومحلي بممارسات الأمن السيبراني وكذلك إدارة المخاطر المصاحبة لتلك الممارسات؛ وهو ما يتوافق مع المنافع التي قد تعود على الشركة في حال القيام بالإدارة الفعالة لمخاطر الأمن السيبراني من جهة؛ وتجنب التكاليف المرتبطة بإهمال ممارسات الأمن السيبراني وإدارة مخاطرها من جهة أخرى.

٦-٢- وظيفة المراجعة الداخلية: المفهوم، التطور، الأدوار، ومتطلبات الدعم

قدم معهد المراجعين الداخليين (IIA, 1999 & IIA, 2009 & IIA, 2017)[٢] تعريفات متسقة لوظيفة المراجعة الداخلية على إنها "نشاط مستقل وموضوعي توكيدي

[١] في عام ٢٠١٧ أطلق المجلس الأعلى للأمن السيبراني ما يعرف بالاستراتيجية الوطنية للأمن السيبراني (٢٠١٧-٢٠٢١) والتي تهدف إلى رصد ومواجهة التحديات والأخطار السيبرانية، وعناصر التهديدات السيبرانية، وأهم القطاعات الحيوية المستهدفة، والاستراتيجيات المتبعة للحد من مخاطر الأمن السيبراني وآليات تنفيذها بهدف تعزيز الثقة في البنية التحتية الرقمية للدولة (يوسف، ٢٠٢٤ & فرج، ٢٠٢٢).

[٢] معهد المراجعين الداخليين (The Institute of Internal Auditors) تم تأسيسه عام ١٩٤١ بهدف المساهمة في تطوير وظيفة المراجعة الداخلية من خلال تحديد المفهوم، والأهداف، ونطاق عمل المراجعة الداخلية، وتحديد الأدوار والمسئوليات للمراجع الداخلي، وإصدار الإرشادات والمعايير المتعلقة بالأداء المهني للمراجعة الداخلية (محمد، ٢٠١٩).

استشاري يهدف إلى إضافة قيمة للمنشأة وتحسين عملياتها وتحقيق أهدافها من خلال إتباع أسلوب منهجي منظم لتقييم وتحسين فعالية عمليات إدارة المخاطر والرقابة والحوكمة" Suleiman and Dandago, 2014 & Elmaasrawy and Tawfik, 2025 &) .(Awinbugri and Daniel., 2019 & Hepworth et al., 2022

ومن التعريف السابق؛ يتضح اتساع نطاق وظيفة المراجعة الداخلية من مجرد وظيفة تهدف إلى التحقق من مدى الالتزام إلى مرحلة يُنظر فيها لوظيفة المراجعة الداخلية على إنها خدمة ذات قيمة مضافة للمنشأة تضمن الشفافية والموضوعية، وتحسين كفاءة العمليات، وحماية الأصول، وتحسين الإدارة المالية، وتحقيق أهداف المنشأة (Suleiman and Dandago, 2014 & Inyang et al., 2021 & Koutoupis and Kampouris, 2021 &)؛ ولم يكن هذا التطور في وظيفة المراجعة الداخلية هو وليد اللحظة؛ ولكنه نتاج لتفاعل مستمر بين المتغيرات البيئية والتنظيمية والتكنولوجية؛ ولذلك فقد مر هذا التطور بأربعة مراحل؛ وهي (Serag and Daoud, 2021 & محمد، ٢٠١٩ & شحاته، ٢٠٢٢):

- **المرحلة الأولى (١٩٠٠-١٩٤١)**: وفيها تم إنشاء قسم منفصل لوظيفة المراجعة الداخلية بهدف تتبع مراجعة العمليات المالية والمحاسبية والتأكد والتحقق من مدي دقة المعالجات المالية والمحاسبية التي تمت من قبَل القائمين بالعمل.
- **المرحلة الثانية (١٩٤١-١٩٧٧):** وفيها تم الاعتراف بالمراجعة الداخلية كمهنة لها مقوماتها التي تمكنها من تحقيق الغرض منها وذلك من خلال إنشاء (IIA) وما صاحبه من وجود معايير مهنية لممارسة ومزاولة المراجعة الداخلية، وقواعد للسلوك المهني يجب الالتزام بها، والالزام بضرورة التعلم والتدريب المستمر لممارسيها. فضلاً عن تقديم (IIA) عام (١٩٤٧) تعريفاً للمراجعة الداخلية على إنها "نشاط تقييمي مستقل داخل المنشأة يهدف لمراجعة العمليات كأساس لتقديم خدمات وقائية وبناءة للإدارة".

■**المرحلة الثالثة (١٩٧٧-١٩٨٧):** وجاءت هذه المرحلة كاستجابة للتطورات والتغيرات في بيئة الأعمال؛ وفيها قام (IIA) بتشكيل لجان لتطوير الإطار المتكامل لمعايير الأداء المهني للمراجعة الداخلية وما صاحبها من إعادة تعريف المراجعة الداخلية لتصبح "نشاط تقييمي مستقل داخل المنشأة يهدف لمراجعة عمليات المنشأة بغرض فحص وتقييم وتحليل الأنشطة داخل المنشأة"؛ ويتضح من هذا التعريف اتساع نطاق وظيفة المراجعة الداخلية من مجرد التوكيد على عملية إعداد التقرير المالي إلى التوكيد على العمليات التشغيلية للمنشأة ككل وهو ما يتطلب التشجيع على وجود هياكل رقابية فعالة.

■**المرحلة الرابعة (١٩٨٧- حتى الآن):** وفيها تم تعريف المراجعة الداخلية وفقا للتعريف الصادر من (IIA, 1999) والمتسق مع التعريفات التي تم إصدارها لاحقاً والذي يشير إلى اتساع نطاق وظيفة المراجعة الداخلية باعتبارها وظيفة رسمية داخل المنشآت الحديثة لتشمل على تحسين كافة عمليات المنشأة وإضافة قيمة لها من خلال أداء دوريها التوكيدي والاستشاري في ثلاث مجالات جديدة وهي إدارة المخاطر وعمليات الحوكمة والرقابة.

وبشأن مصفوفة أدوار ومجالات وظيفة المراجعة الداخلية؛ تعتبر وظيفة المراجعة الداخلية أداة مستقلة من أدوات الرقابة الداخلية الفعالة والمضيفة للقيمة للمنشأة من خلال أداءها لدورين أساسين وهما التوكيدي[١] والاستشاري[٢]؛ وذلك في

[١] خدمات التوكيد هي خدمات مهنية مستقلة تستهدف تحسين جودة ومحتوى المعلومات المالية وغير المالية المفصح عنها لأصحاب المصلحة؛ والعمل على زيادة ثقتهم فيها وخلوها من الأخطاء الجوهرية؛ وهي خدمات ثلاثية الأطراف وهم؛ الطرف المسئول عن توفير المعلومات، والطرف المسئول عن إضفاء الثقة على المعلومات والمتمثل في المراجع الداخلي، والطرف المستخدم للمعلومات والمتمثل في إدارة الشركة؛ ويتمثل المنتج النهائي للدور التوكيدي للمراجع الداخلي في تقديم تقرير يوضح نتيجة التوكيد في شكل رأي أو استنتاج أو تقييم (Badawy, 2021 & Elmaasrawy and Tawfik, 2025).

[٢] الخدمات الاستشارية تهدف إلى تقديم خدمات استشارية وإصدار أحكام بشأن موقف معين؛ وهي خدمات ثنائية الأطراف وهم؛ مقدم الخدمة والمتمثل في المراجع الداخلي، وطالب الخدمة والمتمثل في إدارة الشركة؛ ويتمثل المنتج النهائي للدور الاستشاري للمراجع الداخلي في تقديم النصح والمشورة التي تضيف قيمة إلى عمليات الرقابة الداخلية وإدارة المخاطر والحوكمة شريطة الحفاظ على استقلاليته وموضوعيته عند أداء هذا الدور (Elmaasrawy and Tawfik, 2025).

ثلاثة مجالات رئيسية وهي إدارة المخاطر والرقابة الداخلية وحوكمة الشركات. **فبالنسبة للدور التوكيدي للمراجعة الداخلية في مجال حوكمة الشركات؛** فيتمثل في التوكيد على مدى شفافية ومصداقية وسلامة التقارير المقدمة لإدارة الشركة حول مدى الالتزام بالممارسات القياسية لحوكمة الشركات؛ **أما فيما يتعلق بالدور التوكيدي للمراجعة الداخلية في مجال الرقابة الداخلية** فيتمثل في إبداء الرأي حول مدى سلامة تصميم وكفاءة وفعالية تشغيل هيكل الرقابة الداخلية في تحقيق أهدافه المتمثلة في صدق القوائم المالية، والالتزام بالقوانين واللوائح، ودعم كفاءة وفعالية العمليات التشغيلية؛ **أما فيما يتعلق بالدور التوكيدي للمراجعة الداخلية في مجال إدارة المخاطر؛** فيتمثل في إضفاء الصدق على تقارير إدارة المخاطر المعدة من قبَل المسئولون عن عمليات إدارة المخاطر والمقدمة إلى إدارة الشركة، وتقييم مدى فعالية العمليات المستخدمة في تحديد مخاطر الأعمال الجوهرية وإدارتها، ومدى فعالية تصميم وتشغيل عمليات إدارة المخاطر (Babiker, 2025 & محمد، ٢٠١٩).

وبالنظر إلى الدور الاستشاري للمراجعة الداخلية في مجال حوكمة الشركات؛ فيتمثل في تقديم النصح للإدارة بشأن كيفية التعامل وتشغيل آليات حوكمة الشركات، والمساهمة في وضع آليات واضحة للمساءلة فيما يتعلق بمدى تحقيق الأهداف المنشودة، وتقديم توصيات لتحسين عمليات الحوكمة؛ أما فيما يتعلق **بالدور الاستشاري للمراجعة الداخلية في مجال الرقابة الداخلية؛** فيتمثل في إبداء المشورة بشأن إعداد وتصميم نموذج لهيكل الرقابة الداخلية، واقتراح آليات لتحسين فعاليته لتدنية نقاط الضعف وتحقيق الكفاءة التشغيلية لموارد الشركة، واقتراح وتصميم برامج تدريبية لتعريف الموظفين بالتشريعات والقوانين واللوائح التي يجب الالتزام بها عند القيام بالأنشطة ذات الصلة بعمليات الشركة؛ في حين أن **الدور الاستشاري للمراجعة الداخلية في مجال إدارة المخاطر** فيتمثل في تقديم النصح للإدارة بشأن تحديد وتوصيف وقياس المخاطر التي تواجهها الشركة، وكذلك أهم المقترحات المتعلقة باستراتيجية إدارة المخاطر، والعمل على تقديم توصيات بشأن تحسين عمليات إدارة المخاطر والاستجابة لها (Babiker, 2025 & محمد، ٢٠١٩).

وفي الآونة الأخيرة؛ ازداد اهتمام الشركات بالدور الذي تلعبه المراجعة الداخلية كأحد الأدوات الرقابية في مجال تحقيق الأمن السيبراني، واتخاذ الإجراءات التصحيحية اللازمة للحد من المخاطر السيبرانية المتوقعة، وتحسين استراتيجية الشركة في إدارة تلك المخاطر وذلك من خلال دوريها التوكيدي والاستشاري. وبالتركيز على الدور التوكيدي والاستشاري للمراجعة الداخلية في مجال الأمن السيبراني؛ فيمكن القول أن **الدور التوكيدي للمراجعة الداخلية في مجال الأمن السيبراني** يتمثل في توفير توكيد بشأن فعالية تصميم وتنفيذ عمليات إدارة المخاطر السيبرانية، وتوفير دليل مستقل عن سياسات الأمن السيبراني ومدى الالتزام بها، وتوفير توكيد بأن المخاطر السيبرانية قد تم تقييمها بشكل مناسب، فضلاً عن التوكيد على تقارير إدارة المخاطر بشأن إدارة مخاطر الأمن السيبراني؛ بينما يتمثل **الدور الاستشاري للمراجعة الداخلية في مجال الأمن السيبراني** في تقديم النصح والمشورة والإرشاد لإدارة الشركة بشأن تحديد وتوصيف وقياس مخاطر الأمن السيبراني المحيطة بالبيئة التكنولوجية للشركة، وكيفية التصدي لتلك المخاطر والاستجابة لها والحد منها لتفادي آثارها السلبية على قدرة الشركة على تحقيق الأهداف المنشودة، وإجراء تحديث دوري ومتابعة لتلك المخاطر، ووضع توصيات بشأن الحد الأدنى المقبول لمخاطر الأمن السيبراني، وكيفية تحسين عمليات إدارتها، وإعداد خطط طوارئ للتعامل مع أي هجمات الكترونية محتملة (Elmaasrawy and Tawfik, 2025 & Babiker, 2025 & Inyang et al., 2021 & Johari et al., 2023 & يوسف، ٢٠٢٤).

وبناءاً على ما سبق؛ أمتد نطاق نشاط المراجعة الداخلية لتشمل على مجالات متعلقة بالأمن السيبراني وما يصاحبه من تحمل المراجع الداخلي لأعباء ومسئوليات جديدة؛ وتتمثل مسئوليات ومجالات مراجعة الأمن السيبراني في أربعة مجالات وهي؛ (١) **مراجعة السياسات والحوكمة**: وتتضمن مراجعة سياسات وإجراءات واستراتيجيات المنشأة المتعلقة بتحديد وتقييم وإدارة المخاطر السيبرانية للتأكد من كفايتها وملائمتها لطبيعة عمل الشركة وحجمها وبيئة عملها، فضلاً عن القيام بتحديثها ومتابعتها بشكل دوري، وتقديم التوصيات بشأن كيفية التعامل مع المخاطر وإدارتها

وتحديد مستوى الخطر المقبول؛ (٢) **مراجعة الضوابط الفنية**: وتتضمن التحقق من أن استثمارات الأمن السيبراني قد تم إنفاقها بحكمة في المكان المناسب وبالمبلغ المناسب، وتقديم توكيد للجنة المراجعة ومجلس الإدارة بشأن كفاية البنية التحتية المعلوماتية لتحقيق الأمن السيبراني في ظل الظروف القائمة؛ (٣) **استمرارية الأعمال**: وتتضمن وضع الخطط لمواصلة العمليات في حالة وقع أي تهديد سيبراني، والعمل على إدارة الأزمات والاستجابة السريعة للمخاطر والتعافي منها في التوقيت الملائم؛ (٤) **مراجعة الضوابط التشغيلية والرقابية**: وتتضمن مراجعة سياسات ومعايير وإجراءات الأمن السيبراني للتأكد من فعاليتها وملائمتها وترابطها بجانب التحقق من أن الضوابط الرقابية تغطي كافة النصوص الواردة في تلك السياسات والمعايير والإجراءات، فضلاً عن التحقق من اكتمال عمليات التوثيق وتحديثها باستمرار وتقديم التوصيات بشأنها (عطية، ٢٠٢١ & فريد، ٢٠٢٢).

وبناءاً على ما سبق؛ تعتبر وظيفة المراجعة الداخلية بدوريها التوكيدي والاستشاري عنصر فعال في تقييم مخاطر الأمن السيبراني والحد منها وإدارتها، وتعزيز التدابير الاستباقية لإدارة الأزمات وتحديثها باستمرار، وإضافة قيمة للمنشأة من خلال تحسين وتطوير إطار عمل إدارة المخاطر المؤسسية، وتطوير برامج حوكمة تكنولوجيا المعلومات، وتحقيق الأهداف الاستراتيجية للمنشأة، والحد من السلوك الانتهازي للإدارة، وحماية الأصول وتأمينها، وزيادة دقة وموضوعية وموثوقية المعلومات المالية والتشغيلية، وزيادة كفاءة وفعالية العمليات التشغيلية، وزيادة الالتزام بالقوانين واللوائح والمعايير والسياسات والإجراءات، وزيادة ثقة العملاء، وتحسين سمعة الشركة، وزيادة حصتها السوقية، وزيادة كفاءة وفعالية عملية المراجعة الخارجية[١] (Hepworth et al., 2022 & Babiker, 2025 &

[١] أدى التحول الرقمي إلى زيادة مخاطر المراجعة الخارجية نتيجة للتسجيل الالكتروني واختفاء المستندات والأدلة الورقية وظهور الأدلة الإلكترونية التي يصعب تتبعها وصعوبة الرقابة على البرامج الإلكترونية وزيادة مخاطر فقد البيانات والمستندات الالكترونية وسوء استخدام البنية التحتية المعلوماتية؛ الأمر الذي تطلب ضرورة وجود تكامل بين وظيفتي المراجعة الداخلية والمراجعة الخارجية لما له من آثار إيجابية تساعد على زيادة دقة وموثوقية وجودة البيانات المالية وما يرتبط به من زيادة ثقة أصحاب المصلحة، وتقليل تأخير تقرير المراجعة الداخلية، والحد من مخاطر

Slapnicar et al., 2022 & Awinbugri and Daniel., 2019 & Seetharaman et a., 2008 & Alina et al., 2017 & Dikokoe, 2021).

وبناءاً على ما سبق؛ **يرى الباحثان** أن إطار عمل المراجعة الداخلية فيما يتعلق بمجال الأمن السيبراني يتمثل في تزويد مجلس الإدارة ولجان المراجعة ولجان المخاطر التابعة لها بضمانات مستقلة حول فعالية ضوابط تحقيق الأمن السيبراني، واستراتيجيات إدارة مخاطر الأمن السيبراني، ومراجعة مدى كفاية العمل الذي يقوم به موظفي أمن المعلومات، ومراجعة مدى قدرة آليات حوكمة تكنولوجيا المعلومات على تدعيم استراتيجيات وأهداف المنشأة، والتعرف على الثغرات في السياسات والإجراءات التي يتم تنفيذها والمتعلقة بأمن المعلومات، فضلاً عن تقديم النصح والمشورة بشأن تحديد وتوصيف وقياس مخاطر الأمن السيبراني، وأفضل الممارسات لتحقيق الأمن السيبراني وإدارة المخاطر الصاحبة له.

ولكي تقوم وظيفة المراجعة الداخلية بدوريها التوكيدي والاستشاري في مجال الأمن السيبراني بفعالية وكفاءة لابد من توافر مجموعة من المتطلبات لدعم الدور الفعال للمراجع الداخلي في هذا المجال؛ ومن أهم تلك المتطلبات؛ (١) **وجود تنظيم مهني للمراجعة الداخلية:** والذي يشير إلى وجود تنظيم مهني للمراجعة الداخلية الحديثة تنصب مهامها على تنظيم عمل المراجع الداخلي، والإشراف عليه، والحفاظ على استقلاله التنظيمي، وتنمية قدراتهم العلمية والعملية في مجال نظم تكنولوجيا المعلومات، وإصدار الإرشادات والضوابط المهنية اللازمة لتطوير المنهج التقليدي للمراجعة الداخلية[١] ورفع

المراجعة الخارجية، وتخفيض أتعاب مراقب الحسابات. ويلعب مراقب الحسابات دوراً هاماً في مجال الأمن السيبراني من خلال التوكيد عن مخاطر الأمن السيبراني وما يرتب عليه من الحد من عدم تماثل المعلومات وزيادة قدرة أصحاب المصلحة في تقييم الأداء الحالي والمستقبلي للشركة، وتقدير اسعار الأسهم والارباح المتوقعة ومن ثُم اتخاذ قرارات اقتصادية رشيدة وتحسين كفاءة السوق. ويتوقف قرار مراقب الحسابات الخارجي بالاعتماد على وظيفة المراجعة الداخلية على الوضع الوظيفي للمراجعة الداخلية داخل الشركة ومدي استقلاليتها وموضوعيتها (Suleiman and Dandago, 2014 & Badawy, 2021 & الصيرفي، ٢٠٢٥ & محمود، وآخرون، ٢٠٢٥).

[١] أحد أهم الطرق لتطوير المنهج التقليدي للمراجعة الداخلية في مجال الأمن السيبراني هو إتباع المنهجية الرشيقة في المراجعة الداخلية؛ ويمكن تعريف المراجعة الداخلية الرشيقة على إنها "طريقة للتفكير تركز على القيمة، وتعزيز التعاون مع اصحاب المصالح، وتحقيق الانضباط الزمني في تنفيذ مهام المراجعة، وتقديم أفكار وتوفير الاستجابات في

جودتها وخصوصا في ظل الأدوار والمسئوليات المستحدثة في بيئة التحول الرقمي وما يصاحبها من مخاطر متعلقة بالأمن السيبراني، **(٢) رفع مستوى التأهيل العلمي والعملي لفريق المراجعة الداخلية بالمنشأة:** فوجود فريق مراجعة داخلي ملم بالنواحي المتعلقة بتقنيات وآليات المراجعة في ظل نظم تكنولوجيا المعلومات المتطورة، وحاصل بعض أعضائه على شهادات الأمن المناسبة مثل (CSP & CDP & CISM & CISSP) وشهادات مراجعة أمن أنظمة المعلومات (CRISC & QICA & CISA) سيزيد من قدرتهم على تطوير علاقات أفضل مع وظائف أمن المعلومات وتكنولوجيا المعلومات[١] وما يتعبه من المساهمة الفعالة في بناء برنامج لإدارة مخاطر الأمن السيبراني أكثر جودة وفعالية؛ **(٣) تكرار الاجتماعات بين إدارة المراجعة الداخلية ولجنة المراجعة:** يلعب المراجع الداخلي دوراً فعالاً في مساعدة لجنة المراجعة في الإشراف على العمليات المرتبطة بالأمن السيبراني؛ وكلما زاد تكرار الاجتماعات بين المراجع الداخلي ولجنة المراجعة كلما قل احتمالية حدوث مشاكل تتعلق بمراجعة الأمن السيبراني نظراً للتواصل الدائم وما يصاحبه من تقارب في وجهات النظر بين إدارة المراجعة الداخلية ولجنة المراجعة؛ **(٤) مشاركة إدارة المراجعة الداخلية في إدارة المخاطر المؤسسية:** هذه المشاركة من شأنها مساعدة المراجعين الداخليين في إتباع المدخل الابتكاري

الوقت المناسب وذلك من خلال تطوير الأعمال والتخطيط وتكراره والتعاون مع كافة الأطراف ذات الصلة". ومن التعريف السابق نستنتج أن للمراجعة الداخلية الرشيقة العديد من المزايا ومنها (محروس، وصالح، ٢٠٢٢):

- تقديم مجموعة واسعة من المنتجات لما لها من قدرة على تكييف منتجاتها وخدماتها وفقاً للاحتياجات المتغيرة لأصحاب المصالح.
- تحقيق مرونة في خطط المراجعة، والتعامل الاستباقي مع المخاطر، والتعجيل بأداء مهام المراجعة في الوقت المناسب، وتقليل الفاقد من الموارد.
- تحويل مقاييس الأداء الرئيسية للمراجعة من المقاييس التقليدية (مثل إكمال خطة المراجعة، ونتائج المراجعة) إلى التركيز على مقاييس حديثة مثل رضا العملاء وعدد مرات التفاعل مع الخاضعين للرقابة والوقت المستغرق في تنفيذ أعمال المراجعة.
- تكوين فريق مراجعة متعدد التخصصات ويتمتع بالكفاءات والخبرات اللازمة لأداء مهام المراجعة والأنشطة المتنوعة بكفاءة وفعالية.

[١] العلاقات الجيدة بين وظيفتي المراجعة الداخلية ووظيفة أمن وتكنولوجيا المعلومات تزيد من القدرة على اكتشاف الهجمات السيبرانية قبل حدوثها؛ وتمنح للمراجعين الداخليين المزيد من القدرة على الوصول إلى أفضل الضوابط والإجراءات المتعلقة بتحقيق الأمن السيبراني شريطة أن تكون تلك العلاقات قائمة على الثقة والتشاور وتبادل الرؤى (Elmaasrawy and Sihvonen, 2019 & Hepworth et al., 2022).

الاستراتيجي، والتركيز على أهداف العمل بدلاً من التركيز على أهداف المراجعة فقط وما يصاحبه من زيادة قدرتهم على إجراء تقييم شامل للمخاطر السيبرانية، وتقديم نصائح وإرشادات للجنة المراجعة وأعضاء مجلس الإدارة حول تطوير خطة المراجعة الداخلية بشكل متضمن لمجالات الأمن السيبراني ومخاطرها؛ **(٥) تطوير نظام التعليم المحاسبي:** من خلال الاهتمام بتطوير برامج التعليم المحاسبي الرقمي وتحديثها باستمرار بما يتفق مع المتغيرات الديناميكية التكنولوجية المحيطة ببيئة العمل، وخصوصاً فيما يتعلق بالأدوار والمسئوليات المستحدثة التي تقع على عاتق المراجعين الداخليين في ظل بيئة التحول الرقمي وما يصاحبه من مخاطر الأمن السيبراني؛ **(٦) زيادة وعي الشركات بأهمية وظيفة المراجعة الداخلية كوظيفة مضيفة للقيمة:** ويتحقق ذلك من خلال توفير الاستقلال التنظيم لوظيفة المراجعة الداخلية، وتحديث اللوائح المالية والإدارية التنظيمية لوظيفة المراجعة الداخلية، والتنسيق بين لجنة المراجعة وإدارة المراجعة الداخلية، وتوفير الدعم من قبَل الإدارة التكنولوجية وما يصاحبه من المساعدة في اكتشاف نقاط الضعف الأمنية وتصميم توصيات لتحسين كفاءة وفعالية إدارة المخاطر السيبرانية، فضلاً عن تحديد واجبات ومسئوليات المراجعين الداخليين بالشركة وهو ما يؤدي إلى تدنية مستوى فجوة التوقعات Expectation Gab في المراجعة الداخلية[1]؛ (٧) **تنظيم وتفعيل الإفصاح عن مخاطر الأمن السيبراني وإدارتها**[2] (Islam et al., 2018 & Usman et al.,

[1] يمكن التفرقة بين ثلاث فجوات في المراجعة الداخلية وهي؛ (١) **فجوة المعلومات** والتي تشير إلى الفرق بين ما يحتاجه المستخدم وبين ما يحصل عليه فعلاً من خلال الأدوار التوكيدية والاستشارية للمراجعة الداخلية؛ (٢) **فجوة الاتصال** والتي تشير إلى الفرق بين ما يرغب فيه ويفهمه المستخدم وبين ما يتم توصيله فعلاً من قبَل المراجع الداخلي؛ (٣) **فجوة التوقعات** والتي تشير إلى الفرق بين ما يتوقعه المستخدم من المراجع الداخلي عند أدائه لدوريه التوكيدي والاستشاري وبين حقيقة ما تعنيه المراجعة الداخلية، وتنقسم فجوة التوقعات إلى مكونين رئيسين؛ **فالمكون الأول هو فجوة المعقولية** والتي تشير إلى الفرق بين ما يتوقعه الإدارة من المراجع الداخلي وبين ما يمكن أن يؤديه المراجع الداخلي بصورة معقولة؛ أما **المكون الثاني فهو فجوة الأداء** وتشير إلى الفرق بين ما تتوقعه الإدارة من مهام منجزة من قبَل المراجع الداخلي بصورة معقولة وبين الأداء الفعلي للمراجع الداخلي (محمد، ٢٠١٩). ومن الجدير بالذكر أن فجوة التوقعات هي فجوة ديناميكية غير صفرية، غير ساكنة بطبيعتها، تنمو بمرور الوقت، وليس من المنطقي القضاء عليها ولكن يمكن العمل على تضييقها (مرسي، ٢٠٢٣).

[2] كان لصدور قانون Sarbanes-Oxley عام ٢٠٠٢ تأثير بالغ الأثر على الإفصاح الاختياري عن أنشطة أمن المعلومات حيث زاد حجم الافصاح الاختياري حول مشاركة الشركة في تحديد وتقييم المخاطر السيبرانية والحد منها وإدارتها وهو ما يؤثر إيجابياً على تقليل احتمالات حدوث الهجمات السيبرانية والأحداث السلبية المصاحبة لها، والتأثير الإيجابي على أسعار الأسهم وقيمة الشركة، وتدعيم الاستقرار المالي للشركة؛ كما أنه وفقاً لنظرية الإشارة وفي ظل

2024 & Johari et al., 2023 & Steinbart et al., 2012 & Inyang et al., 2021 & Awinbugri and Daniel., 2019 & Vuko et al., 2025 Steinbart et al., 2018 & Serag and Daoud, 2021 & أميرهم، ٢٠٢٢ & أبو الخير، ٢٠٢٣ & شحاته، ٢٠٢٢).

وبناءاً على ما سبق؛ **يرى الباحثان** أن المراجعين الداخليين يواجهون العديد من التوقعات الجديدة والمتزايدة بخصوص الأمن السيبراني وما هو يتطلب من الشركات ضرورة القيام بتكثيف أهمية وظيفة المراجعة الداخلية للقيام بمزيد من الجهود لتقديم النصح والمشورة والتوكيد بشكل موضوعي ومستقل بشأن الضوابط والإجراءات الموضوعة للأمن السيبراني والعمل على تحسينها؛ فضلاً عن إقامة علاقات ثقة مع الوظائف الأخرى مثل وظيفة أمن المعلومات وتكنولوجيا المعلومات ودمجها في عمليات إدارة المخاطر السيبرانية، بالإضافة إلى قيام المراجع الداخلي بتعزيز المهارات والخبرات العلمية والعملية المتعلقة بتكنولوجيا المعلومات وإجراءات المراجعة في ظل بيئة التحول الرقمي وهو ما يترتب عليه زيادة فعالية هيكل الرقابة الداخلية بشأن مجالات الأمن السيبراني، وزيادة ثقة المراجع الخارجي في وظيفة المراجعة الداخلية، وتحسين الوضع الأمني للشركة وبالتالي تحسين الوضع الأمني العام.

٦-٣- تحليل الدراسات السابقة واشتقاق فروض البحث.

٦-٣-١- تحليل العلاقة بين توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني والقيمة المضافة من وظيفة المراجعة الداخلية؛ واشتقاق الفرض الأول.

عدم تماثل المعلومات بين الإدارة واصحاب المصلحة فإن زيادة حجم الإفصاحات الاختيارية من قبَل الشركة بشأن المعلومات المتعلقة بالأمن السيبراني قد يكون دليلاً على جودة الشركة وفعاليتها في تحقيق الأمن السيبراني وتطبيق الضوابط ذات الصلة وإدارة المخاطر المرتبطة به، وتقليل مستوى عدم تماثل المعلومات (Haapamaki and Sihvonen, 2019 & Song et al., 2024 & Hossain et al., 2025 & Badawy, 2021 & Usman et al., 2024)

قد لا تلبي جهود مسئولي تكنولوجيا المعلومات وأمن المعلومات احتياجات الإدارة فيما يتعلق بالفهم الواضح والعميق للمخاطر السيبرانية وإداراتها وذلك لسببين؛ أولهما: افتقار الإدارة للخبرة بمجال نظم تكنولوجيا المعلومات إذ غالباً ما تكون التقارير المقدمة معقدة فنياً ويصعب ربطها بأهداف العمل نظراً لتركيزها بشكل رئيسي على المخاطر التكنولوجية، وثانيهما: غياب التقييم والتوكيد الموضوعي والمستقل؛ وعليه فقد تلعب المراجعة الداخلية دوراً هاماً وفعالاً في التقييم الشامل للمخاطر السيبرانية، وتوفير توكيد بشأن إدارتها، وتوليد رؤى ثاقبة حول كيفية تحسين حوكمة أمن المعلومات، والحد من المخاطر السيبرانية، وتحسين ممارسات إدارة مخاطر الأمن السيبراني (Elmaasrawy and Tawfik, 2025 & Deloitte, 2017).

وفي نفس الشأن؛ استهدفت دراسة Kahyaoglu and Caliyurt (2018) تحليل آليات تحقيق الأمن السيبراني من منظور المراجعة الداخلية وإدارة المخاطر؛ وقد توصلت الدراسة إلى أن المراجعة الداخلية المتعلقة بالأمن السيبراني قد تعوض النقص الشديد في وعي أعضاء مجلس الإدارة بمخاطر الأمن السيبراني وآليات الحد منها وإداراتها، وتساعد على توفير توكيد مستقل بشأن إدارة مخاطر الأمن السيبراني بما يوفر الثقة لدي الأطراف أصحاب المصلحة، فضلا عن مساعدة مجلس إدارة الشركة في فهم تقارير إدارة تكنولوجيا المعلومات نظراً لتعقدها وتركيزها العميق على الجوانب الفنية بدلاً من الجوانب المالية والتشغيلية.

وفي نفس الصدد؛ استهدفت دراسة Islam et al. (2018) اختبار أثر المراجعة الداخلية على إدارة مخاطر الأمن السيبراني بالتطبيق على عينة تتكون من (٩٧٠) استجابة من خبراء المراجعة الداخلية؛ وقد توصلت الدراسة إلى أن زيادة جودة عملية المراجعة الداخلية يؤدي إلى تحسين حوكمة الشركات، وزيادة جودة التقارير المالية، والحد من السلوك الانتهازي الإداري، وإجراء تقييم شامل للمخاطر السيبرانية وهو ما يؤدي في النهاية إلى الإدارة الفعالة لمخاطر الأمن السيبراني.

وفي نفس الشأن؛ استهدفت دراسة Stafford et al. (2018) اختبار أثر فعالية وظيفة المراجعة الداخلية على التزام موظفي الشركة بسياسات وضوابط تحقيق الأمن السيبراني؛ وقد توصلت الدراسة إلى أن وظيفة المراجعة الداخلية قد تحد من عدم التزام موظفي الشركة بضوابط تحقيق الأمن السيبراني، وتزيد من القدرة على تحديد واكتشاف مجالات الخطر السيبراني، وتساعد على توليد النصح لموظفي الشركة بالفوائد والمنافع التي تعود على الشركة نتيجة الالتزام بالسياسات والإجراءات المتعلقة بتحقيق الأمن السيبراني والحد من المخاطر المصاحبة لها؛ وتوجيه الاستشارات المتعلقة بكيفية تحسين السلوكيات الانتهازية لموظفي الشركة والناتجة عن عدم الرضا؛ وكذلك الاستشارات المتعلقة بتدريب وتحفيز موظفي الشركة للانخراط في ممارسات تحقيق الأمن السيبراني؛ إلا أن هذا الدور الفعال بوظيفة المراجعة الداخلية في مجال الأمن السيبراني يتوقف على مدي إلمام المراجع الداخلي بالجوانب المتعلقة بتكنولوجيا المعلومات.

وفي نفس الصدد؛ استهدفت دراسة Shamsuddin et al. (2018) استكشاف العوامل المؤثرة على فعالية وظيفة المراجعة الداخلية في مجال الأمن السيبراني بالتطبيق على المؤسسات المصرفية الماليزية؛ وقد تم استخدام (١٢٠) استبياناً للحصول على بيانات الدراسة من المراجعين الداخليين في سبعة بنوك تجارية ماليزية؛ وقد توصلت الدراسة إلى أن هناك ثلاثة عوامل تؤثر على فعالية وظيفة المراجعة الداخلية في مجال الأمن السيبراني وهم؛ وعي المراجعين الداخليين بأهمية الأمن السيبراني، والسياسة التنظيمية ذات الصلة بالأمن السيبراني، وإدارة المخاطر التنظيمية المتعلقة بالأمن السيبراني.

وفي نفس الشأن؛ استهدفت دراسة Dikokoe (2021) اختبار أثر وظيفة المراجعة الداخلية على إدارة مخاطر الأمن السيبراني؛ ولتحقيق هدف الدراسة تم إجراء تحليل محتوى للتقارير والقوائم المالية السنوية لعينة من الجهات الحكومية بجنوب أفريقيا؛ وقد توصلت الدراسة إلى أن المراجعة الداخلية الفعالة قد تساعد على

زيادة درجة الالتزام بالقوانين واللوائح، والتحديد الدقيق للمخاطر السيبرانية وفهمها، والتقييم الموضوعي لفعالية وكفاية الممارسات والإجراءات المعنية بالحد من الآثار السلبية المرتبطة بمخاطر الأمن السيبراني، وتقديم توكيدات لتقييم مدي فعالية ممارسات إدارة مخاطر الأمن السيبراني، وتقديم توصيات لتحسين إجراءات الأمن السيبراني، وبالتالي تحسين بيئة الرقابة.

كما استهدفت دراسة أميرهم (٢٠٢٢) دراسة واختبار أثر جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني وانعكاساته على ترشيد قرارات المستثمرين؛ ولتحقيق هذا الهدف تم إجراء دراسة ميدانية على عينة من مسئولي المراجعة الداخلية، ومسئولي تكنولوجيا المعلومات، ومسئولي إدارة المخاطر، والمستثمرين في شركات الاتصالات المقيدة بورصة الأوراق المالية المصرية؛ وقد توصلت الدراسة إلى أن وظيفة المراجعة الداخلية تلعب دوراً رئيسياً وفعالاً في تقييم عمليات إدارة مخاطر الأمن السيبراني، وفي تكوين رؤي حول كيفية تحسين وحوكمة أمن المعلومات وجهود إدارة المخاطر، وتزويد الإدارة ولجنة المراجعة بتوكيد مستقل بشأن مدى فعالية سياسات وإجراءات واستراتيجيات إدارة مخاطر الأمن السيبراني؛ وبالتالي العمل على تحسين وترشيد عملية اتخاذ القرارات الاستثمارية.

وفي نفس الصدد؛ استهدفت دراسة Slapnicar et al. (2022) اختبار أثر فعالية وظيفة المراجعة الداخلية في تحقيق الأمن السيبراني، والتعرف على كيفية مساهمتها في إدارة مخاطر الأمن السيبراني؛ وذلك من خلال إجراء دراسة تجريبية على مجموعة دولية تتكون من (١٨٣) مراجع داخلي مستخدم لنظم تكنولوجيا المعلومات؛ وقد توصلت الدراسة إلى أن وظيفة المراجعة الداخلية تؤثر إيجابياً على تحقيق الأمن السيبراني وممارسات إدارة مخاطر الأمن السيبراني؛ إلا أن التأثير الإيجابي السابق

ذكره يتوقف على التخطيط المسبق لإدارة المخاطر[١]، والتنفيذ الفعال لضوابط المراجعة الداخلية المتعلقة بالأمن السيبراني.

كما استهدفت دراسة Johari et al. (2023) اختبار أثر التحول الرقمي والتهديدات الأمنية السيبرانية على تطور دور المراجع الداخلي وذلك من خلال إجراء دراسة تجريبية على مجموعة من المراجعين الداخليين المتخصصين في مراجعة نظم تكنولوجيا المعلومات باعتبارهم الجهة المسئولة عن إجراء التقييم المتعلق بالأمن السيبراني بالمنشأة، وقد توصلت الدراسة إلى أن بيئة الأعمال الرقمية قد أثرت على وظيفة المراجعة الداخلية من خلال ثلاث طرق رئيسية وهم؛ (١) زيادة المهارات التحليلية والمعرفة الرقمية وتقنيات المراجعة الحديثة لدى المراجع الداخلي بما يمكنه من تحديد وتقييم التهديدات السيبرانية المحتملة بكفاءة وفعالية، (٢) التعاون الفعال بين وظيفتي المراجعة الداخلية وتكنولوجيا المعلومات، (٣) زيادة الطلب على الدور التوكيدي والاستشاري للمراجعة الداخلية في مجال الأمن السيبراني لمساعدة المنشأة على التعامل مع رقمنة بيئة الأعمال والمخاطر المصاحبة لها والنجاح في ظل بيئة العمل الرقمية.

وفي نفس الشأن استهدفت دراسة Babiker (2025) اختبار أثر إجراءات المراجعة الداخلية في تحسين فعالية الأمن السيبراني وذلك من خلا استطلاع آراء (٣٠) مراجعاً داخلياً من المملكة العربية السعودية ومصر؛ وقد توصلت الدراسة إلى وجود تأثير إيجابي لكفاءة وفعالية عملية المراجعة الداخلية على تحسين فعالية عمليات الأمن السيبراني من خلال العمل على رصد وتحديد وتحليل للمخاطر السيبرانية بشكل دقيق، وتحديد نقاط الضعف بالمنشأة، والمساعدة في تقديم النصح والمشورة بشأن إدارة تلك المخاطر بشكل فعال.

[١] يتمثل التخطيط المسبق لإدارة المخاطر في تحديد الاصول الرقيمة الأكثر قيمة للمنشأة، وتحديد عواقب تعرضها للمخاطر، وتقييم نقاط الضعف المرتبطة بالأصول الرقمية، وتقييم احتمالية تعرضها لهجمات سيبرانية، وتطبيق المراجعة الفورية عبر الانترنت، والتقييم المستمر لحالة أمان النظام (Slapnicar et al., 2022).

وبناءاً على تحليل الدراسات السابقة؛ **خلص الباحثان** إلى أن وظيفة المراجعة الداخلية قد تلعب دوراً هاماً وفعالاً في إدارة مخاطر الأمن السيبراني والحد منها، وإجراء تقييم شامل للمخاطر السيبرانية، وزيادة دقة وموضوعية وموثوقية المعلومات المحاسبية، وتحسين الأداء التشغيلي للمنشأة، وزيادة درجة الالتزام بالقوانين واللوائح، وبالتالي تحسين سمعة المنشأة؛ وقد يزداد فعالية هذا الدور بالنسبة للأطراف أصحاب المصلحة فيما يتعلق بتحقيق الأمن السيبراني في حال التوكيد من قبَل وظيفة المراجعة الداخلية على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني؛ **وبناءاً عليه يمكن اشتقاق الفرض الأول (H1) كالتالي:**

H1: يؤثر توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني إيجاباً ومعنوياً على القيمة المضافة من وظيفة المراجعة الداخلية.

٦-٣-٢- تحليل أثر الإسناد الخارجي لوظيفة المراجعة الداخلية ونوع وخبرة أصحاب المصالح على العلاقة محل الدراسة؛ واشتقاق الفرض الأخرى.

٦-٣-٢-١- تحليل أثر الإسناد الخارجي لوظيفة المراجعة الداخلية على العلاقة محل الدارسة؛ واشتقاق الفرض الثاني.

أصبحت عملية الإسناد من الممارسات المهنية الشائعة ليس في مجال المراجعة الداخلية فحسب؛ بل أيضاً في العديد من المجالات الأخرى لما لها من مزايا تساعد الشركة في التركيز على المزايا التنافسية والأنشطة الرئيسية للشركة، وتحسين جودة الخدمات المقدمة، وتوفير النفقات نظراً لتمتع الموفر الخارجي للخدمة باقتصاديات الحجم الكبير (Rittenberg et al., 1999).

ويمكن **تعريف الإسناد بوجه عام** على إنه "الارتباط مع أفراد أو منشآت من خارج المنشأة للقيام بأداء خدمات كانت تؤدي في السابق من قبَل اشخاص داخل المنشأة أو يمكن تأديتها داخل المنشأة" (Ahlawat and Lowe, 2004). كما يمكن تعريف الإسناد على إنه "عملية تعاقدية بين المنشأة وأي طرف خارجي؛ وبموجبها يقوم

الطرف الخارجي بتوفير خدمات ومنتجات للمنشأة كان يمكن توفيرها من خلال مصادر داخل المنشأة" (Carey et al., 2006).

وبالتركيز على **الإسناد الخارجي في مجال المراجعة الداخلية؛** نجد أنه في الآونة الأخيرة؛ أدت التطورات التكنولوجية والتغيرات الحديثة والتحول نحو البيئة الرقمية إلى إحداث تطورات كبيرة في وظيفة المراجعة الداخلية تستدعي ضرورة التوجه نحو الاستعانة بمصادر خارجية للقيام بأداء وظائف المراجعة الداخلية (Seetharaman et al., 2008). ويمكن تعريف الإسناد الخارجي لوظيفة المراجعة الداخلية على إنه "قرار استراتيجي لإدارة الشركة بتعهيد أداء كل أو بعض وظائف المراجعة الداخلية التي يجب أداؤها داخل الشركة لطرف من خارج الشركة بناءاً على تحليل المنافع والتكاليف المنظورة وغير المنظورة للقرار" (محمد، ٢٠١٩).

وبشأن **التأصيل النظري والمهني للإسناد الخارجي لوظيفة المراجعة الداخلية؛** ففي عام ١٩٩٦أصدر (AICPA) من خلال لجنة أخلاقيات المهنة القاعدة التفسيرية رقم (١٠١) والتي ترتبط بإمكانية الاستعانة بالمراجع الخارجي للقيام بوظيفة المراجعة الداخلية ما لم يضعف ذلك من استقلاليته (Rittenberg and Covaleski, 2001). ووفقاً لقانون Oxley Act Sarbanes- الذي تم إصداره عام ٢٠٠٢ فقد نص القسم رقم (٢٠٢) على منع قيام المراجع الخارجي بتقديم خدمات أخرى لعملاء المراجعة الداخلية؛ ولكن لم يمنع هذا القانون إسناد وظائف المراجعة الداخلية لطرف خارجي آخر بخلاف المراجع الخارجي الذي يقوم بمراجعة التقارير والقوائم المالية، وهو ما تم تأييده من خلال لجنة (SEC) (Suleiman and Dandago, 2014 & Caplan et al., 2007).

وفي نفس الصدد؛ قام (IIA) عام ١٩٩٤ بمعارضة الإسناد الخارجي لوظيفة المراجعة الداخلية وضرورة وجود قسم مستقل لإدارة المراجعة الداخلية بالمنشأة بحجة أن المراجعين الداخليين أكثر معرفة بأعمال وعمليات المنشأة مقارنةً بالطرف الخارجي مما يزيد من كفاءة وفعالية وظيفة المراجعة الداخلية؛ إلا أنه تراجع في عام

١٩٩٦ وأوضح أنه يجب التركيز على من يؤدي الخدمة بصورة أفضل بغض النظر عما إذا كان من داخل المنشأة أو من خارجها؛ وقد تنامي هذا الدور للطرف الخارجي للقيام بوظيفة المراجعة الداخلية حيث أقر (IIA, 2009) بأن العديد من اتفاقيات الشراكة مع المقدمين الخارجيين لوظيفة المراجعة الداخلية كانت فعالة في مساعدة المنشآت في تحقيق ميزة تنافسية والحصول على خدمات مراجعة داخلية قادرة على تحقيق الأهداف الاستراتيجية للمنشأة وبتكلفة أقل وهو ما يؤدي في النهاية إلى إضافة قيمة للمنشأة وتحسين عملياتها (Suleiman and Dandago, 2014 & Caplan et al., 2007 & محمد، ٢٠١٩).

وبشأن **الاستراتيجيات المتعلقة بالإسناد الخارجي لوظيفة المراجعة الداخلية؛** فهناك عدة بدائل وهي (Del Vecchio and Clinton, 2003 & Seetharaman et al., 2008 & محمد، ٢٠١٩): (١) الإسناد الخارجي الكلي (Total Outsourcing): وتعني أداء كافة أنشطة وظيفة المراجعة الداخلية من قبّل طرف خارجي؛ (٢) الإسناد الخارجي الجزئي (Partial Outsourcing): وفيه يتم إسناد بعض مهام وظيفة المراجعة الداخلية إلى إدارة المراجعة الداخلية الخاصة بالمنشأة، ويتم إسناد باقي المهام الأخرى إلى طرف خارجي للقيام بها؛ (٣) الإسناد الخارجي التعاوني المشترك (Co-Outsourcing): وفيه يتم أداء مهام وظيفة المراجعة الداخلية بالتعاون المشترك بين إدارة المراجعة الداخلية والطرف الخارجي جنباً إلى جنب دون تقسيم مهام معينة لأحدهما.

وهناك مجموعة من **المحددات التي تؤثر على قرار الإسناد الخارجي**[١] **لوظيفة المراجعة الداخلية؛** وهي القضايا الاستراتيجية للمنشأة، والظروف المالية للمنشأة،

[١] هناك مجموعة من النظريات التي تفسر قرار المنشأة بالإسناد الخارجي؛ وهي (محمد، ٢٠١٩): (١) **نظرية إقتصاديات تكلفة العمليات** (Transaction Cost Economics): وفيها يتم الإسناد الخارجي لوظيفة المراجعة الداخلية إذا كانت المنافع المحققة للشركة أكبر من التكلفة المرتبطة بها؛ (٢) **النظرية المعتمدة على الكفاءة** (The Competence Based View Theory): وفيها يتم الإسناد الخارجي للأنشطة غير الرئيسية وغير الجوهرية، في حين أن الأنشطة الرئيسية والجوهرية التي تمثل بمثابة ميزة تنافسية للشركة يتم أدائها داخل المنشأة؛ (٣) **النظرية**

والكفاءات والمهارات المهنية المتوافرة لدي المنشأة، ودرجة عدم تماثل المعلومات، ودرجة المرونة التنظيمية للمنشأة، ومستوى مخاطر الأمن السيبراني، ومستوى السلوك الأخلاقي لإدارة الشركة، وحجم الشركة، ودرجة الرفع المالي، واحتياجات ومتطلبات إدارة الشركة، والظروف التنافسية للمنشأة (Houqe et al., 2015 & Peursem and Jiang, 2008 & Schneider, 2008 & Calvin et al., 2025).

وبشأن دوافع ومنافع إسناد وظيفة المراجعة الداخلية؛ فهي تتمثل في السماح لإدارة الشركة بالتركيز على الأنشطة الاستراتيجية الرئيسية، وتوفير درجة كبيرة من الاستقلالية والموضوعية والحيادية، وتوفير مخزون من الخبرات والمعارف المهنية المتخصصة والاستفادة منها في الوصول إلى أفضل الممارسات المتعلقة بتحديد وتقييم المخاطر وإداراتها وتقييم فعالية آليات إدارة المخاطر[١]، وزيادة قدرة الشركة على الوصول إلى التخصص الصناعي والاستفادة من المزايا المتعلقة به، ومساعدتها على تجنب التكاليف الباهظة المتعلقة بتدريب وتعيين موظفين داخليين للقيام بوظيفة المراجعة الداخلية وما يرتبط بها من تكاليف توظيف عمالة دائمة طويلة الأجل وبالتالي تحويل التكاليف الثابتة إلى تكاليف متغيرة، وزيادة المرونة التنظيمية بما يزيد من قدرتها على التعامل مع ظروف السوق المتغيرة ومتطلبات الشركة الديناميكية، وزيادة جودة عملية المراجعة الداخلية، وانخفاض تكلفة رأس المال، وتحسين الأداء المالي للشركة، وزيادة قدراتها التنافسية، وبالتالي زيادة اعتماد المرجع الخارجي على مخرجات وظيفة المراجعة الداخلية (Houqe et al., 2015 & Schneider, 2008 & Peursem and Jiang,

---

المعتمدة على الموارد (Resource Based View Theory): وفيها يتم الإسناد الخارجي للوظائف في حال عدم امتلاك الشركة للموارد الكافية التي تمكنها من أدائها بشكل كفء وفعال، وبالتالي فإن قرار الإسناد الخارجي هو قرار استراتيجي يستخدم لسد الفجوة بين إمكانيات المنشأة ومتطلباتها؛ (٤): **النظرية التعاقدية** (Contractual Theory): تقوم الشركة باتخاذ قرار الإسناد الخارجي في حال التأكد من الالتزام بالشروط التعاقدية من قبل أطراف التعاقد؛ (٥): **نظرية الوكالة** (Agency Theory): وفيها يقوم الطرف الأصيل (طالب الخدمة) بإسناد الأنشطة التي تتسم بعدم التأكد من نتائجها ونقل المخاطر المرتبطة بها إلى الوكيل (الطرف الخارجي موفر الخدمة).

[١] يتمتع موفر الخدمة الخارجي بالقدرة على توجيه مزيد من الاستثمارات نحو التكنولوجيا الحديثة، واستخدام أفضل الموارد البشرية والمادية لملاحقة ومتابعة التطورات والتغيرات الحديثة والمستمرة في أساليب المراجعة الداخلية؛ فضلاً عن تعاملاته مع عدد كبير من الشركات وهو ما يزيد من الخبرة والمعرفة المهنية المتوافرة لدي الموفر الخارجي لوظيفة المراجعة الداخلية وبالتالي تحسين الكفاءة والفعالية للمهام المنجزة (محمد، ٢٠١٩).

2008 & Del Vecchio and Clinton, 2003 & Suleiman and Dandago, 2014 & Rittenberg and Covaleski, 2001 & Seetharaman et al., 2008 (& Caplan et al., 2007

وبشأن تكاليف إسناد وظيفة المراجعة الداخلية؛ هناك العديد من وجهات النظر المعارضة لقرار الإسناد الخارجي لوظائف المراجعة الداخلية لما لها من عيوب وتكاليف مرتبطة بها ومنها؛ (١) إمكانية وصول الطرف الخارجي المسند إليه وظيفة المراجعة الداخلية إلى مجموعة واسعة من المعلومات السرية غير المتاحة للجميع مما يعرضها للتسرب وبالتالي إمكانية التأثير السلبي على الاستقرار التنظيمي للمنشأة وقدراتها التنافسية (Rittenberg and Covaleski, 2001 & Suleiman and Dandago, 2014)؛ (٢) عدم التواجد المستمر لموفر الخدمة الخارجي داخل المنشأة مما يضعف من قدرة وظيفة المراجعة الداخلية على الاستجابة للاحتياجات الديناميكية الطارئة للإدارة، وافتقار الموفر الخارجي للمعرفة الكافية بعمليات وأعمال المنشأة (Schneider, 2008 & محمد، ٢٠١٩)؛ (٣) غياب البيئة التدريبية وفرص التعلم لموظفي المنشأة مقارنةً بوجود قسم لوظيفة المراجعة الداخلية يساعد في توفير كوادر مهنية لإدارة المنشأة، وتوفير فرص لاكتسابهم مزيد من المعرفة حول هياكل الرقابة الداخلية وأعمال وعمليات المنشأة (Schneider, 2008 & Del Vecchio and Clinton, 2003)؛ (٤) حصول الموفر الخارجي للخدمة على أتعاب أكبر مقابل الخدمات المقدمة في حالة احتكاره لسوق تقديم هذه الخدمات؛ فضلاً عن احتمالية انخفاض ولاء موفر الخدمة للمنشأة مقارنةً بموظفيها (Rittenberg et al., 1999)؛ (٥) في حالة الإسناد التعاوني قد ينشأ صراع بين موظفي إدارة المراجعة الداخلية وموفر الخدمة الخارجي؛ نظراً لفقدان موظفي قسم المراجعة الداخلية للأمن الوظيفي (Del Vecchio and Clinton, 2003).

وبناءاً على ما سبق؛ **يرى الباحثان** أنه على الرغم من المنافع التي يمكن الحصول عليها من الإسناد الخارجي لوظائف المراجعة الداخلية متمثلة في توفير الخبرة والمعرفة

المتخصصة بأفضل الممارسات وتوظيفها لإجراء تقييم دقيق وشامل لأنظمة الشركة وضوابطها وعملياتها، الحد من مخاطر عدم الالتزام وتدعيم برامج الحوكمة وإدارة المخاطر الشاملة للمنشأة، والاستباقية في اكتشاف المخاطر وتقديم توصيات ورؤي جديدة بشأن إجراءات الاستجابة لها والتعافي منها إن حدثت، وتقديم توصيات لتحسين العمليات وتحسين الكفاءة التشغيلية وتعزيز أمن المعلومات. إلا أن هناك مجموعة من الآثار السلبية المصاحبة لعمليات الإسناد الخارجي لوظيفة المراجعة الداخلية ومنها احتمالية عدم إلمام الموفر الخارجي بطبيعة وبيئة عمل المنشأة، واختلاف أهدافه عن أهداف المنشأة وخصوصاً في حالة الافتقار إلى قنوات أتصال فعالة بين الموفر والمنشأة. ولذلك **يرى الباحثان** أنه من الأفضل الجمع بين الإسناد الداخلي والخارجي لأداء وظيفة المراجعة الداخلية من خلال الاعتماد على استراتيجية الإسناد التعاوني مع العمل على التحديد الدقيق لواجبات ومسئوليات كل طرف، والتعاون الفعال المشترك بينهما بما يساعد على خلق بيئة عمل مستقرة قابلة للتكيف، والتواجد المستمر للمراجع الداخلي داخل المنشأة وتدنية التكاليف الأساسية لوظيفة المراجعة الداخلية، والسماح بمراقبة أداء موفري الخدمة الخارجيين الذين يتم الاستعانة بهم .

وبشأن تأثير الإسناد الخارجي لوظيفة المراجعة الداخلية على القيمة المضافة من توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني؛ فقد أوضحت دراسة Seetharaman et al (2008) أن الإسناد الخارجي لوظيفة المراجعة الداخلية يؤثر إيجابا على إدراك الأطراف أصحاب المصلحة للقيمة المضافة من وظيفة المراجعة الداخلية؛ حيث أن الإسناد الخارجي قد يؤدي إلى تدعيم استقلالية المراجع، وزيادة دقة التقارير والقوائم المالية المفصح عنها، وبالتالي زيادة جودة عملية المراجعة، فضلاً عن مساعدته في التحديد الدقيق للمخاطر المحيطية ببيئة عمل المنشأة وتقييمها والحد منها.

وفي نفس السياق؛ أوضحت دراسة Alina et al (2017) أن الإسناد الخارجي لوظيفة المراجعة الداخلية من شأنه تحسين التوجه التقني، وتوسيع نطاق الرقابة على

مخاطر الأمن السيبراني وإداراتها، وتحسين العمليات المرتبطة بها، وإضفاء مزيد من الثقة على افصاحات إدارة المخاطر بشأن إدارة المخاطر السيبرانية؛ وبالتالي التأثير الإيجابي على الأداء المالي والتشغيلي للمنشأة. كما أشارت دراسة Kahyaoglu and Caliyurt (2018) إلى أن وجود توكيد بشأن مزاعم الإدارة حول إدارة مخاطر الأمن السيبراني من قبّل طرف خارجي مستقل قائم بوظيفة المراجعة الداخلية سيزيد من ثقة الأطراف أصحاب المصلحة بشكل أكبر مقارنةً بتوفير ذلك التوكيد من المراجع الداخلي التابع لإدارة المراجعة الداخلية بالشركة وهو ما يضيف قيمة للأطراف أصحاب المصلحة.

كما استهدفت دراسة Calvin et al (2025) دراسة خصائص وظيفة المراجعة الداخلية التي تضمن تحقيق الأمن السيبراني، وذلك من خلال إجراء دراسة استقصائية على أكثر من ٣٦٠٠ ممارس مهني لوظيفة المراجعة الداخلية من ١٥٩ دولة حول العالم خلال النصف الثاني من عام ٢٠٢١ بنسبة ردود وصلت إلى ١١٤٢ رد نهائي؛ وقد توصلت الدراسة إلى أنه نظراً لحداثة الأنشطة المتعلقة بتكنولوجيا المعلومات والأمن السيبراني فقد أصبح من الضروري الاستعانة بمصادر خارجية للقيام بوظيفة المراجعة الداخلية لأن قسم المراجعة الداخلية بالمنشأة سيكون أقل احتمالاً لامتلاك المعرفة المطلوبة داخلياً لتحقيق الأمن السيبراني والتحقق منه؛ وبالتالي فإن قرار الاستعانة بمصادر خارجية للقيام بوظيفة المراجعة الداخلية من شأنه زيادة قدرة المراجع الداخلي على توفير توكيد موضوعي ودقيق بشأن تحقيق الأمن السيبراني.

وفي نفس الشأن؛ استهدفت دراسة Vuko et al (2025) تحليل العوامل المفسرة لفعالية وظيفة المراجعة الداخلية في مجال التوكيد بشأن إدارة مخاطر الأمن السيبراني؛ وذلك من خلال إجراء دراسة تجريبية على عينة دولية من المراجعين الداخليين ذات الصلة بمراجعة تكنولوجيا المعلومات؛ وقد توصلت الدراسة إلى أن الإسناد الخارجي لوظيفة المراجعة الداخلية يؤثر إيجابياً في فعالية وظيفة المراجعة الداخلية، ويساهم بشكل إيجابي في تحقيق الأمن السيبراني والحد من المخاطر

المرتبطة به، ويزيد من ثقة الأطراف أصحاب المصلحة في التوكيد المقدم من قبَل القائم بوظيفة المراجعة الداخلية بشأن إدارة مخاطر الأمن السيبراني.

وبناءاً على ما سبق؛ **خلص الباحثان** إلى أن الإسناد الخارجي لوظيفة المراجعة الداخلية من شأنه التأثير الإيجابي على جودة أداء مهام المراجعة الداخلية وخصوصاً فيما يتعلق بمجال الأمن السيبراني والمخاطر المرتبطة به؛ **ويرى الباحثان** أن معظم الدراسات السابقة قد اختبرت أثر الإسناد الخارجي لوظائف المراجعة الداخلية إما كمتغير مستقل أو كمتغير رقابي؛ وأن هناك ندرة نسبية في الكتابات التي درست واختبرت أثر الإسناد الخارجي لوظائف المراجعة الداخلية كمتغير مُعدَل للعلاقة محل الدراسة. **ويعتقد الباحثان** أن التفاعل بين الإسناد الخارجي لوظائف المراجعة الداخلية وتوكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني من شأنه ينتج متغيراً تفاعلياً جديداً يؤثر على قوة و/أو اتجاه العلاقة التأثيرية محل الفرض الأول (H1) مقارنةً بتجاهل ذلك الأثر التفاعلي؛ **وعليه يمكن اشتقاق الفرض الثاني (H2) كالتالي**:

H2: يختلف التأثير الإيجابي المعنوي لتوكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني على القيمة المضافة من وظيفة المراجعة الداخلية باختلاف تفعيل التوجه نحو الإسناد الخارجي لوظيفة المراجعة الداخلية من عدمه.

٦-٣-٢-٢- تحليل أثر خبرة ونوع الأطراف أصحاب المصالح على العلاقة محل الدراسة؛ واشتقاق الفرض الثالث والرابع.

بشأن خبرة الأطراف أصحاب المصالح؛ فيمكن القول أن زيادة الخبرة المالية لدى أعضاء لجان المراجعة قد يؤدي إلى تحسين عمليات الإشراف والرقابة على الالتزام بالقوانين واللوائح وإعداد التقارير والقوائم المالية؛ وبالتالي التأثير الإيجابي على دقتها وموضوعيتها، فضلاً عن تقديم توكيدات مستقلة دقيقة بشأن فعالية عمليات إدارة المخاطر مما يزيد من ثقة المستثمرين في المعلومات المفصح عنها من قبّل تلك المنشآت؛ ومن ثَم التأثير الإيجابي على قرارات الاستثمار من قبّل الأطراف أصحاب المصالح، وتحسين

الأداء التشغيلي والمالي للمنشأة، وتحسين حصتها السوقية، (Ojeka et al., 2014 & Festus et al., 2020 & Chukwunedu et al., 2014).

وفي نفس الشأن؛ أوضحت دراسة Gul et al (2013) أن خبرة مراقبي الحسابات قد يزيد من قدرتهم على حل المشاكل، والتحديد الدقيق لنقاط الضعف والقوة في المنشأة، وإصدار الأحكام المهنية الدقيقة وخصوصاً فيما يتعلق بتقدير مخاطر أعمال عميل المراجعة، والتقييم الفعال لجودة الممارسات والضوابط المطبقة لإدارة المخاطر بالمنشأة، والحد من السلوك الانتهازي، وزيادة جودة التقارير والقوائم المالية.

كما أن خبرة المراجع الداخلي قد تؤثر بشكل كبير على المهام والوظائف المكلف بأدائها؛ فهي تزيد من قدرته على إجراء مزيد من عمليات المراجعة الفعالة وبالتالي تحقيق الأهداف المنشودة، وبناء علاقات أعمق مع إدارة أمن نظم المعلومات والأطراف أصحاب المصلحة؛ وبالتالي التقييم الفعال للمخاطر السيبرانية، والحد من مخاطر الأمن السيبراني، وتوفير توكيد أكثر دقة بشأن ضوابط الأمن السيبراني المطبقة من قبّل إدارة الشركة، وتقديم رؤى استباقية وبرامج فعالة للحد من مخاطر الأمن السيبراني، وتوظيف قدراتهم ومهاراتهم بالشكل الكفء والفعال في فهم التأثير الكامل للتهديدات السيبرانية على المنشأة، وبالتالي الإدارة الفعالة لمخاطر الأمن السيبراني وتقديم توصيات لمجلس الإدارة ولجان المراجعة بشأن الإدارة الفعالة للمخاطر المصاحبة للأمن السيبراني، وبالتالي مساعدة مجلس الإدارة ولجان المراجعة في فهم طبيعة بيئة العمل الرقمي (Kahyaoglu and Caliyurt, 2018 & Islam et al., 2018 & Usman et al., 2024 & Johari et al., 2023 & Deloitte, 2017)

وعلى عكس نتائج الدراسات السابقة؛ فقد استهدفت دراسة الأباصيري (٢٠١٨) اختبار أثر التعديلات في شكل ومحتوى تقرير المراجع الخارجي غير المعدل على مدى إمكانية المستثمر المؤسسي على القوائم المالية للشركات المقيدة بالبورصة المصرية في ظل الدور المعدل لخبرة المستثمر المؤسسي وذلك من خلال إجراء دراسة تجريبية في بيئة الأعمال والممارسة المهنية المصرية؛ وقد توصلت الدراسة

إلى عدم وجود تأثير معنوي لخبرة المستثمر المؤسسي على العلاقة محل الدراسة في بيئة الممارسة المهنية المصرية. كما أوضحت دراسة مرسي (٢٠٢٣) عدم وجود تأثير معنوي لمستوى خبرة الأطراف أصحاب المصالح على العلاقة بين الإفصاح عن توكيد المراجع الداخلي بشأن فعالية نظام الإبلاغ عن الغش المالي والفساد على إدراك الأطراف أصحاب المصلحة لفجوة التوقعات بالمراجعة الداخلية.

وبناءاً على ما سبق؛ **خلص الباحثان** أن خبرة الأطراف أصحاب المصالح قد تؤثر إيجاباً على قدرات الأطراف أصحاب المصلحة في إدراك القيمة المضافة من توكيد المراجع الداخلي، والتقييم الفعال لسياسات وإجراءات تحقيق الأمن السيبراني وإدارة المخاطر المصاحبة لها. و**يرى الباحثان** أن معظم الدراسات السابقة قد اختبرت أثر خبرة أصحاب المصالح إما كمتغير مستقل أو كمتغير رقابي، وأن هناك ندرة في الكتابات التي درست واختبرت أثر خبرة أصحاب المصالح كمتغير مُعدّل للعلاقة محل الدراسة. **ويعتقد الباحثان** أن التفاعل بين خبرة أصحاب المصالح وتوكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني من شأنه ينتج متغيراً تفاعلياً جديداً يؤثر على قوة و/أو اتجاه العلاقة التأثيرية محل الفرض الأول (H1) مقارنةً بتجاهل ذلك الأثر التفاعلي؛ **وعليه يمكن اشتقاق الفرض الثالث (H3) كالتالي:**

H3: يختلف التأثير الإيجابي المعنوي لتوكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني على القيمة المضافة من وظيفة المراجعة الداخلية باختلاف خبرة أصحاب المصالح.

و**بشأن نوع الأطراف أصحاب المصلحة**؛ فهناك اختلافات واضحة بين الإناث والذكور من حيث المعرفة، والقدرة على حل المشاكل، والقدرة على تحمل المخاطر، والقيام بممارسات انتهازية، والمشاركة في صفقات تجارية جدية (Gul et al., 2013). وفي هذا الشأن؛ يمكن القول أن وجود عنصر نسائي ضمن لجان المراجعة سيزيد من عمليات الرقابة على أداء المنشأة، وزيادة عمليات المتابعة والإشراف على عمليات تعيين مراقبي الحسابات وتحديد مكافآتهم، مما يزيد من جودة التقارير والقوائم

المالية المفصح عنها (Chukwunedu et al., 2014). كما أن وجود عنصر نسائي ضمن فريق مجلس الإدارة سيزيد من درجة الالتزام بالقوانين واللوائح، والحد من عدم تماثل المعلومات لكون العنصر النسائي أكثر تحفظاً وأقل ميلاً للمخاطرة مقارنةً بالذكور؛ وهو ما يزيد من اهتمامهم بتحديد وتقييم المخاطر والحد منها، وتوجيه المزيد من الاستثمارات نحو أنشطة المسئولية البيئية والاجتماعية للشركات، وهو ما يساعد على حماية سمعة المنشأة، وتحسين الأداء المالي والتشغيلي للمنشأة، وزيادة القيمة السوقية للمنشأة (Bear et al., 2010 & Fellner and Maciejovsky, 2007 & Huang et al., 2014).

وفي نفس الصدد؛ يمكن القول أن وجود عنصر نسائي ضمن فريق مراقب الحسابات من شأنه زيادة درجة الالتزام بالمعايير الأخلاقية وبالتالي زيادة جودة عملية المراجعة، وزيادة جودة التقارير والقوائم المالية المفصح عنها، ورفع كفاءة السوق؛ حيث سيعي الإناث إلى بذل المزيد من الجهد والعناية المهنية عند القيام بمهام المراجعة مقارنةً بالذكور؛ وذلك بهدف تحقيق الأمن الوظيفي، وتجنب المخاطرة والتقاضي والتكاليف المصاحبة لها (Mnif and Cherif, 2022 & Gul et al., 2013).

وعلى عكس نتائج الدراسات السابقة؛ أوضحت دراسة مرسي (٢٠٢٣) عدم وجود تأثير معنوي لنوع جنس الأطراف أصحاب المصالح على العلاقة بين الإفصاح عن توكيد المراجع الداخلي بشأن فعالية نظام الإبلاغ عن الغش المالي والفساد على إدراك الأطراف أصحاب المصلحة لفجوة التوقعات بالمراجعة الداخلية.

وبناءاً على ما سبق؛ **خلص الباحثان** إلى احتمالية وجود فجوة كبيرة بين الأطراف أصحاب المصلحة من الإناث والذكور؛ وبالتالي يمكن القول أن نوع الأطراف أصحاب المصلحة قد يؤثر على قدرات الأطراف أصحاب المصلحة في إدراك القيمة المضافة من توكيد المراجع الداخلي، والتقييم الفعال لسياسات وإجراءات تحقيق الأمن السيبراني وإدارة المخاطر المصاحبة لها. **ويرى الباحثان** أن معظم الدراسات السابقة قد اختبرت أثر نوع أصحاب المصالح إما كمتغير مستقل أو كمتغير رقابي، وأن هناك ندرة في الكتابات

التي درست واختبرت أثر نوع أصحاب المصالح كمتغير مُعدّل للعلاقة محل الدراسة. **ويعتقد الباحثان** أن التفاعل بين نوع أصحاب المصالح وتوكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني من شأنه ينتج متغيراً تفاعلياً جديداً يؤثر على قوة و/أو اتجاه العلاقة التأثيرية محل الفرض الأول (H1) مقارنةً بتجاهل ذلك الأثر التفاعلي؛ **وعليه يمكن اشتقاق الفرض الرابع (H4) كالتالي**:

H4: يختلف التأثير الإيجابي المعنوي لتوكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني على القيمة المضافة من وظيفة المراجعة الداخلية باختلاف نوع أصحاب المصالح.

٦-٤- منهجية البحث:

تحقيقاً لهدف البحث؛ ومن ثَم اختبار فروضه تجريبياً؛ يستهدف هذا القسم عرض منهجية البحث وذلك من خلال تناول كل من؛ أهداف الدراسة التجريبية، مجتمع وعينة الدراسة، توصيف وقياس متغيرات الدراسة، نموذج البحث، أدوات وإجراءات الدراسة التجريبية، التصميم التجريبي المستخدم والمعالجات والمقارنات التجريبية، أدوات التحليل الإحصائي المستخدمة في تحليل البيانات، وذلك وصولاً لاختبار فروض البحث. كما يتضمن البحث القيام ببعض التحليلات الأخرى بغرض إضفاء مزيد من الوضوح والفهم على العلاقات محل الدراسة بالتحليل الأساسي، وللتعرف ايضاً على مدى متانة نتائج التحليل الأساسي؛ وذلك على النحو التالي (Islam et al., 2018 & Slapnicar et al., 2022):

٦-٤-١- أهداف الدراسة التجريبية:

تستهدف الدراسة التجريبية اختبار فروض البحث في بيئة الممارسة المهنية المصرية؛ والتوصل إلى دليل تجريبي بشأن القيمة المضافة من توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني، والأثر المُعدّل لكل

من الإسناد الخارجي لوظيفة المراجعة الداخلية، وخبرة ونوع الأطراف أصحاب المصالح –كمتغيرات مُعدّلة[١]- على هذه القيمة المضافة.

٦-٤-٢- مجتمع وعينة الدراسة:

يتكون مجتمع الدراسة من كافة الأطراف أصحاب المصالح الرئيسين المستفيدين من وظيفة المراجعة الداخلية (ممثل لجانب الطلب على وظيفة المراجعة الداخلية) سواء كانت **الأطراف أصحاب المصالح داخليين** مثل: أعضاء مجالس الإدارة، وأعضاء لجان المراجعة؛ أو **الأطراف أصحاب المصالح خارجيين** مثل: إدارة منح الائتمان وإدارة أمناء الاستثمار بالبنوك، وشركات السمسرة، والمستثمرين، والمحللين الماليين، ومراقبي حسابات، وذلك قياساً على (Johari et al., 2023 & Islam et al., 2018 & مرسي، ٢٠٢٣ & يوسف، ٢٠٢٤ & أميرهم، ٢٠٢٢).

وتتمثل عينة الدراسة في (٧٦) استجابة[٢]؛ (٩) من أعضاء مجالس إدارة الشركات، (٤) من اعضاء لجان المراجعة، (٣٢) من أعضاء إدارة منح الائتمان بالبنوك، (٧) من أعضاء إدارة أمناء الاستثمار بالبنوك، (٤) محلل مالي، (١) موظفاً بشركات السمسرة، (١٩) مراقب حسابات خارجي.

[١] **المتغيرات المُعدّلة للعلاقة (Moderating Variables)**هي تلك المتغيرات التي قد تؤثر على اتجاه و/أو قوة العلاقة بين المتغيرات المستقلة والمتغيرات التابعة؛ حيث تعتبر بمثابة محفزات للعلاقة بين المتغير التابع والمتغير المستقل، ويشتق المتغير المُعدّل اعتماداً على الدراسات السابقة، ويعتبر جزء مطلوباً من الدراسة البحثية بالإضافة إلى كونه جزء أساسي من فروض البحث. وهي تختلف عن **المتغيرات الرقابية Control Variables** وهي تلك المتغيرات التي تؤثر مباشرة على المتغير التابع ولكن طبيعة هذا التأثير غير محددة نسبياً؛ ولا يعتبر هذا المتغير جزءاً أساسياً من الدراسة البحثية. في حين أن كلا النوعين من المتغيرين يختلفا عن **المتغيرات الوسيطة Mediator Variables** وهي تلك المتغيرات التي تتوسط العلاقة بين المتغيرات المستقلة والتابعة؛ وتقوم بنقل تأثير المتغيرات المستقلة إلى المتغير التابع (موسى، ٢٠١٨ & الصيرفي، ٢٠٢٥).

[٢] تم إرسال الحالات التجريبية لمفردات العينة إما باستخدام مواقع التواصل الاجتماعي بالاعتماد على تقنية Google Form؛ أو من خلال التواصل المباشر والتسليم اليدوي للحالات التجريبية؛ وقد استلم الباحثان عدد (٧٧) استجابة؛ وقد تم استبعاد عدد (٦) استجابات لعدم اكتمالها في الرد على جميع الأسئلة المتعلقة بالحالات التجريبية الأربعة المرفقة لديهم. وبالتالي بلغت نسبة الردود الصحيحة إلى إجمالي الردود المستلمة (٩٢.٢%).

ويمكن توضيح الإحصاء الوصفي لعينات الدراسة من خلال الجدول التالي (٦-١) كما يلي:

جدول (٦-١)
الإحصاء الوصفي لعينة الدراسة

البيان	عضو مجلس إدارة	عضو لجنة مراجعة	إدارة منح الائتمان بالبنوك	إدارة أمناء الاستثمار بالبنوك	محلل مالي	شركات سمسرة	مراقب حسابات خارجي	الإجمالي
عدد مفردات العينة	9	4	32	7	4	1	19	76
نسبة عدد مفردات العينة إلى الإجمالي	11.8%	5.3%	42.1%	9.2%	5.3%	1.3%	25%	100%
عدد المفردات من حيث الخبرات العملية								
مرتفع الخبرة	9	4	19	4	3	0	14	53
منخفض الخبرة	0	0	13	3	1	1	5	23
نسبة الخبرات العملية								
مرتفع الخبرة	100%	100%	59.38%	57.1%	75%	0%	73.7%	69.7%
منخفض الخبرة	0%	0%	40.63%	42.9%	25%	100%	26.3%	30.3%
عدد المفردات من حيث النوع								
ذكر	7	4	14	4	4	1	13	47
أنثى	2	0	18	3	0	0	6	29
نسبة النوع								
ذكر	77.8%	100%	43.75%	57.1%	100%	100%	68.4%	61.8%
أنثى	22.2%	0%	56.25%	42.9%	0%	0%	31.6%	38.2%

(المصدر: إعداد الباحثان)

ويتضح من الجدول السابق؛ أن النسبة الأكبر من المشاركين كانت من الأفراد ذوي الخبرة المرتفعة ممن يمتلكون خبرة تزيد عن (١٠) عاماً بنسبة مشاركة (69.7%) مقارنةً بنسبة المشاركة من ذوي الخبرة المنخفضة ممن يمتلكون خبرة أقل من (١٠) سنوات والتي تبلغ (30.3%) من إجمالي عينة الدراسة. كما يتضح أن النسبة الأكبر من المشاركين كانت من الذكور بنسبة مشاركة (61.8%) مقارنةً بنسبة مشاركة الإناث والتي تبلغ (38.2%) من إجمالي عينة الدراسة.

٦-٤-٣- توصيف وقياس متغيرات الدراسة:

تشمل متغيرات الدراسة في ظل التحليل الأساسي على متغير مستقل واحد، ومتغير تابع، وثلاثة متغيرات مُعدّلة للعلاقة. وتم توصيف المتغيرات وقياسها كما يتضح من الجدول التالي:

٦-٤-٣-١- المتغير المستقل: توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني:

ويقصد به إضفاء الصدق على التقارير المعدة من قبَل المسئولون عن عمليات إدارة المخاطر والمقدمة إلى إدارة الشركة ولجان المراجعة بشأن إدارة مخاطر الأمن السيبراني، وتقييم مدى فعالية العمليات المستخدمة في تحديد مخاطر الأمن السيبراني وإدارتها، ومدى فعالية تصميم وتشغيل عمليات إدارة المخاطر السيبرانية (Elmaasrawy and Tawfik, 2025 & Babiker, 2025 & Johari et al., 2023).؛ وتم قياس هذا المتغير من خلال إمداد مفردات العينة بمعلومات عن حالة لشركة ليس لديها توكيد من قبّل القائم بوظيفة المراجعة الداخلية بشأن إدارة مخاطر الأمن السيبراني (الحالة التجريبية الأولي والثالثة)؛ وحالة لنفس الشركة ولكن لديها توكيد من قبّل القائم بوظيفة المراجعة الداخلية بشأن إدارة مخاطر الأمن السيبراني (الحالة التجريبية الثانية والرابعة) والمقارنة بين الردود بشأن القيمة المضافة من وظيفة المراجعة الداخلية؛ قياساً على (يوسف، ٢٠٢٤).

٦-٤-٣-٢- المتغير التابع: القيمة المضافة من توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني:

ويقصد به عملية تنفيذ وتشغيل الأساليب الرقابية، وأنشطة المخاطر الأخرى بغرض حماية التقارير والقوائم المالية، وتحسين الأداء التشغيلي للمنشأة، وزيادة درجة الالتزام بالقوانين واللوائح، وزيادة القدرات التنافسية للشركة ومن ثُم تحسين سمعة الشركة (يوسف، ٢٠٢٤)؛ ويعتبر قياس القيمة المضافة من الوظائف الإنتاجية

من الأمور السهلة والمباشرة؛ إلا أن قياس القيمة المضافة من الوظائف الخدمية كوظيفة المراجعة الداخلية من الأمور الصعبة وغير المباشرة نظرا لقياسه بمؤشرات تقريبية يستدل منها على القيمة المضافة؛ ولذلك تقاس القيمة المضافة من وظيفة المراجعة الداخلية بمقدار انعكاس وظيفة المراجعة الداخلية كأداة للرقابة الداخلية على فعالية الرقابة الداخلية وسمعة الشركة (Koutoupis and Kampouris, 2021 & Inyang et al., 2021 & Awinbugri and Daniel., 2019 & Seetharaman et al., 2008)؛ وقد تم قياس هذا المتغير من خلال الاعتماد على ردود مفردات العينة على مقياس ليكرت من صفر حتى (١٠) بشأن؛ قياساً على (Serag and Daoud, 2021):

- مدى صدق التقارير والقوائم المالية المفصح عنها كمقياس لفاعلية الرقابة الداخلية.
- مدى الالتزام بالقوانين واللوائح المطبقة داخل المنشأة كمقياس لفاعلية الرقابة الداخلية.
- مدى التحسن في الأداء التشغيلي للمنشأة كمقياس لفاعلية الرقابة الداخلية.
- مدى التحسن في الحصة السوقية للمنشأة كمقياس لسمعة المنشأة.

على أن يتم تجميع تلك الردود لكل مفردة وقسمتها على (٤) للحصول على مؤشر يمكن من خلاله قياس القيمة المضافة من توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني؛ وبذلك تتراوح قيمة المؤشر لكل مفردة ما بين (صفر) إلى (١٠)؛ وتشير الدرجة الأعلى إلى زيادة القيمة المضافة من توكيد المراجع الداخلي بشأن إدارة مخاطر الأمن السيبراني.

٦-٤-٣-٣- المتغيرات المعدلة:

٦-٤-٣-٣-١- الإسناد الخارجي لوظيفة المراجعة الداخلية:

يقصد به قرار من قبّل إدارة الشركة بتعهيد أداء كل وظائف المراجعة الداخلية المتعلقة بالشركة والتي كان يجب أداؤها داخل الشركة إلى أطراف خارجية بناءاً على تحليل العلاقة بين التكاليف والمنافع المنظورة وغير المنظورة للقرار (محمد، ٢٠١٩)؛

وقد تم قياس هذا المتغير من خلال إمداد مفردات العينة بمعلومات عن حالة لشركة لديها إدارة للمراجعة داخلية وبالتالي يتم أداء وظائف المراجعة الداخلية من خلال أفراد داخل المنشأة (الحالة التجريبية الأولي والثانية)؛ وحالة لنفس الشركة ولكنها لا تمتلك إدارة للمراجعة الداخلية ولذلك فهي تقوم بإسناد وظيفة المراجعة الداخلية لطرف خارجي (الحالة التجريبية الثالثة والرابعة) قياساً على (Vuko et al., 2025 & Calvin et al., 2025).

٦-٤-٣-٣-٢- خبرة الأطراف أصحاب المصلحة:

يقصد به المخزون المعرفي العملي عن ممارسة العمل المهني للأطراف أصحاب المصلحة؛ وقد تم قياس هذا المتغير من خلال متغير وهمي يأخذ القيمة (صفر) إذا كانت الأطراف أصحاب المصلحة لديها خبرة أقل من ١٠ سنوات؛ ويأخذ القيمة (١) إذا كانت الأطراف أصحاب المصلحة لديها خبرة أكبر من أو يساوي عشر سنوات وذلك قياساً على (Chukwunedu et al., 2014 & مرسي، ٢٠٢٣).

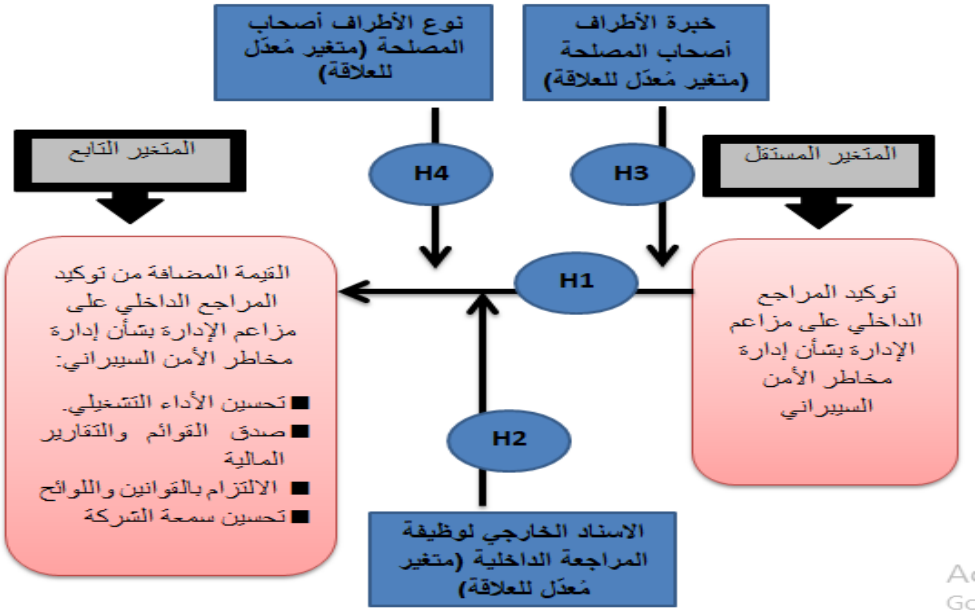
٦-٤-٣-٣-٣- نوع جنس الأطراف أصحاب المصلحة:

يقصد به نوع جنس الأطراف أصحاب المصلحة سواء كان ذكر أو أنثي؛ وقد تم قياس هذا المتغير من خلال متغير وهمي يأخذ القيمة (صفر) إذا كانت الأطراف أصحاب المصلحة أنثي؛ ويأخذ القيمة (١) إذا كانت الأطراف أصحاب المصلحة ذكر وذلك قياساً على (Fellner and Maciejovsky, 2007).

٦-٤-٤- نموذج البحث:

بناءاً على فروض البحث، ومتغيرات الدراسة، يمكن صياغة نموذج البحث في ظل التحليل الأساسي من خلال الشكل (١) كما يلي:

يظهر الشكل رقم (١) التالي نموذج البحث في ظل التحليل الأساسي:



(المصدر: إعداد الباحثان)

٦-٤-٥- أدوات وإجراءات الدراسة التجريبية:

تشتمل أدوات الدراسة التجريبية على تصميم وتقديم مجموعة من الحالات التجريبية الافتراضية (ملحق رقم ١) لمنشأة مقيدة بالبورصة المصرية وتعمل في مجال الاتصالات وتكنولوجيا المعلومات؛ والمقترنة بمجموعة من الأسئلة المرافقة لها. وعرضها على مفردات العينة، وإجراء المقابلات الشخصية مع بعض أفراد العينة؛ فضلاً عن استخدام نموذج Google Form لإرسال الحالات التجريبية لأفراد العينة. كما تم استخدام البرنامج الإحصائي SPSS لإجراء الاختبارات الإحصائية اللازمة لاختبار فروض البحث.

وبشأن إجراءات الدراسة التجريبية؛ فقد اشتملت الحالات التجريبية على ما يلي:

- **القسم الأول: البيانات الشخصية لمفردات العينة**: ويهدف هذا القسم الحصول على بعض البيانات الأساسية عن مفردات عينة الدراسة؛ والمتمثلة في الاسم، والنوع، والوظيفة الحالية، وطبيعة العمل، والمؤهلات الدراسية التي تم الحصول عليها، وكذلك عدد سنوات الخبرة في مجال العمل؛ وذلك بهدف قياس بعض الخصائص الديموغرافية لمفردات العينة.
- **القسم الثاني: المصطلحات الفنية ذات الصلة بموضوع البحث:** ويشمل هذا القسم على مجموعة من المصطلحات الفنية ذات الصلة بموضوع الدراسة، والتي قد يصعب على بعض مفردات العينة التعامل معها وفهمها وإدراك المراد منها بسهولة.
- **القسم الثالث: الحالات التجريبية:** ويحتوي هذا القسم على الحالات الافتراضية، والتي تتضمن على أربعة حالات تجريبية؛ **فبشأن الحالة التجريبية الأولي** فهي تتضمن وجود إدارة مراجعة داخلية بالمنشأة، مع عدم وجود تقرير من قبّل المراجع الداخلي بالتوكيد على مزاعم الإدارة عن إدارة مخاطر الأمن السيبراني؛ في حين أن **الحالة التجريبية الثانية** تتضمن وجود إدارة مراجعة داخلية بالمنشأة، مع وجود تقرير من قبّل المراجع الداخلي بالتوكيد على مزاعم الإدارة عن إدارة مخاطر الأمن السيبراني. أما بخصوص **الحالة التجريبية الثالثة** فهي تتضمن عدم وجود إدارة للمراجعة الداخلية بالمنشأة، ولذلك فهي تقوم بالإسناد الخارجي لوظيفة المراجعة الداخلية، مع عدم وجود تقرير من قبّل القائم بوظيفة المراجع الداخلي بالتوكيد على مزاعم الإدارة عن إدارة مخاطر الأمن السيبراني. أما فيما يتعلق **بالحالة التجريبية الرابعة** فهي تتضمن عدم وجود إدارة للمراجعة الداخلية بالمنشأة، ولذلك فهي تقوم بالإسناد الخارجي لوظيفة المراجعة الداخلية، مع وجود تقرير من قبّل القائم بوظيفة المراجع الداخلي بالتوكيد على مزاعم الإدارة عن إدارة مخاطر الأمن السيبراني. وفي جميع الحالات التجريبية الأربعة السابقة تم الطلب من مفردات العينة الإجابة على بعض الاسئلة المتعلقة بقياس القيمة

المضافة من توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني.

٦-٤-٦- التصميم التجريبي المستخدم والمعالجات والمقارنات التجريبية:

لاختبار فروض البحث؛ تم الاعتماد على تصميماً تجريبياً (٢×٣×٢) وذلك على النحو المبين بالجدول (٦-٢) كما يلي:

جدول (٦-٢)
التصميم التجريبي (٢×٣×٢)

محددات القيمة المضافة / بدائل التوكيد	طبيعة الإسناد		خبرة الأطراف أصحاب المصالح		نوع جنس الأطراف أصحاب المصالح	
	إسناد داخلي	إسناد خارجي	أقل من ١٠ سنوات (منخفضة)	أكثر من ١٠ سنوات (مرتفعة)	ذكر	أنثى
عدم التوكيد على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني	(١) أ-الأداء التشغيلي ب-صدق القوائم المالية ج-الالتزام بالقوانين واللوائح د- سمعة الشركة	(٢) أ-الأداء التشغيلي ب-صدق القوائم المالية ج-الالتزام بالقوانين واللوائح د- سمعة الشركة	(٣) أ-الأداء التشغيلي ب-صدق القوائم المالية ج-الالتزام بالقوانين واللوائح د- سمعة الشركة	(٤) أ-الأداء التشغيلي ب-صدق القوائم المالية ج-الالتزام بالقوانين واللوائح د- سمعة الشركة	(٥) أ-الأداء التشغيلي ب-صدق القوائم المالية ج-الالتزام بالقوانين واللوائح د- سمعة الشركة	(٦) أ-الأداء التشغيلي ب-صدق القوائم المالية ج-الالتزام بالقوانين واللوائح د- سمعة الشركة
التوكيد على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني	(٧) أ-الأداء التشغيلي ب-صدق القوائم المالية ج-الالتزام بالقوانين واللوائح د- سمعة الشركة	(٨) أ-الأداء التشغيلي ب-صدق القوائم المالية ج-الالتزام بالقوانين واللوائح د- سمعة الشركة	(٩) أ-الأداء التشغيلي ب-صدق القوائم المالية ج-الالتزام بالقوانين واللوائح د- سمعة الشركة	(١٠) أ-الأداء التشغيلي ب-صدق القوائم المالية ج-الالتزام بالقوانين واللوائح د- سمعة الشركة	(١١) أ-الأداء التشغيلي ب-صدق القوائم المالية ج-الالتزام بالقوانين واللوائح د- سمعة الشركة	(١٢) أ-الأداء التشغيلي ب-صدق القوائم المالية ج-الالتزام بالقوانين واللوائح د- سمعة الشركة

(المصدر: إعداد الباحثان)

ووفقاً لما سبق؛ يظهر عدد (١٢) معالجة تجريبية وهي على النحو التالي:

المعالجة رقم (١): عدم وجود توكيد من قبّل القائم بوظيفة المراجعة الداخلية على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني / وجود إدارة للمراجعة الداخلية بالمنشأة (الإسناد الداخلي لوظيفة المراجعة الداخلية) / إدراك الأطراف أصحاب المصلحة للقيمة المضافة من توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني.

المعالجة رقم (٢): عدم وجود توكيد من قبّل القائم بوظيفة المراجعة الداخلية على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني / عدم وجود إدارة للمراجعة الداخلية بالمنشأة (الإسناد الخارجي لوظيفة المراجعة الداخلية بالكامل) / إدراك الأطراف أصحاب المصلحة للقيمة المضافة من توكيد القائم بوظيفة المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني.

المعالجة رقم (٣): عدم وجود توكيد من قبّل القائم بوظيفة المراجعة الداخلية على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني / انخفاض مستوى خبرة الأطراف أصحاب المصلحة / إدراك الأطراف أصحاب المصلحة للقيمة المضافة من توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني.

المعالجة رقم (٤): عدم وجود توكيد من قبّل القائم بوظيفة المراجعة الداخلية على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني / ارتفاع مستوى خبرة الأطراف أصحاب المصلحة / إدراك الأطراف أصحاب المصلحة للقيمة المضافة من توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني.

المعالجة رقم (٥): عدم وجود توكيد من قبّل القائم بوظيفة المراجعة الداخلية على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني / صاحب المصلحة ذكر /

إدراك الأطراف أصحاب المصلحة للقيمة المضافة من توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني.

المعالجة رقم (٦): عدم وجود توكيد من قبّل القائم بوظيفة المراجعة الداخلية على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني / صاحب المصلحة أنثى / إدراك الأطراف أصحاب المصلحة للقيمة المضافة من توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني.

المعالجة رقم (٧): وجود توكيد من قبّل القائم بوظيفة المراجعة الداخلية على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني / وجود إدارة للمراجعة الداخلية بالمنشأة (الإسناد الداخلي لوظيفة المراجعة الداخلية) / إدراك الأطراف أصحاب المصلحة للقيمة المضافة من توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني

المعالجة رقم (٨): وجود توكيد من قبّل القائم بوظيفة المراجعة الداخلية على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني / عدم وجود إدارة للمراجعة الداخلية بالمنشأة (الإسناد الخارجي لوظيفة المراجعة الداخلية بالكامل) / إدراك الأطراف أصحاب المصلحة للقيمة المضافة من توكيد القائم بوظيفة المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني.

المعالجة رقم (٩): وجود توكيد من قبّل القائم بوظيفة المراجعة الداخلية على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني / انخفاض مستوى خبرة الأطراف أصحاب المصلحة / إدراك الأطراف أصحاب المصلحة للقيمة المضافة من توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني.

المعالجة رقم (١٠): وجود توكيد من قبّل القائم بوظيفة المراجعة الداخلية على مزاعم إدارة المخاطر بشأن إدارة مخاطر الأمن السيبراني / ارتفاع مستوى خبرة الأطراف أصحاب المصلحة / إدراك الأطراف أصحاب المصلحة للقيمة المضافة

من توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني.

المعالجة رقم (١١): وجود توكيد من قبّل القائم بوظيفة المراجعة الداخلية على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني / صاحب المصلحة ذكر / إدراك الأطراف أصحاب المصلحة للقيمة المضافة من توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني.

المعالجة رقم (١٢): وجود توكيد من قبّل القائم بوظيفة المراجعة الداخلية على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني / صاحب المصلحة أنثى / إدراك الأطراف أصحاب المصلحة للقيمة المضافة من توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني.

ولاختبار فروض البحث؛ تم إجراء مجموعة من المقارنات بين نتائج المعالجات لاختبار القيمة المضافة من توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني، وتأثير إختلاف طبيعة إسناد وظائف المراجعة الداخلية، ونوع ومستوى خبرة الأطراف أصحاب المصلحة على هذه القيمة المضافة؛ وتتمثل تلك المقارنات في الآتي:

المقارنة الأولى: [(١) + (٢) + (٣) + (٤) + (٥) +(٦)] * [(٧) + (٨) + (٩) + (١٠) + (١١) +(١٢)]؛ وذلك لاختبار أثر توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني على القيمة المضافة من وظيفة المراجعة الداخلية؛ **ومن ثُم اختبار الفرض الأول (H1).**

المقارنة الثانية: [(٢) * (٨)] * [(١) * (٧)]؛ وذلك لاختبار أثر الإسناد الخارجي لوظيفة المراجعة الداخلية من عدمه على العلاقة محل الدراسة؛ **ومن ثُم اختبار الفرض الثاني (H2).**

المقارنة الثالثة: [(٤) * (١٠)] * [(٣) * (٩)]؛ وذلك لاختبار أثر خبرة الأطراف أصحاب المصلحة من عدمها على العلاقة محل الدراسة؛ **ومن ثُم اختبار الفرض الثالث (H3).**

المقارنة الرابعة: [(٦) * (١٢)] * [(٥) * (١١)]؛ وذلك لاختبار أثر نوع الأطراف أصحاب المصلحة سواء كان ذكر أو أنثى على العلاقة محل الدراسة؛ **ومن ثُم اختبار الفرض الرابع (H4).**

٦-٤-٧- الاختبارات الاحصائية المستخدمة في اختبار فروض البحث:

اعتمد الباحثان على عدد من الأساليب الإحصائية المختلفة لتحليل البيانات التي تم التوصّل إليها؛ وقد قام الباحثان باستخدام الجداول الإلكترونية الخاصة ببرنامج Microsoft Excel بغرض إدخال ردود وإجابات المشاركين في الدراسة التجريبية، بالإضافة إلى استخدام الحزمة الإحصائية للعلوم الاجتماعية IBM SPSS الإصدار رقم (26)، وفيما يلي استعراض للأساليب والاختبارات الإحصائية المستخدمة كما يلي:

٦-٤-٧-١- اختبار الثبات (الاعتمادية) (Reliability Test):

تم استخدام مقياس Cronbach´s Alpha لقياس مدى ثبات الأسئلة المرافقة للحالات التجريبية، واختبار مدى الموثوقية في استجابات مفردات العينة على الأسئلة المقدمة لهم، وتحديد مدى إمكانية تعميم النتائج المتوصل إليها من عينة الدراسة على مجتمع الدراسة ككل؛ ويُعبر الثبات عن الحصول على نفس النتائج باحتمال مساوي لنفس قيمة المعامل عند تكرار استخدام نفس المقياس على نفس حجم العينة المُشتقة من نفس مجتمع الدراسة. وتتراوح قيمة هذا المقياس بين (0) و(1)؛ فإذا كانت قيمة هذا المعامل مساوية لـ (0) فهذا يعني عدم وجود ثبات في البيانات؛ أما إذا كانت قيمة هذا المعامل مساوية لـ (1) فهذا يعني وجود ثبات تام في البيانات؛ ويعتبر قيمة هذا المعامل مقبولة إذا تعدت قيمة الـ (٦٠%) وهو ما قد يشير إلى إمكانية الاعتماد على

نتائج الدراسة وتعميمها على مجتمع الدراسة (الصيرفي، ٢٠٢٥ & يوسف، ٢٠٢٤). ويوضح الجدول التالي (جدول ٦-٤) نتيجة معامل Cronbach´s Alpha والذي يبلغ قيمته (0.989)؛ وهو ما يشير إلى أن الحالات التجريبية والأسئلة المرافقة لها تتمتع بدرجة عالية من الثبات؛ فضلاً عن إمكانية الاعتماد على استجابات مفردات العينة على الأسئلة المقدمة لهم.

جدول (٦-٣)

نتائج اختبار Cronbach´s Alpha

Cronbach´s Alpha	N of Item
0.989	4

(المصدر: إعداد الباحثان)

٦-٤-٧-٢- اختبار التحليل العاملي (Factor Analysis):

يهدف التحليل العاملي إلى تلخيص عدد البيانات والمتغيرات المتعلقة بظاهرة معينة إلى أقل عدد يمكن من خلاله تفسير الظاهرة محل الدراسة؛ ومن ضمن اختبارات التحليل العاملي ما يعرف باختبار KMO (Kaiser-Meyer-Olkin)؛ حيث يستخدم اختبار KMO لتحديد ما إذا كان حجم عينة الدارسة مناسباً وكافياً أم لا؟؛ ويعتبر حجم العينة مقبولاً إذا تجاوز قيمة اختبار KMO قيمة الـ (50%)؛ وإذا كانت القيمة الاحتمالية P-Value أقل من (5%) (محمد، ٢٠١٩ & الصيرفي، ٢٠٢٥). وقد أظهرت نتائج التحليل الإحصائي (جدول ٦-٤) قيمة اختبار KMO كما يلي:

جدول (٦-٤)

نتائج اختبار Factor Analysis

Kaiser–Meyer–Olkin Measure of Sampling Adequacy		0.882
Bartlett`s Test of	Approx. Chi-Square	2503.133

Sphericity	df	6
	Sig.	0.000

(المصدر: إعداد الباحثان)

ويتضح من الجدول السابق أن قيمة معامل KMO للعينة يبلغ (0.882) وهو ما يتجاوز قيمة (50%)؛ كمان أن قيمة P-Value أقل من (5%)؛ وهذا يدل على ملاءمة وكفاية حجم العينة لاختبار العلاقات محل الدراسة.

٦-٤-٧-٣- اختبار الاعتدالية (Test of Normality):

يتم استخدام اختبار الاعتدالية لتحديد نوع توزيع المجتمع الذي سُحبت منه عينة الدراسة؛ وذلك بهدف تحديد ما إذا كان مجتمع الدراسة يتبع التوزيع الطبيعي المعتدل أم التوزيع غير الطبيعي غير المعتدل؟؛ وهو ما يساعد في تحديد ما إذا كان سيتم استخدام الاختبارات المعلميةParametric Tests أم الاختبارات اللامعلمية Non Parametric Tests؟. وقد تم استخدام اختبار Kolomgrov-Smirrnov، واختبار Shapiro-Wilk لمعرفة ما إذا كان التوزيع الاحتمالي للمجتمع الذي سُحبت منه العينة يتبع التوزيع الطبيعي أم التوزيع غير الطبيعي (الصيرفي، ٢٠٢٥)، ويمكن صياغة الفرض الإحصائي لهذه الاختبار كما يلي:

فرض العدم (H0): تم سحب عينة الدراسة من مجتمع يتبع توزيع طبيعي معتدل.

الفرض البديل (H1): تم سحب عينة الدراسة من مجتمع لا يتبع توزيع طبيعي معتدل.

وبتطبيق مستوى الثقة (95%) ودرجة خطأ (5%)؛ فإنه إذا كانت قيمة الاحتمالية P-Value أكبر من أو يساوي (5%) يتم قبول فرض العدم ورفض الفرض البديل؛ وهو ما يشير إلى أن مجتمع الدراسة يتبع التوزيع طبيعي معتدل؛ بينما إذا كانت قيمة P-Value أقل من (٥%) يتم قبول الفرض البديل ورفض فرض العدم وهو ما يشير إلى أن مجتمع الدراسة لا يتبع التوزيع طبيعي معتدل.

وفي هذا الشأن؛ يوضح الجدول (٦-٥) نتائج اختبار الاعتدالية؛ وقد أوضحت نتائج التحليل الإحصائي أنه وفقا لاختباري Kolomgrov-Smirrnov أو Shapiro-Wilk كانت القيمة الاحتمالية P-Value لكل سؤال من الأسئلة في أي حالة من الحالات التجريبية الأربع أقل من (5%)؛ وهو ما يشير إلى **رفض فرض العدم وقبول الفرض البديل؛** بما يعني عدم إتباع المجتمع الذي سُحبت منه عينة الدراسة للتوزيع الطبيعي المعتدل. ولذلك سيتم اللجوء إلى الاعتماد على الاختبارات اللامعلمية Non Parametric Tests لأغراض إجراء التحليل الإحصائي الخاص باختبار فروض البحث.

جدول (٦-٥)

نتائج اختبار Test of Normality

	Kolmogorov - Smirnov			Shapiro - Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Q1 – Case1	0.197	76	0.000	0.899	76	0.000
Q2 – Case1	0.292	76	0.000	0.844	76	0.000
Q3 – Case1	0.230	76	0.000	0.901	76	0.000
Q4 – Case1	0.309	76	0.000	0.852	76	0.000
Q1 – Case2	0.230	76	0.000	0.885	76	0.000
Q2 – Case2	0.207	76	0.000	0.899	76	0.000
Q3 – Case2	0.182	76	0.000	0.936	76	0.000
Q4 – Case2	0.187	76	0.000	0.929	76	0.000
Q1 – Case3	0.148	76	0.000	0.955	76	0.000
Q2 – Case3	0.190	76	0.000	0.935	76	0.000
Q3 – Case3	0.148	76	0.000	0.951	76	0.000
Q4 – Case3	0.131	76	0.000	0.950	76	0.000
Q1 – Case4	0.215	76	0.000	0.865	76	0.000
Q2 – Case4	0.179	76	0.000	0.883	76	0.000
Q3 – Case4	0.190	76	0.000	0.886	76	0.000
Q4 – Case4	0.184	76	0.000	0.886	76	0.000

(المصدر: إعداد الباحثان)

٦-٤-٨- نتائج اختبار فروض البحث:

فيما يلي يعرض الباحثان لنتائج اختبار فروض البحث الرئيسية كلاً على حدى كما يلي:

٦-٤-٨-١- نتائج اختبار الفرض الأول (H1):

استهدف **الفرض الأول (H1)** اختبار أثر توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني على القيمة المضافة من وظيفة المراجعة الداخلية؛ وقد استخدم الباحثان اختبار Wilcoxon Signed Rank Test اللامعلمي للعينتين غير المستقلتين[١]؛ وقد تم إعادة صياغة الفرض الأول (H1) في صورة فرض عدم وفرض بديل كما يلي:

فرض العدم : H0 : (M1+M3) = (M2+M4): لا يؤثر توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني إيجاباً ومعنوياً على القيمة المضافة من وظيفة المراجعة الداخلية. ويشير **M1** إلى وسيط ردود الحالة التجريبية الأولي، بينما يشير **M3** إلى وسيط ردود الحالة التجريبية الثالثة، بينما يشير **M2** إلى وسيط ردود الحالة التجريبية الثانية، في حين أن **M4** يشير إلى وسيط ردود الحالة التجريبية الرابعة.

الفرض البديل: H1: (M1+M3) ≠ (M2+M4): يؤثر توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني إيجاباً ومعنوياً على القيمة المضافة من وظيفة المراجعة الداخلية.

وبالرجوع إلى نتائج التحليل الإحصائي يمكن توضيح النتائج في الجدول التالي (جدول ٦-٦):

جدول (٦-٦)

نتائج اختبار Wilcoxon Signed Rank Test للفرض الرئيسي الأول (H1)

[١] اختبار Wilcoxon Signed Rank Test هو أحد الاختبارات اللامعلمية والذي يستهدف اختبار مدى وجود اختلافات معنوية وذات دلالة احصائية بين وسيطي مجموعتين أو عينتين غير مستقلتين من الأفراد أو المشاهدات، وهو يعتبر بمثابة البديل اللامعلمي لاختبار T المعلمي لعينتين غير مستقلتين؛ ووفقاً لهذا الاختبار فإذا كانت القيمة الاحتمالية P-Value أقل من (5%) يتم رفض فرض العدم وقبول الفرض البديل بما يشير إلى وجود اختلافات معنوية بين وسيطي المعالجتين. أما إذا كانت القيمة الاحتمالية P-Value أكبر من أو يساوي (5%) يتم رفض الفرض البديل وقبول فرض العدم بما يشير إلى عدم وجود اختلافات معنوية بين وسيطي المعالجتين (شبل، ٢٠١٩).

Test Statistics[a]

	Z	Asymp. Sig. (2-tailed)
التغير في القيمة المضافة نتيجة التحول من عدم توكيد المراجع الداخلي إلى توكيد المراجع الداخلي بشأن إدارة مخاطر الأمن السيبراني	-7.576	0.000

(المصدر: إعداد الباحثان)

وبناءاً عليه؛ يمكن القول أن القيمة الاحتمالية P-Value أقل من (5%)؛ وهو ما يعني وجود اختلاف ذو دلالة إحصائية بين متوسط إجابات المشاركين في الحالة التجريبية الأولي والثالثة مقارنةً بالحالة التجريبية الثانية والرابعة؛ وهو ما يشير إلى وجود تأثير لتوكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني على القيمة المضافة من وظيفة المراجعة الداخلية مقارنةً بعدم وجود توكيد من قبّل المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني. ولتحديد اتجاه تأثير العلاقة محل الدراسة يتم مقارنة متوسط الرتب الموجبة مقابل متوسط رتب السالبة، كما يتضح من الجدول التالي (جدول ٦- ٧).

جدول (٦-٧)

نتائج اختبار Wilcoxon Signed Rank Test للفرض الرئيسي الأول (H1) (الرتب)

Ranks

		N	Mean Rank	Ranks
التغير في القيمة المضافة نتيجة التحول من عدم توكيد المراجع الداخلي إلى توكيد المراجع الداخلي بشأن إدارة مخاطر الأمن السيبراني الداخلية	Negative Ranks	0	0.00	0.00
	Positive Ranks	76	38.5	2926.00
	Ties	0		
	Total	76		

(المصدر: إعداد الباحثان)

ومن الجدول السابق يتضح أن متوسط الرتب الموجبة أكبر من متوسط الرتب السالبة؛ وهو ما يشير إلى أن القيمة المضافة من وظيفة المراجعة الداخلية في حال وجود توكيد للمراجع الداخلي بشأن إدارة مخاطر الأمن السيبراني أكبر منها في حالة عدم وجود توكيد

للمراجع الداخلي بشأن إدارة مخاطر الأمن السيبراني؛ وهو ما يعني وجود تأثير إيجابي معنوي لتوكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني على القيمة المضافة من وظيفة المراجعة الداخلية مقارنةً بعدم التوكيد. وهو ما يشير إلى **رفض فرض العدم وقبول الفرض البديل؛ وبالتالي قبول الفرض الأول (H1)**؛ وهو ما يتفق مع ما توصل إليه البعض (Dikokoe , 2021 & Kahyaoglu and Caliyurt, 2018). وهو ما يدعم القول بأن وجود توكيد من قبّل القائم بوظيفة المراجعة الداخلية بشأن إدارة مخاطر الأمن السيبراني قد يساعد على إجراء تقييم شامل للمخاطر السيبرانية، وزيادة دقة وموضوعية وموثوقية المعلومات المحاسبية، وتحسين الأداء التشغيلي للمنشأة، وزيادة درجة الالتزام بالقوانين واللوائح، وبالتالي الإدارة الفعالة لمخاطر الأمن السيبراني؛ وتحسين سمعة المنشأة؛ وهو ما يؤدي إلى زيادة القيمة المضافة من وظيفة المراجعة الداخلية مقارنةً بعدم وجود توكيد من قبّل القائم بوظيفة المراجعة الداخلية بشأن إدارة مخاطر الأمن السيبراني.

٦-٤-٨-٢- نتائج اختبار الفرض الثاني (H2):

استهدف الفرض الثاني (H2) اختبار ما إذا كان التأثير الإيجابي المعنوي لتوكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني على القيمة المضافة من وظيفة المراجعة الداخلية سيختلف باختلاف طبيعة إسناد وظائف المراجعة الداخلية سواء كان إسناد داخلي أو إسناد خارجي. وقد استخدم الباحثان اختبار Wilcoxon Signed Rank Test اللامعلمي للعينتين غير المستقلتين؛ وقد تم إعادة صياغة الفرض الثاني (H2) في صورة فرض عدم وفرض بديل كما يلي:

فرض العدم : (M3-M1) =(M4-M2) : H0: لا يختلف التأثير الإيجابي المعنوي لتوكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني على القيمة المضافة من وظيفة المراجعة الداخلية مقارنةً بعدم التوكيد من قبّل المراجع الداخلي باختلاف طبيعة إسناد وظيفة المراجعة الداخلية.

الفرض البديل: H1: (M4-M2)≠ (M3-M1): يختلف التأثير الإيجابي المعنوي لتوكيد المراجعة الداخلية على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني على القيمة المضافة من وظيفة المراجعة الداخلية مقارنةً بعدم التوكيد من قبّل المراجع الداخلي باختلاف طبيعة إسناد وظيفة المراجعة الداخلية.

وبالرجوع إلى نتائج التحليل الإحصائي يمكن توضيح النتائج في الجدول التالي (جدول ٦-٨):

جدول (٦-٨)

نتائج اختبار Wilcoxon Signed Rank Test للفرض الرئيسي الثاني (H2)

Test Statistics[a]

	Z	Asymp. Sig. (2-tailed)
التغير في القيمة المضافة نتيجة التحول من عدم التوكيد إلى التوكيد في ظل الإسناد الخارجي لوظيفة المراجعة الداخلية – التغير في القيمة المضافة نتيجة التحول من عدم التوكيد إلى التوكيد في ظل الإسناد الداخلي لوظيفة المراجعة الداخلية	-5.385	0.000

(المصدر: إعداد الباحثان)

وبناءاً عليه؛ يمكن القول أن القيمة الاحتمالية P-Value أقل من (5%)؛ وهو ما يعني اختلاف القيمة المضافة من توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني مقارنةً بعدم التوكيد باختلاف طبيعة إسناد وظيفة المراجعة الداخلية. ولتحديد اتجاه تأثير العلاقة محل الدراسة يتم مقارنة متوسط الرتب الموجبة مقابل متوسط رتب السالبة، كما يتضح من الجدول التالي (جدول ٦- ٩):

جدول (٦-٩)

نتائج اختبار Wilcoxon Signed Rank Test للفرض الرئيسي الثاني (H2) (الرتب)

Ranks

		N	Mean Rank	Ranks
التغير في القيمة المضافة نتيجة التحول من عدم التوكيد إلى التوكيد في ظل الإسناد الخارجي لوظيفة المراجعة الداخلية – التغير في القيمة المضافة نتيجة التحول من عدم التوكيد إلى التوكيد في ظل الإسناد الداخلي لوظيفة المراجعة الداخلية	Negative Ranks	15	24.77	371.50
	Positive Ranks	58	40.16	2329.5
	Ties	3		
	Total	76		

(المصدر: إعداد الباحثان)

ومن الجدول السابق يتضح أن متوسط الرتب الموجبة أكبر من متوسط الرتب السالبة؛ وهو ما يشير إلى أن التغير في القيمة المضافة نتيجة التحول من عدم التوكيد إلي توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني في ظل الإسناد الخارجي لوظائف المراجعة الداخلية يزيد عن مقدار التغير في القيمة المضافة نتيجة التحول من عدم التوكيد إلي توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني في ظل الإسناد الداخلي لوظائف المراجعة الداخلية؛ وهو ما يشير إلى أن توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني في ظل الإسناد الخارجي لوظيفة المراجعة الداخلية يؤثر إيجابياً ومعنوياً بشكل أكبر على القيمة المضافة من وظيفة المراجعة الداخلية مقارنةً بالإسناد الداخلي لوظيفة المراجعة الداخلية. وهو ما يشير إلى **رفض فرض العدم وقبول الفرض البديل؛ وبالتالي قبول الفرض الثاني (H2)**؛ وهو ما يتفق مع ما توصل إليه البعض (Vuko et al., 2025 & Calvin et al., 2025 & Seetharaman et al., 2008) . وهو ما يدعم القول بأن الإسناد الخارجي لوظيفة المراجعة الداخلية قد يؤدي إلى زيادة جودة وفعالية إجراءات وضوابط تحقيق الأمن السيبراني، وزيادة درجة الالتزام بالقوانين واللوائح من قبّل الإدارة، ويزيد من القدرة على إدارة مخاطر الأمن السيبراني بكفاءة؛ فضلا عن أن توفير توكيد من قبّل المراجع الخارجي المُسند إليه وظيفة المراجعة الداخلية بشأن الممارسات المرتبطة بإدارة مخاطر الأمن السيبراني قد يزيد من ثقة الأطراف أصحاب المصلحة بشكل

أكبر مقارنةً بتوفير ذلك التوكيد من المراجع الداخلي التابع لإدارة المراجعة الداخلية بالشركة وهو ما يضيف قيمة للأطراف أصحاب المصلحة.

٦-٤-٨-٣- نتائج اختبار الفرض الثالث (H3):

استهدف الفرض الثالث **(H3)** اختبار ما إذا كان التأثير الإيجابي المعنوي لتوكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني على القيمة المضافة من وظيفة المراجعة الداخلية سيختلف باختلاف خبرة الأطراف أصحاب المصالح أم لا؟.

وقد تم اختبار ذلك الفرض إحصائياً من خلال حساب الفرق بين إدراك فئة الأطراف أصحاب المصلحة من ذوي الخبرة المرتفعة للقيمة المضافة من توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني، وبين إدراكهم في حال عدم وجود توكيد من قبّل المراجع الداخلي، وأيضاً حساب الفرق بين إدراك فئة الأطراف أصحاب المصلحة ذوي الخبرة المحدودة للقيمة المضافة من توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني، وبين إدراكهم في حال عدم وجود توكيد من قبّل المراجع الداخلي. ثم يتم مقارنة الفروق بين إدراك العينتين لاختبار ما إذا كان التأثير الإيجابي المعنوي لتوكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني على القيمة المضافة من وظيفة المراجعة الداخلية مقارنةً بعدم التوكيد سيختلف باختلاف مستوى الخبرة لدى الأطراف أصحاب المصلحة وذلك باستخدام اختبار **Mann-Whitney Test** اللامعلمي للعينتين المستقلتين[١].

[١] اختبار Mann-Whitney test هو أحد الاختبارات اللامعلمية والذي يستهدف اختبار مدى وجود اختلافات معنوية ذات دلالة إحصائية بين وسيطي مجموعتين أو عينتين مستقلتين من الأفراد أو المشاهدات؛ وهو يعتبر بمثابة البديل اللامعلمي لاختبار T المعلمي لعينتين مستقلتين (موسي، ٢٠١٨). ووفقاً لهذا الاختبار فإذا كانت القيمة الاحتمالية P-Value أقل من (5%) يتم رفض فرض العدم وقبول الفرض البديل بما يشير إلى وجود اختلافات معنوية بين وسيطي

وقد تم إعادة صياغة **الفرض الثالث (H3)** في صورة فرض عدم وفرض بديل كما يلي:

فرض العدم:H0: لا يختلف التأثير الإيجابي المعنوي لتوكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني على القيمة المضافة من وظيفة المراجعة الداخلية باختلاف خبرة أصحاب المصالح.

الفرض البديل: H1: يختلف التأثير الإيجابي المعنوي لتوكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني على القيمة المضافة من وظيفة المراجعة الداخلية باختلاف خبرة أصحاب المصالح.

وبالرجوع إلى نتائج التحليل الإحصائي يمكن توضيح النتائج في الجدول التالي (جدول ٦-١٠):

جدول (٦-١٠)

نتائج اختبار Mann-Whitney Test للفرض (H3)

	Mann-Whitney U	Wilcoxon W	Z	Asymp. Sig. (2-tailed)
التغير في القيمة المضافة لوظيفة المراجعة الداخلية نتيجة التحول من عدم التوكيد إلى التوكيد بشأن إدارة مخاطر الأمن السيبراني في ظل الدور المعدل لخبرة أصحاب المصالح	1989.00	3070.00	-1.803	0.71

(المصدر: إعداد الباحثان)

وبناءاً عليه؛ يمكن القول أن القيمة الاحتمالية P-Value أكبر من (5%)؛ وهو ما يشير إلى **رفض فرض البديل وقبول الفرض العدم**؛ وهو ما يعني عدم وجود تأثير معنوي لمستوى الخبرة لدى الأطراف أصحاب المصالح على القيمة المضافة من وظيفة المراجعة الداخلية نتيجة التحول من عدم توكيد القائم بوظيفة المراجعة الداخلية

العينتين المستقلتين. أما إذا كانت القيمة الاحتمالية P-Value أكبر من أو يساوي (5%) يتم رفض الفرض البديل وقبول فرض العدم بما يشير إلى عدم وجود اختلافات معنوية بين وسيطي العينتين المستقلتين (شبل، ٢٠١٩).

على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني مقارنةً بالتوكيد من قبّل القائم بوظيفة المراجعة الداخلية. وهو ما يشير إلى **رفض الفرض الثالث (H3)** وهو ما يتفق مع دراسات (الأباصيري، ٢٠١٨ & مرسي، ٢٠٢٣) ويتعارض مع دراسات (Gul et al., 2013 & Festus et al., 2020). **ويرى الباحثان** أنه يمكن إرجاع ذلك إلى إدراك الأطراف أصحاب المصلحة بغض النظر عن مستوى خبرتهم لأهمية القيمة المضافة من توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني؛ فضلاً عن أن الاعتماد على عدد سنوات العمل كمقياس لتحديد مستوى الخبرة قد يكون مقياساً غبر عادلاً لم يأخذ في الحسبان لعدة عوامل أخرى قد تؤثر على مستوى الخبرة مثل مستوى الذكاء ومستوى التدريب العملي والتأهيل العلمي للتطورات الحديثة في مجال العمل. وبالتالي يمكن القول أن توكيد المراجعة الداخلية بشأن إدارة مخاطر الأمن السيبراني يؤثر إيجابياً ومعنوياً على إدراك الأطراف أصحاب المصالح من ذوي الخبرة المرتفعة والمنخفضة للقيمة المضافة من وظيفة المراجعة الداخلية.

٦-٤-٨-٤- نتائج اختبار الفرض الرابع (H4):

استهدف الفرض الرابع **(H4)** اختبار ما إذا كان التأثير الإيجابي المعنوي لتوكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني على القيمة المضافة من وظيفة المراجعة الداخلية سيختلف باختلاف نوع الأطراف أصحاب المصالح أم لا؟.

وقد تم اختبار ذلك الفرض إحصائياً من خلال حساب الفرق بين إدراك فئة الأطراف أصحاب المصلحة من الذكور للقيمة المضافة من توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني، وبين إدراكهم في حال عدم وجود توكيد من قبّل المراجع الداخلي، وأيضاً حساب الفرق بين إدراك فئة الأطراف أصحاب المصلحة من الإناث للقيمة المضافة من توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني، وبين إدراكهم في حال عدم وجود توكيد

من قبّل المراجع الداخلي. ثم يتم مقارنة الفروق بين إدراك العينتين لاختبار ما إذا كان التأثير الإيجابي المعنوي لتوكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني على القيمة المضافة من وظيفة المراجعة الداخلية مقارنةً بعدم التوكيد سيختلف باختلاف نوع الأطراف أصحاب المصلحة وذلك باستخدام اختبار **Mann-Whitney Test** اللامعلمي للعينتين المستقلتين.

وقد تم إعادة صياغة **الفرض الرابع (H4)** في صورة فرض عدم وفرض بديل كما يلي:

<u>فرض العدم:H0</u>: لا يختلف التأثير الإيجابي المعنوي لتوكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني على القيمة المضافة من وظيفة المراجعة الداخلية باختلاف نوع أصحاب المصالح.

<u>الفرض البديل: H1</u>: يختلف التأثير الإيجابي المعنوي لتوكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني على القيمة المضافة من وظيفة المراجعة الداخلية باختلاف نوع أصحاب المصالح.

وبالرجوع إلى نتائج التحليل الإحصائي يمكن توضيح النتائج في الجدول التالي (جدول ٦-١١):

جدول (٦-١١)

نتائج اختبار Mann-Whitney Test للفرض (H4)

	Mann-Whitney U	Wilcoxon W	Z	Asymp. Sig. (2-tailed)
التغير في القيمة المضافة لوظيفة المراجعة الداخلية نتيجة التحول من عدم التوكيد إلى التوكيد بشأن إدارة مخاطر الأمن السيبراني في ظل الدور المعدل لنوع أصحاب المصالح	2602.500	4313.500	-0.469	0.639

(المصدر: إعداد الباحثان)

وبناءاً عليه؛ يمكن القول أن القيمة الاحتمالية P-Value أكبر من (5%)؛ وهو ما يشير إلى **رفض فرض البديل وقبول الفرض العدم؛** وهو ما يعني عدم وجود تأثير معنوي لنوع الأطراف أصحاب المصالح على القيمة المضافة من وظيفة المراجعة الداخلية نتيجة التحول من عدم توكيد القائم بوظيفة المراجعة الداخلية على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني مقارنةً بالتوكيد من قبّل القائم بوظيفة المراجعة الداخلية. وهو ما يشير إلى **رفض الفرض الرابع (H4)** وهو ما يتفق مع دراسة (مرسي، ٢٠٢٣) ويتعارض مع دراسات (Bear et al., 2010 & Fellner and Maciejovsky, 2007). **ويرى الباحثان** أنه يمكن إرجاع ذلك إلى إدراك الأطراف أصحاب المصلحة بغض النظر عن نوعهم لأهمية القيمة المضافة من توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني؛ وبالتالي يمكن القول أن توكيد المراجع الداخلي بشأن إدارة مخاطر الأمن السيبراني يؤثر إيجابياً ومعنوياً على إدراك الأطراف أصحاب المصالح من الذكور والإناث للقيمة المضافة من وظيفة المراجعة الداخلية.

٦-٤-٨-٥-خلاصة نتائج اختبار فروض البحث:

يمكن عرض خلاصة نتائج اختبار فروض البحث من خلال الجدول رقم (٦-١٢) كالتالي:

جدول رقم (٦-١٢) خلاصة نتائج اختبار فروض البحث

الفرض	صيغة الفرض البديل	نتيجة اختبار الفرض
H1	يؤثر توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني إيجاباً ومعنوياً على القيمة المضافة من وظيفة المراجعة الداخلية.	قبول الفرض
H2	يختلف التأثير الإيجابي المعنوي لتوكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني على القيمة المضافة من وظيفة المراجعة الداخلية باختلاف تفعيل التوجه نحو الإسناد الخارجي لوظيفة المراجعة الداخلية من عدمه.	قبول الفرض
H3	يختلف التأثير الإيجابي المعنوي لتوكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني على القيمة المضافة من وظيفة المراجعة الداخلية باختلاف خبرة أصحاب المصالح.	رفض الفرض
H4	يختلف التأثير الإيجابي المعنوي لتوكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني على القيمة المضافة من وظيفة المراجعة الداخلية باختلاف نوع أصحاب المصالح.	رفض الفرض

(المصدر: إعداد الباحثان)

٦-٤-٩- التحليلات الأخرى:

فيما يلي مجموعة من التحليلات الأخرى؛ والهدف منها التحقق من صحة ودقة نتائج التحليل الأساسي؛ وفي هذا الشأن تم إجراء تحليلان؛ وهما التحليل الإضافي، والتحليل الأساسي كما يلي:

٦-٤-٩-١- التحليل الإضافي:

يمكن اعتبار التحليل الإضافي على إنه إحدى المنهجيات المتعلقة بإضفاء مزيد من الدقة والوضوح والفهم للعلاقات الأساسية والرئيسية محل الدراسة؛ بالإضافة إلى قدرته على معالجة أي قصور أو عيوب قد تكون موجودة في نموذج البحث الأساسي؛ وذلك من خلال إعادة تشغيل نموذج البحث لاختبار **الفرض الأول (H1)** والمتمثل في اختبار أثر توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني على مقاييس القيمة المضافة من وظيفة المراجعة الداخلية كلاً على حدى والمتمثلة في الأداء التشغيلي للمنشاة، ومدي صدق التقارير والقوائم المالية، ومدي الالتزام بالقوانين واللوائح من قبل المنشأة، وسمعة الشركة مقاسة بحصتها السوقية.

ولإعادة اختبار الفرض الأول (H1)؛ تم استخدام اختبار Wilcoxon Signed Rank Test للتحقق من مدى وجود اختلاف في القيمة المضافة من توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني مقاسة بـ (الأداء التشغيلي للمنشأة، وصدق التقارير والقوائم المالية، والالتزام بالقوانين واللوائح، سمعة الشركة) مقارنةً حالتي عدم التوكيد (الحالة التجريبية الأولى والثالثة) / حالتي التوكيد (الحالة التجريبية الثانية والرابعة).

وقد أظهرت النتائج الإحصائية (جدول ٦-١٣) وجود اختلاف ذو دلالة إحصائية بين متوسط إجابات المشاركين في الحالات التجريبية الأولي والثالثة مقارنةً بإجابات المشاركين في الحالات التجريبية الثانية والرابعة وذلك فيما يتعلق بالقيمة المضافة من توكيد المراجع الداخلي بشأن إدارة مخاطر الأمن السيبراني مقاسة بـ؛ الأداء التشغيلي للمنشأة (Z=-7.589 & P-Value=0.000)، صدق التقارير والقوائم المالية (Z=-

Z=-7.587 & P-Value=0.000)،، الالتزام بالقوانين واللوائح (Z=-7.592 & P-Value=0.000)،، سمعة الشركة مقاسة بالحصة السوقية (Z=-7.589 & P-Value=0.000)، وهو ما يشير إلى وجود تأثير معنوي لتوكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني على كل من الأداء التشغيلي للمنشأة، وصدق التقارير والقوائم المالية، والالتزام بالقوانين واللوائح، والحصة السوقية للمنشأة مقارنةً بعدم وجود توكيد من قبّل المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني.

جدول (٦-١٣)

نتائج اختبار Wilcoxon Signed Rank Test للفرض الأول (H1) (التحليل الإضافي)

Test Statistics[a]

	Z	Asymp. Sig. (2-tailed)
التغير في الأداء التشغيلي للمنشأة نتيجة التحول من عدم توكيد المراجع الداخلي إلى توكيد المراجع الداخلي بشأن إدارة مخاطر الأمن السيبراني	-7.589	0.000
التغير في صدق التقارير والقوائم المالية للمنشأة نتيجة التحول من عدم توكيد المراجع الداخلي إلى توكيد المراجع الداخلي بشأن إدارة مخاطر الأمن السيبراني	-7.583	0.000
التغير في درجة التزام المنشأة بالقوانين واللوائح نتيجة التحول من عدم توكيد المراجع الداخلي إلى توكيد المراجع الداخلي بشأن إدارة مخاطر الأمن السيبراني	-7.587	0.000
التغير في الحصة السوقية للمنشأة نتيجة التحول من عدم توكيد المراجع الداخلي إلى توكيد المراجع الداخلي بشأن إدارة مخاطر الأمن السيبراني	-7.592	0.000

(المصدر: إعداد الباحثان)

ولتحديد اتجاه تأثير العلاقة محل الدراسة يتم مقارنة متوسط الرتب الموجبة مقابل متوسط رتب السالبة، كما يتضح من الجدول التالي (جدول ٦- ١٤) كما يلي:

جدول (٦-١٤)

نتائج اختبار Wilcoxon Signed Rank Test للفرض الأول (H1) (التحليل الإضافي) (الرتب)

Ranks

		N	Mean Rank	Ranks
التغير في الأداء التشغيلي للمنشأة نتيجة التحول من عدم توكيد المراجع الداخلي إلى توكيد المراجع الداخلي بشأن إدارة مخاطر الأمن السيبراني	Negative Ranks	0	0.000	0.00
	Positive Ranks	76	38.50	2926.00
	Ties	0		
	Total	76		
التغير في صدق التقارير والقوائم المالية للمنشأة نتيجة التحول من عدم توكيد المراجع الداخلي إلى توكيد المراجع الداخلي بشأن إدارة مخاطر الأمن السيبراني	Negative Ranks	0	0.00	0.00
	Positive Ranks	76	38.50	2926.00
	Ties	0		
	Total	76		
التغير في درجة التزام المنشأة بالقوانين واللوائح نتيجة التحول من عدم توكيد المراجع الداخلي إلى توكيد المراجع الداخلي بشأن إدارة مخاطر الأمن السيبراني	Negative Ranks	0	0.00	0.00
	Positive Ranks	76	38.50	2926.00
	Ties	0		
	Total	76		
التغير في الحصة السوقية للمنشأة نتيجة التحول من عدم توكيد المراجع الداخلي إلى توكيد المراجع الداخلي بشأن إدارة مخاطر الأمن السيبراني	Negative Ranks	0	0.00	0.00
	Positive Ranks	76	68.5	2926.00
	Ties	0		
	Total	76		

(المصدر: إعداد الباحثان)

ويتضح من الجدول السابق؛ وجود اتجاه لدى المشاركين في التجربة نحو تحسين الأداء التشغيلي للمنشأة، وزيادة صدق التقارير والقوائم المالية للمنشأة، وزيادة مستوى التزام المنشأة بالقوانين واللوائح، وزيادة الحصة السوقية للمنشأة وتحسين سمعتها في ظل توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني مقارنةً بعدم توكيد المراجع الداخلي حيث كانت الرتب الموجبة للعناصر السابقة أكبر من الرتب السالبة؛ وتدعم هذه النتائج مجتمعة **قبول الفرض الأول للبحث (H1) وهو ما يدعم نتائج التحليل الأساسي.**

٦-٤-٩-٢- تحليل الحساسية Sensitivity Analysis:

تعد منهجية تحليل الحساسية من ضمن التحليلات التي تستخدم في المنهجيات المتطورة للتحقق من دقة وصحة نتائج التحليل الإحصائي الأساسي؛ وقد يتم ذلك من خلال اختبار فروض البحث على مدار فترات زمنية مختلفة، /أو من خلال إعادة اختبار فروض البحث بالتطبيق على عينة مختلفة، و/أو من خلال قياس المتغير التابع و/أو المتغير المستقل بمقاييس بديلة مختلفة عن المقاييس المستخدمة في ظل التحليل الأساسي. وعليه فقد تم إعادة تشغيل نموذج البحث لاختبار الفرض الثالث والرابع وذلك من خلال تقسيم عينة البحث إلى مجموعتين؛ **الأولي هي مجموعة الأطراف أصحاب المصالح الداخليين** (أعضاء بمجلس الإدارة، وأعضاء بلجان المراجعة)، **والثانية هي مجموعة الأطراف أصحاب المصالح الخارجيين** (محللين ماليين، وشركات سمسرة، ومراقبي حسابات، وإدارة منح الائتمان بالبنوك، وإدارة أمناء الاستثمار بالبنوك).

ويمكن توضيح الإحصاء الوصفي لعينات الدراسة في ظل تحليل الحساسية لاختبار الفرض الثالث والرابع (H3&H4) من خلال الجدول التالي (٦-١٥) كما يلي:

جدول (٦-١٥)

الإحصاء الوصفي لعينة الدراسة في ظل تحليل الحساسية لاختبار الفرض (H3&H4)

البيان	أصحاب المصالح الداخليين (٩ أعضاء مجلس إدارة، ٤ لجان مراجعة)	أصحاب المصالح الخارجيين (٣٢ إدارة منح الائتمان، ٧ إدارة أمناء الاستثمار، ٤ محلل مالي، ١ شركات سمسرة، ١٩ مراقب حسابات خارجي)	الإجمالي
عدد مفردات العينة	13	63	76
نسبة عدد مفردات العينة إلى الإجمالي	17.1%	82.9%	100%
عدد المفردات من حيث الخبرات العملية مرتفع الخبرة منخفض الخبرة	 13 0	 40 23	 53 23
نسبة الخبرات العملية مرتفع الخبرة منخفض الخبرة	 100% 0%	 63.5% 36.5%	 69.7% 30.3%
عدد المفردات من حيث النوع ذكر	 11	 36	 47

أنثى	2	27	29
نسبة النوع			
ذكر	84.6%	57.1%	61.8%
أنثى	15.4%	42.9%	38.2%

(المصدر: إعداد الباحثان)

فبالنسبة للفرض الثالث (H3)؛ بلغت عينة الدراسة من الأطراف أصحاب المصالح الداخليين ذوي الخبرة المرتفعة (13)؛ بينما بلغت عينة الدراسة من الأطراف أصحاب المصالح الداخليين ذوي الخبرة المنخفضة (0) وبالتالي لا يمكن إجراء اختبار Mann-Whitney Test لاختبار الفرض الثالث (H3) على مستوى عينة الدراسة من الأطراف أصحاب المصالح الداخليين. في حين بلغت عينة الدراسة من الأطراف أصحاب المصالح الخارجيين ذوي الخبرة المرتفعة (40)؛ بينما بلغت عينة الدراسة من الأطراف أصحاب المصالح الخارجيين ذوي الخبرة المنخفضة (23) ويوضح الجدول الثاني (جدول ٦-١٦) نتائج اختبار الفرض الثالث (H3) على مستوى الأطراف أصحاب المصالح الخارجيين، وبمقارنتها بالتحليل الأساسي.

جدول (٦-١٦)

نتائج اختبار Mann-Whitney Test للفرض (H3) (تحليل الحساسية)

نوع التحليل		Mann-Whitney U	Wilcoxon W	Z	Asymp. Sig. (2-tailed)
التحليل الاساسي	التغير في القيمة المضافة لوظيفة المراجعة الداخلية نتيجة التحول من عدم التوكيد إلى التوكيد بشأن إدارة مخاطر الأمن السيبراني في ظل الدور المعدل لخبرة أصحاب المصالح	1989.00	3070.00	-1.803	0.71
تحليل الحساسية	التغير في القيمة المضافة لوظيفة المراجعة الداخلية نتيجة التحول من عدم التوكيد إلى التوكيد بشأن إدارة مخاطر الأمن السيبراني في ظل الدور المعدل لخبرة أصحاب المصالح الخارجيين	1540.00	2621.00	-1.522	0.128

(المصدر: إعداد الباحثان)

ويتضح من الجدول السابق؛ عدم وجود تأثير معنوي لمستوى خبرة الأطراف أصحاب المصالح الخارجيين على القيمة المضافة من توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني مقارنةً بعدم توكيد المراجع الداخلي حيث بلغت القيمة الاحتمالية (P-Value = 0.128)؛ وهو ما يعني رفض الفرض الثالث (H3)؛ هو ما يتوافق مع نتائج التحليل الأساسي.

أما بالنسبة للفرض الرابع (H4)؛ بلغت عينة الدراسة من الأطراف أصحاب المصالح الداخليين من الذكور (11)؛ بينما بلغت عينة الدراسة من الأطراف أصحاب المصالح الداخليين من الإناث (2). في حين بلغت عينة الدراسة من الأطراف أصحاب المصالح الخارجيين من الذكور (36)؛ بينما بلغت عينة الدراسة من الأطراف أصحاب المصالح الخارجيين من الإناث (27) ويوضح الجدول الثاني (جدول ٦-١٧) نتائج اختبار الفرض الرابع (H4) على مستوى الأطراف أصحاب المصالح الداخليين والخارجيين كلاً على حدى، وبمقارنتها بالتحليل الأساسي.

جدول (٦-١٧)

نتائج اختبار Mann-Whitney Test للفرض (H4) (تحليل الحساسية)

نوع التحليل		Mann-Whitney U	Wilcoxon W	Z	Asymp. Sig. (2-tailed)
التحليل الاساسي	التغير في القيمة المضافة لوظيفة المراجعة الداخلية نتيجة التحول من عدم التوكيد إلى التوكيد بشأن إدارة مخاطر الأمن السيبراني في ظل الدور المعدل لنوع أصحاب المصالح	2602.500	4313.500	-0.469	0.639
تحليل الحساسية	التغير في القيمة المضافة لوظيفة المراجعة الداخلية نتيجة التحول من عدم التوكيد إلى التوكيد بشأن إدارة مخاطر الأمن السيبراني في ظل الدور المعدل لنوع أصحاب المصالح الخارجيين	1867.500	3352.500	-0.378	0.706
	التغير في القيمة المضافة لوظيفة المراجعة الداخلية نتيجة التحول من عدم التوكيد إلى التوكيد بشأن إدارة مخاطر الأمن السيبراني في ظل الدور المعدل لنوع أصحاب المصالح الداخليين	37.00	290.00	-0.499	0.618

(المصدر: إعداد الباحثان)

ويتضح من الجدول السابق؛ عدم وجود تأثير معنوي لنوع الأطراف أصحاب المصالح الخارجيين على القيمة المضافة من توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني مقارنةً بعدم توكيد المراجع الداخلي حيث بلغت القيمة الاحتمالية (P-Value = 0.706)؛ كما يتضح عدم وجود تأثير معنوي لنوع الأطراف أصحاب المصالح الداخليين على القيمة المضافة من توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني مقارنةً بعدم توكيد المراجع الداخلي حيث بلغت القيمة الاحتمالية (P-Value = 0.618)؛ وهو ما يشير إلى رفض الفرض الرابع (H4)؛ وهو ما يتوافق مع نتائج التحليل الأساسي.

وفي نفس السياق؛ فقد قام الباحثان بإعادة تشغيل نموذج البحث لاختبار الفرض الأول (H1) والفرض الثاني (H2) من خلال تغيير عينة الدراسة؛ وعليه فقد تم استخدام عينة من أعضاء هيئة التدريس ومعاونيهم وطلبة الدراسة العليا وذلك قياساً على (Serag and Daoud, 2021)؛ ويمكن توضيح الإحصاء الوصفي لعينات الدراسة في ظل تحليل الحساسية لاختبار الفرض (H1&H2) من خلال الجدول التالي (٦-١٨) كما يلي:

جدول (٦-١٨)

الإحصاء الوصفي لعينة الدراسة في ظل تحليل الحساسية

البيان	طلبة دراسات عليا	أعضاء هيئة تدريس	أعضاء هيئة معاون	الإجمالي
عدد مفردات العينة	68	35	27	130
نسبة عدد مفردات العينة إلى الإجمالي	52.3%	26.9%	20.8	100%
عدد المفردات من حيث الخبرات العملية				
مرتفع الخبرة	41	35	13	89
منخفض الخبرة	27	0	14	41
نسبة الخبرات العملية				
مرتفع الخبرة	60.3%	100%	48.1%	68.5%
منخفض الخبرة	39.7%	0%	51.9%	31.5%
عدد المفردات من حيث النوع				
ذكر	30	17	12	59
أنثى	38	18	15	71
نسبة النوع				
ذكر	44.1%	48.6%	44.4%	45.4%
أنثى	55.9%	51.4%	55.6%	54.6%

(المصدر: إعداد الباحثان)

فبالنسبة للفرض الأول (H1)؛ يوضح الجدول التالي (جدول ٦-١٩) نتائج اختبار Wilcoxon Test للفرض الأول (H1) في ظل تحليل الحساسية ومقارنته بنتائج التحليل الأساسي كما يلي:

جدول (٦-١٩)

نتائج اختبار Wilcoxon Signed Rank Test للفرض الرئيسي الأول (H1) في ظل تحليل الحساسية

Test Statistics[a] & Rank

		التحليل الأساسي			تحليل الحساسية		
		N	Mean Rank	Ranks	N	Mean Rank	Ranks
التغير في القيمة المضافة نتيجة التحول من عدم توكيد المراجع الداخلي إلى توكيد المراجع الداخلي بشأن إدارة مخاطر الأمن السيبراني	Negative Ranks	0	0.00	0.00	0	0.00	0.00
	Positive Ranks	76	38.5	2926.0	130	65.50	8515.0
	Ties	0			0		
	Total	76			130		
	Z	-7.576			-9.904		
	Asymp. Sig. (2-tailed)	0.000			0.000		

(المصدر: إعداد الباحثان)

ومن الجدول السابق؛ يتضح أن القيمة الاحتمالية لتحليل الحساسية P-Value أقل من (5%)؛ كما أن مجموع الرتب الموجبة أكبر من مجموع الرتب السالبة؛ وهو ما يعني وجود اختلاف ذو دلالة إحصائية بين متوسط إجابات المشاركين في الحالة التجريبية الأولي والثالثة مقارنةً بالحالة التجريبية الثانية والرابعة؛ وهو ما يشير إلى وجود تأثير إيجابي معنوي لتوكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني على القيمة المضافة من وظيفة المراجعة الداخلية مقارنةً بعدم وجود توكيد من قبّل المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر

الأمن السيبراني بالنسبة لعينة الأكاديميين وطلبة الدراسات العليا. وهو ما يشير إلى قبول الفرض الأول (H1)؛ هو ما يدعم نتائج التحليل الأساسي المعتمد على عينة من الأطراف أصحاب المصالح الداخليين والخارجيين.

أما بالنسبة **للفرض الثاني (H2)**؛ يوضح الجدول التالي (جدول ٦-٢٠) نتائج اختبار Wilcoxon Test للفرض الثاني (H2) في ظل تحليل الحساسية ومقارنته بنتائج التحليل الأساسي كما يلي:

جدول (٦-٢٠)

نتائج اختبار Wilcoxon Signed Rank Test للفرض الثاني (H2) في ظل تحليل الحساسية

Test Statistics[a] & Rank

		التحليل الأساسي			تحليل الحساسية		
		N	Mean Rank	Ranks	N	Mean Rank	Ranks
التغير في القيمة المضافة نتيجة التحول من عدم التوكيد إلى التوكيد في ظل الإسناد الخارجي لوظيفة المراجعة الداخلية – التغير في القيمة المضافة نتيجة التحول من عدم التوكيد إلى التوكيد في ظل الإسناد الداخلي لوظيفة المراجعة الداخلية	Negative Ranks	15	24.77	371.50	45	66.30	2983.5
	Positive Ranks	58	40.16	2329.5	79	60.34	4766.5
	Ties	3			6		
	Total	76			130		
	Z	-5.385			-2.228		
	Asymp. Sig. (2-tailed)	0.000			0.026		

(المصدر: إعداد الباحثان)

ومن الجدول السابق؛ يتضح أن القيمة الاحتمالية P-Value في تحليل الحساسية أقل من (5%)؛ كما أن مجموع الرتب الموجبة أكبر من مجموع الرتب السالبة؛ وهو ما يشير إلى وجود اختلاف في القيمة المضافة من توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني مقارنةً بعدم التوكيد باختلاف طبيعة إسناد

وظيفة المراجعة الداخلية؛ فضلاً عن أن التغير في القيمة المضافة نتيجة التحول من عدم التوكيد إلي توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني في ظل الإسناد الخارجي لوظائف المراجعة الداخلية يزيد عن مقدار التغير في القيمة المضافة نتيجة التحول من عدم التوكيد إلي توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني في ظل الإسناد الداخلي لوظائف المراجعة الداخلية؛ وهو ما يشير إلى أن توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني في ظل الإسناد الخارجي لوظيفة المراجعة الداخلية يؤثر إيجابياً ومعنوياً بشكل أكبر على القيمة المضافة من وظيفة المراجعة الداخلية مقارنةً بالإسناد الداخلي لوظيفة المراجعة الداخلية وذلك بالنسبة لعينة الأكاديميين وطلبة الدراسات العليا. وهو ما يشير إلى قبول الفرض الثاني (H2)؛ وهو ما يدعم نتائج التحليل الأساسي المعتمد على عينة من الأطراف أصحاب المصالح الداخليين والخارجيين.

٦-٥- نتائج البحث، والتوصيات، ومجالات البحث المقترحة:

استهدف هذا البحث إجراء دراسة تجريبية لاختبار القيمة المضافة من توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني؛ إضافة إلى دراسة الأثر المعدل لكل من طبيعة الإسناد لوظيفة المراجعة الداخلية ونوع وخبرة الأطراف أصحاب المصالح؛ وذلك بتطبيق على عينة من الأطراف أصحاب المصلحة والمهتمين بوظيفة المراجعة الداخلية.

وفي ضوء التحول الرقمي من قبّل معظم الشركات في الوقت الراهن؛ فقد زادت المهام التوكيدية والاستشارية المطلوبة من المراجع الداخلي في ظل العمل في بيئة أعمال تتسم بارتفاع درجة المخاطر المحيطة بها. ولزيادة كفاءة وفعالية وظيفة المراجعة الداخلية في ظل الوضع الراهن فقد تطلب الأمر توجيه مزيد من الاهتمام نحو التأهيل العلمي والعملي للمراجع الداخلي، والإلمام بنظم مراجعة تكنولوجيا المعلومات، وزيادة القدرة على تقييم وإدارة مخاطر الأمن السيبراني والحد منها،

والعمل على وضع ضوابط وسياسات وإجراءات من شأنها تحقيق الأمن السيبراني؛ وقد يتحقق هذا الأمر عند القيام بإسناد وظيفة المراجعة الداخلية لطرف خارجي مستقل نظراً لتمتعه بتوافر الإمكانيات المادية والفنية والتكنولوجية؛ فضلاً عن الخبرة التي تؤهله للقيام بالمهام السابق ذكرها بكفاءة وفعالية.

وقد أظهرت نتائج الدراسة التجريبية أن توكيد القائم بوظيفة المراجعة الداخلية على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني تؤثر إيجابياً ومعنوياً على القيمة المضافة من وظيفة المراجعة الداخلية؛ من خلال التأثير الإيجابي على الأداء التشغيلي للمنشأة، وزيادة دقة وصدق التقارير والقوائم المالية المُفصح عنها، وزيادة مستوى التزام المنشأة بالقوانين واللوائح وتحسين سمعة المنشأة وحصتها السوقية.

كما توصلت الدراسة إلى الى وجود تأثير معنوي لطبيعة إسناد وظيفة المراجعة الداخلية على القيمة المضافة من توكيد المراجع الداخلي على مزاعم الإدارة بشأن إدارة مخاطر الأمن السيبراني وأن الأثر الإيجابي لتوكيد المراجع الداخلي في مجال إدارة مخاطر الأمن السيبراني على قيمته المضافة يزداد في حالة الإسناد الخارجي لوظيفة المراجعة الداخلية مقارنةً بالإسناد الداخلي لوظائفها. كما توصلت الدراسة إلى عدم اختلافات ذات دلالة معنوية لخبرة ونوع الأطراف أصحاب المصلحة في إدراك القيمة المضافة من توكيد المراجع الداخلي على مزاعم إدارة المخاطر بشأن إدارة مخاطر الأمن السيبراني.

وأخيراً؛ فقد أظهرت النتائج الإحصائية للتحليل الاضافي، وتحليل الحساسية تدعيم كل النتائج التي تم التوصل إليها في ظل التحليل الأساسي.

وفي ضوء أهداف البحث، ومشكلته، وحدوده، وما انتهى إليه البحث من نتائج في شقيه النظري والتطبيقي؛ **يوصي الباحث بما يلي**:

- ضرورة اهتمام الشركات بالتأهيل العلمي والعملي للمراجعين الداخليين لاكتسابهم مهارات وقدرات تؤهلهم لإضافة قيمة للمنشأة في مجال إدارة

مخاطر الأمن السيبراني، ومواكبة المتطلبات التنظيمية الحديثة المتعلقة بمعايير أمن المعلومات. حيث أن التحدي الرئيسي الذي يواجه وظيفة المراجعة الداخلية يتمثل في مواكبة التطورات التكنولوجية الديناميكية باستمرار.

- العمل على تحسين متطلبات الافصاح عن المخاطر السيبرانية وآليات الحد منها وإدارتها في الوقت المناسب.
- العمل على تغيير وتعديل مناهج المحاسبة والمراجعة لتشمل على محتويات متعلقة بتحليل البيانات واستخدام التقنيات التكنولوجية الحديثة والتدريب عليها.
- قيام الجهات المهنية المعنية بالمراجعة الداخلية بتطوير معايير المراجعة الداخلية والإرشادات ذات الصلة بما يساعد المراجع الداخلي على القيام بالأدوار التوكيدية والاستشارية في مجال الأمن السيبراني.
- دمج استراتيجية تحقيق الأمن السيبراني ضمن استراتيجية إدارة المخاطر في الشركات؛ مع ضرورة تمتعها بالمرونة اللازمة لمواكبة أي تغيرات غير محسوبة وتوافقها مع طبيعة بيئة عمل الشركة.
- توفير إطار ومعيار موحد يتعلق بتوكيد المراجع الداخلي عن مزاعم إدارة المخاطر بشأن إدارة مخاطر الأمن السيبراني لتجنب عدم الاتساق في التقارير الموجهة إلى مجلس الإدارة ولجان المراجعة.

وبناءاً على ما خلص إليه البحث في الدراسة النظرية والتطبيقية من نتائج؛ وفي ضوء مشكلة البحث؛ ووفقاً لحدوده، **يعتقد الباحث وجود بعض مجالات البحث المستقبلية ذات الصلة، ومن أهمها ما يلي:**

- أثر المشترك للإفصاح عن إدارة مخاطر الأمن السيبراني وجودة هيكل الرقابة الداخلية على قرارات الاستثمار في الأسهم والأداء المالي للشركة: دليل تجريبي ميداني.

- أثر توكيد مراقب الحسابات على إفصاح الشركات المقيدة بالبورصة عن إدارة مخاطر الأمن السيبراني على قرارات الاستثمار في الأسهم - الدور المعدل لنوع المستثمر وهيكل الملكية: دليل تجريبي ميداني مصري.
- المقدرة التقييمية الإضافية للمحتوى المعلوماتي للإفصاح عن مخاطر الأمن السيبراني - هيكل التمويل وسمعة الشركة كمتغيرات معدلة: دليل من الشركات المقيدة بالبورصة المصرية.
- اثر قيام المراجع الداخلي بدوره الاستشاري في مجال إدارة مخاطر الأمن السيبراني على قرار مراقب الحسابات بالاعتماد عليه – استقلالية وظيفة المراجعة الداخلية وتوقيتها كمتغيرات معدلة: دراسة تجريبية ميدانية.
- القيمة المضافة من الدورين الاستشاري والتوكيدي للمراجعة الداخلية في مجال إدارة مخاطر دخول الشركة لأسواق جديدة: السمات النوعية للمراجع الداخلي والتحول الرقمي كمتغيرات معدلة: دليل تجريبي ميداني من مصر.
- نحو مؤشر لقياس مستوى الإفصاح عن مخاطر الأمن السيبراني يلائم بيئة الأعمال المصرية واختبار المقدرة التقييمية لمحتواه المعلوماتي – القطاع الصناعي كمتغير معدل: دليل من الشركات المقيدة بالبورصة المصرية.

المراجع:

أولاً: المراجع باللغة العربية:

- أبو الخير، محمد حارس محمد طه. (٢٠٢٣). "أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الاستقرار المالي في البنوك الإلكترونية: دراسة ميدانية". ***المجلة العلمية للدراسات والبحوث المالية والإدارية***، كلية التجارة، جامعة السادات، المجلد (١٥)، العدد (١): ١- ٦٥.
- الأباصيري، بسمة حسن محمد. (٢٠١٨). "***أثر إعادة هيكلة شكل ومحتوى تقرير المراجع الخارجي غير المعدل على مدى إمكانية اعتماد المستثمر المؤسسي على القوائم المالية: دراسة تجريبية***". رسالة دكتوراه غير منشورة، كلية التجارة، جامعة الاسكندرية.

- الصيرفي، اسماء أحمد. (٢٠٢٥). "أثر إفصاح الشركات عن تفعيل إدارة مخاطر الأمن السيبراني على تقدير مراقب الحسابات لمستوى مخاطر المراجعة الخارجية". ***مجلة البحوث المحاسبية***، كلية التجارة، جامعة طنطا، المجلد (١٢)، العدد (١): ١٠٦- ١٥٠.
- أميرهم، جيهان عادل. (٢٠٢٢). "أثر جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني وانعكاساته على ترشيد قرارات المستثمرين (دراسة ميدانية)". ***مجلة البحوث المالية والتجارية***، كلية التجارة، جامعة بورسعيد، المجلد (٢٣)، العدد (١): ٣٢٥- ٣٧٧.
- شبل، منى سليمان محمود. (٢٠١٩). "***أثر الإفصاح المحاسبي عن انبعاثات غازات الاحتباس الحراري على قراري الاستثمار والإقراض – دراسة تجريبية***". رسالة دكتوراه غير منشورة، كلية التجارة، جامعة الإسكندرية.
- شحاته، السيد شحاته. (٢٠٢٢). "نحو دور فاعل للمراجع الداخلي في إدارة مخاطر الأمن السيبراني في الشركات المقيدة بالبورصة المصرية". ***المجلة العلمية للدراسات والبحوث المالية والإدارية***، كلية التجارة، جامعة مدينة السادات، المجلد (١٣)، العدد (٢): ٢٦- ٣٧.
- عطية، أحمد محمد صلاح. (٢٠٢١). "التحول الرقمي في مصر: هل يلقي بمسئوليات جديدة على المراجع؟". ***مجلة البحوث التجارية***، كلية التجارة، جامعة الزقازيق، المجلد (٤٣)، العدد (١): ٥٣- ٦٥.
- فرج، هاني خليل. (٢٠٢٢). "أثر توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكتروني على قرار الاستثمار بالأسهم- دراسة تجريبية". ***مجلة المحاسبة والمراجعة لاتحاد الجامعات العربية***، كلية التجارة، جامعة بني سويف، المجلد (١١)، العدد (٢): ١٢٩- ٢٠٩.
- فريد، حنان هارون. (٢٠٢٢). "الدور المقترح لمراجع الحسابات في إضفاء الثقة على تقرير إدارة مخاطر الأمن السيبراني واثره في دلالة القوائم المالية: دراسة تجريبية". ***المجلة العلمية للدراسات التجارية والبيئية***، المجلد (١٣)، العدد (٤): ٤١٢- ٤٨٨.
- قرار رئيس مجلس الوزراء رقم ٢٢٥٩. (٢٠١٤). "إنشاء المجلس الأعلى للأمن السيبراني". ***الجريدة الرسمية***، العدد (٥٠)، مكرر (أ).
- قرار رئيس مجلس الوزراء رقم ١٦٣٠. (٢٠١٦). "تحديد اختصاصات ومهام المجلس الأعلى للأمن السيبراني وتنظيم عمله". ***الجريدة الرسمية.***
- قرار رئيس مجلس الوزراء رقم ٩٩٤. (٢٠١٧). "تنفيذ قرارات وتوصيات المجلس الأعلى للأمن السيبراني"، ***الجريدة الرسمية***، العدد (١٧)، مكرر (ب).

- محروس، رمضان عارف مضان.، وصالح، أبو الحمد مصطفي. (٢٠٢٢). "استخدام المنهجية الرشيقة في تطوير أداء المراجعة الداخلية لمواجهة مخاطر الأمن السيبراني". ***مجلة البحوث المالية والتجارية***، كلية التجارة، جامعة بورسعيد، العدد (٣): ٤٣٢- ٤٩١.
- محمود، يارا محمود يونس، وحافظ، سماح طارق.، والجوهري، إبراهيم السيد. (٢٠٢٥). "أثر توكيد المراجع الخارجي عن مخاطر الأمن السيبراني على قرارات المستثمرين (دراسة تجريبية)". ***المجلة العلمية للدراسات والبحوث المالية والتجارية***، كلية التجارة، جامعة دمياط، المجلد (٦)، العدد (١)، الجزء (٢): ٨٢٧- ٨٦٠.
- محمد، سحر سعيد حامد. (٢٠١٩). ***"أثر الإسناد والتوقيت والوضع الوظيفي للمراجعة الداخلية على قرار المراجع الخارجي بشأن مدى اعتماده على وظيفة المراجعة الداخلية: دراسة تجريبية"***. رسالة دكتوراه غير منشورة، كلية التجارة، جامعة الإسكندرية.
- مرسي، تامر أحمد محمد. (٢٠٢٣). ***"أثر الإفصاح عن توكيد المراجع الداخلي على فعالية الإبلاغ عن الغش والفساد المالي على إدراك اصحاب المصالح لفجوة التوقعات بالمراجعة الداخلية – دراسة تجريبية"***. رسالة دكتوراه غير منشورة، كلية التجارة، جامعة الإسكندرية.
- موسى، سعاد زغلول عبده. (٢٠١٨). ***"أثر توكيد المراجع الخارجي على تقارير الأعمال المتكاملة على قراري الاستثمار ومنح الائتمان – دراسة تجريبية"***. رسالة دكتوراه غير منشورة، كلية التجارة، جامعة الإسكندرية.
- نافع، محمود عبد المقصود. (٢٠٢٢). "أثر تقنيات الثورة الصناعية الرابعة على مهنة المحاسبة والمراجعة: دراسة ميدانية". ***مجلة الإسكندرية للبحوث المحاسبية***، كلية التجارة، جامعة الإسكندرية، المجلد (٦)، العدد (٣): ٣٩٧- ٤٢٩.
- يوسف، حنان محمد إسماعيل. (٢٠٢٤). "القيمة المضافة من فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني: دراسة انتقادية وتجريبية". ***مجلة البحوث المحاسبية***، كلية التجارة، جامعة طنطا، العدد (١): ٥٢٥- ٥٩٤.

ثانياً: المراجع باللغة الأجنبية:

- Abu-Musa, A. A. (2001). "***Evaluating the security of computerized accounting information systems: An empirical study on the Egyptian banking industry***". Master`s Thesis, 1-545.
- Abu-Musa, A. A. (2006). "Investigating the perceived threats of computerized accounting information systems in developing countries: An empirical study on Saudi organizations". ***Journal of King Saud University – Computer and Information Sciences***, 18: 1-30.
- Ahlawat, S. S., & Lowe, D. J. (2004). "An examination of internal auditor objectivity: In-house versus outsourcing". ***Auditing: A Journal of Practice & Theory***. 23(2): 147-158.
- Alina, C. M., & Cerasela, S. E., & Gabriela, G. (2017). "Internal audit role in cybersecurity". ***"Ovidius" University Annals, Economic Sciences Series***, 17 (2): 510-513.
- Awinbugri, A. E., & Daniel, Y. (2019). "determinants of internal audit effectiveness in selected hospitals within the Kumasi Metropolis". ***International Journal of Research and Innovation in Social Science***, 3(7): 165-168.
- Babiker, I. (2025). "The role of internal audit in enhancing cyber security from the auditors` point of view". ***Journal of Business and Environmental Sciences***, 4(1): 127-146.
- Badawy, H. A. (2021). The impact of assurance quality and level on cyber security risk management Program on non-professional Egyptian investors' decisions: An experimental study. ***Alexandria Journal of Accounting Research***, 5(3): 1-56.
- Bear, S., & Rahman, N., & Post, C. (2010). "The impact of board diversity and gender composition on corporate social responsibility and firm reputation". ***Journal of business ethics***, 97(2), 207-221.

- Calvin, C., & Eulerich, M., & Holt, M. (2025). "Characteristics of cybersecurity and IT involvement by the IA activity". ***International Journal of Accounting Information System***, 56, 100726.
- Caplan, D., & Janvrin, D., & Kurtenbach, J. (2007). "Internal audit outsourcing: An analysis of self-regulation by the accounting profession". ***Research I n Accounting Regulation***, 19: 3-34.
- Carey, P., & Subramaniam, N., & Ching, K. C. W. (2006). "Internal audit outsourcing in Australia". ***Accounting and Finance***, 46(1): 11-30.
- Chukwunedu, O. S., & Ogochukwu, O. G., & Onuora, O. A. (2014). "Factors affecting audit committee quality in Nigeria". ***International Journal of Academic Research in Business and Social Sciences***, 4(12): 398-426.
- Deloitte, 2017. "Cybersecurity and the role of internal audit- An urgent call to action". Available at: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-cyber-ia-urgent-call-to-action.pdf
- Dikokoe, T. (2021). "***Role of internal audit in managing cyber security risks***". Master`s Thesis, University of Johannesburg (South Africa).
- Del Vecchio, S. C., & Clinton. D. B. (2003). "Co-sourcing and other alternatives in acquiring auditing services". ***Internal Auditing***, 18(2): 33-39.
- Durst, S., & Hinteregger, C., & Zieba, M. (2024). "The effect of environmental turbulence on cyber security risk management and organization resilience". ***Computer and Security***, 137, 103591.
- Elmaasrawy, H. E., & Tawfik, O. I. (2025). "Impact of the assertive and advisory role of internal auditing on proactive measures to enhance cybersecurity: Evidence from GCC. ***Journal of Science and Technology Policy Management***, 16(1): 68-93.

- Elqadi, M. M. A., & Mohamed, M. A., & Abdelmageed, M. H. (2024). "The role of risk-based internal auditing on the activation of cyber security to control information risk: A field study". ***Journal of Accounting Thought***, 28(2): 117-146.
- Fellner, G., & Maciejovsky, B. (2007). "Risk attitude and market behavior: Evidence from experimental asset markets". ***Journal of Economic Psychology***, 28(3), 338-350.
- Festus, O. O., & Gideon, A. T., & Clement, O. O., & Adesodun, A. I. (2020). "Audit committee characteristics and investors` stake in Nigerian quoted companies". ***Management and Accounting Review***, 19(1): 21-48.
- Gul, F. A., & Wu, D., & Yang, Z. (2013). "Do individual auditors affect audit quality? Evidence from archival data". ***The Accounting Review***, 88(6), 1993-2023.
- Haapamaki, E., & Sihvonen, J. (2019)."Cybersecurity in accounting research". ***Managerial Auditing Journal***, 34(7): 808-834.
- Hepworth, L. R., & Greenman, C., & Esplin, D., & Johnston, R. (2022). "Cybersecurity and data privacy: The rising expectations within internal audit. ***Journal of Forensic and Investigative Accounting,*** 14(3): 454-465.
- Hossain, SK. T., & Yigitcanlar, T., & Nguyen, K., & Xu, Y. (2025). "Cybersecurity in local governments: A systematic review and framework of key challenges". ***Urban Governance***, 5(1): 1-19.
- Houqe, M. N., & Zijl, T. V., & Dunstan, K., & Karim, A. K. M. W. (2015). "Corporate ethics and auditor choice – international evidence". ***Research in Accounting Regulation***, 27: 57-65.
- Huang, T. C., & Huang, H. W., & Lee, C. C. (2014)." Corporate Executive's Gender and Audit Fees". ***Managerial Auditing Journal***, 29(6): 527-547.

- Inyang, O. E., & Enya, F. E., &Outugoma, F. O. (2021). "Internal audit effectiveness in public health sector in South – South Nigeria". ***United International Journal for Research & Technology***, 2(8): 127-132.
- Islam, MD. S., & Farah, N., & Stafford, T. F. (2018). "Factors associated with security/cybersecurity audit by internal audit function: An international study". ***Managerial Auditing Journal***, 33(4): 377-409.
- Johari, Z. A., & Ghazali, A. W., & Isa, Y. M., & Shafie, N. A., & Sanusi, S. (2023). "Digital disruption and cybersecurity threats: Redefining the role of internal auditing". ***International Conference in Technology, Humanities and Management***.
- Kahyaoglu, S. B., & Caliyurt, K. (2018). "Cyber security assurance process from the internal audit perspective". ***Managerial Auditing Journal***, 33(4): 360-376.
- Koutoupis, A. G., & Kampouris, C. G. (2021). "A systematic literature review on the implementation of internal audit in European and non-European public hospitals". ***Journal of Governance and Regulation***, 10(4): 336-342.
- Loeb, M. P., & Zhou, L. (2016). "Investing in cybersecurity: Insights from the Gorden-Loeb Model". ***Journal of Information Security***, 7: 49-59.
- Metwally, A. B. M., & Abdelazim, S. I., & Almarji, M. T. (2022). "Internal auditors` role in confronting cyber and fraud risks related to outsourcing insurance: An exploratory study". ***Alexandria Journal of Accounting Research***, 6(3): 1-31.
- Mnif, Y., & Cherif, I. (2022). "Audit partner workload, gender and audit quality". ***Journal of Applied Accounting Research***, 23(5):1047-1070.
- Ojeka, S. A. & Odianonsen, I. F., & Obigbemi, I. F. (2014). "Effectiveness of audit committee and firm financial performance in

Nigeria: an empirical analysis". ***Journal of Accounting and Auditing: Research & Practice,*** 1-39.

- Peursem, K. V., & Jiang, L. (2008). "Internal audit outsourcing practice and rationales: SME evidence from New Zealand". ***Asian Review Of Accounting***, 16(3): 219-245.
- Rittenberg, L., & Moore, W., & Covaleski, M. (1999). "The outsourcing phenomenon". ***The Internal Auditor***, 56(2): 42-46.
- Rittenberg, L., & Covaleski, M. A. (2001). "Internalization versus externalization of the internal audit function: An examination of professional and organizational imperatives". ***Accounting, Organizations and Society***, 26(7-8): 617-641.
- Seetharaman, A., & Moorthy, M. K., & Saravanan, A. S. (2008). "Outsourcing of internal audit and independence of auditors". ***Corporate Board Ownership and Control***, 4(2): 40-49.
- Serag, A. A., & Daoud, M. M. (2021). "A proposed framework for value-based internal audit and its impact on the added value and the expectation gab of internal audit: (A field study in Egypt)". ***Alexandria Journal of Accounting Research***, 5(1): 1183-1254.
- Schneider, A. (2008). "Outsourcing Internal Auditing". ***The Internal Auditing***, 16-25.
- Shamsuddin, A., & Adam, M. A., & Adnan, S. A., & Madzlan, S. N. I., & Yasin, Y. M. (2018). "The effectiveness of internal audit functions in managing cybersecurity in Malaysia`s banking institutions". ***International Journal of Industrial Management***, 4(1): 1-5.
- Slapnicar, S., & Vuko, T., & Gular, M., & Drascek, M. (2022). "Effectiveness of Cybersecurity audit". ***International Journal of Accounting Information Systems***, 44, 100548.
- Song, J. M., & Wang, T., & Yen, J. C., & C, Y. H. (2024)."Does cybersecurity maturity level assurance improve cybersecurity risk

management in supply chains?". ***International journal of Accounting Information Systems***, 54, 100695.

- Stafford, T., & Deitz, G., & Li, Y. (2018). "The role of internal audit and user training in information security policy compliance". ***Managerial Auditing Journal,*** 33(4): 410-424.
- Steinbart, P. J., & Raschke, R., & Gal, G., & Dilla, W. N. (2012). "The relationship between internal audit and information security: An exploratory investigation". ***Accounting, Organization and Society***, 71: 15-29.
- Steinbart, P. J., & Raschke, R., & Gal, G., & Dilla, W. N. (2018). "The influence of a good relationship between the internal audit and information security functions on information security outcomes". ***International Journal of Accounting Information Systems***, 13: 228-243.
- Suleiman, D. M., & Dandago, K. I. (2014). "The extent of internal audit functions outsourcing by Nigerian deposit money banks". ***Procedia - Social and Behavioral Sciences***, 164: 222-229.
- Usman, A., & Che-Ahmad, A., & Abdulmalik, S. O. (2024). "The role of internal auditors characteristics in cybersecurity risk assessment in financial-based business organizations: A conceptual review". ***Revista De Gestao Social E Ambiental***, 18(6): 1-33.
- Vitali, S., & Giuliani, M. (2024). "Emerging digital technologies and auditing firms: Opportunities and challenges". ***International Journal Of Accounting Information Systems***, 53, 100676.
- Vuko, T., & Slapnicar, S., & Cular, M., & Drascek, M. (2025). "Key drivers of cybersecurity audit effectiveness: A neo-institutional perspective". ***International Journal of Auditing***, 29(1): 188-206.
- Yang, L., & Lau, L., & Gan, H. (2020). "Investor`s perceptions of the cybersecurity risk management reporting framework". ***International Journal of Accounting & Information Management***, 28(1): 167-183.

ملاحق البحث

ملحق البحث (١)

الحالات التجريبية

السيد الأستاذ الفاضل / .....

تحية طيبة وبعد ،،،،،،

يقوم الباحثان بإعداد بحث في مجال العلاقة بين القيمة المضافة من توكيد المراجع الداخلي وإدارة مخاطر الأمن السيبراني في ظل الدور المعدل لإسناد وظيفة المراجعة الداخلية ونوع وخبرة المراجع الداخلي. وتمثل الحالات المرفقة أحد أهم أدوات البحث لإجراء الدراسة التجريبية.

والباحثان إذ يشكركم مسبقاً على حسن تعاونكم معهما؛ ويرجو التكرم من سيادتكم بقراءة الحالات التالية، والإجابة على كافة الأسئلة المرافقة لها، وسوف تحظى هذه الإجابات على السرية التامة الكاملة، كما إنها سوف تُستخدم فقط لأغراض البحث العلمي.

وتفضلوا سيادتكم بقبول فائق الاحترام ،،،،

الباحثان

د/ محمد إبراهيم عبده الفار
مدرس بقسم المحاسبة والمراجعة
كلية التجارة- جامعة دمنهور
٠١٠٠٤٨٧٧٤٨٥
Mohmedelfar@hotmail.com

د/ ياسر محمد عبدالله
مدرس بقسم المحاسبة والمراجعة
كلية التجارة - جامعة دمنهور

أولاً: البيانات الشخصية:

١- الاسم (اختياري): .....

٢- النوع: ذكر (.....) أم أنثى (.....).

٣- الوظيفة الحالية: .....

٤- طبيعة عملك :

- إدارة أمناء الاستثمار بالبنوك (.....).
- شركات السمسرة (.....).
- مستثمرين (.....).
- محللين ماليين (.....).
- إدارة منح الائتمان بالبنوك (.....).
- عضو مجلس إدارة بالمنشأة (.....).
- عضو لجنة مراجعة بالمنشأة (.....).
- عضو هيئة تدريس (.....).
- معيد أو مدرس مساعد (.....).
- طالب دراسات عليا (.....).
- أخرى (.....).

٥- أعلى مؤهل علمي حصلتم سيادتكم عليه: من فضلك أذكره

- بكالوريوس (.....): في.....
- دبلوم / دراسات عليا (.....): في.....؛ وفي .....
- ماجستير مهني (.....): في.....
- ماجستير أكاديمي (.....): في.....
- دكتوراه مهنية: (.....): في .....
- دكتوراه أكاديمية (.....): في.....

٦- عدد سنوات الخبرة في العمل :

- أقل من ٥ سنوات (.....).
- من ٥ سنوات إلى أقل من ١٠ سنوات (.....).
- من ١٠ سنوات إلى أقل من ١٥ سنوات (.....).
- من ١٥ سنة فأكثر (.....).

ثانياً: المصطلحات الفنية ذات الصلة بموضوع البحث:

١- **الأمن السيبراني Cybersecurity:** هي عملية حماية المعلومات من خلال منع واكتشاف والاستجابة لمواجهة الهجمات الالكترونية لضمان توافر وسلامة ومصداقية وسرية المعلومات.

٢- **مخاطر الأمن السيبراني Cybersecurity Risk:** هي أنشطة غير مشروعة تتعرض لها البنية التحتية الأساسية للمنظمة عن طريق استغلال الثغرات الأمنية في نظم المعلومات وذلك بهدف التأثير السلبي في جميع أنشطة المنظمة وإمكانياتها وإلحاق الضرر المادي بها وبسمعتها والكشف عن معلومات المنظمة وإجراء تعديلات عليها أو تدميرها.

٣- **إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management:** هي مجموعة من السياسات والإجراءات الرقابية المصممة لحماية المعلومات والأنظمة الالكترونية من الحوادث الأمنية التي تعرض الأمن السيبراني للشركة لمخاطر قد تمنعها من تحقيق أهدافها؛ وتساعد تلك الإجراءات على اكتشاف الهجمات والاستجابة لها وتخفيف آثارها والقضاء على الآثار الناجمة عنها في اسرع وقت ممكن.

٤- **وظيفة المراجعة الداخلية Internal Audit:** نشاط مستقل وموضوعي يهدف إلى تقديم الخدمات التوكيدية والاستشارية لخلق قيمة مضافة للمؤسسة وتحسين عملياتها والمساعدة على تحقيق أهداف المنظمة من خلال اتباع مدخل منظم ومنهجي لتقييم وتحسين فعالية عمليات إدارة المخاطر والرقابة والحوكمة.

٥- **الدور التوكيدي للمراجعة الداخلية:** هي خدمات مهنية مستقلة تهدف إلى تحسين جودة ومحتوى المعلومات التي يوفرها مسئول داخل المنظمة لخدمة متخذي القرارات وبالتالي فهي خدمة ثلاثية الأطراف بين من يوفر المعلومات (القسم أو المسئول داخل الشركة) ومن يضفي الصدق والثقة على هذه المعلومات (المراجع الداخلي) وبين من سيعتمد على هذه المعلومات في اتخاذ القرارات (الإدارة).

٦- **الدور التوكيدي للمراجعة الداخلية في مجال الأمن السيبراني:** يستهدف توفير ضمان بأن المخاطر السيبرانية قد تم تقييمها بشكل مناسب؛ فضلاً عن تقديم دليل مستقل عن مدى فعالية وكفاءة سياسات الأمن السيبراني ومدى الالتزام بها، وعمليات إدارة مخاطر الأمن السيبراني وضوابط آليات الرقابة الداخلية وفعاليتها في سلامة وتوافر وسرية المعلومات.

ثالثاً: الحالات التجريبية

الحالة التجريبية (١)

(توجد إدارة مراجعة داخلية مع عدم وجود تقرير بالتوكيد على افصاحات إدارة المخاطر السيبرانية)

فيما يلي التقارير والقوائم المالية المستقلة المختصرة الخاصة بشركة (XZ) المساهمة والخاضعة للقانون ١٥٩ لسنة ١٩٨١ عن السنة المنتهية في ٢٠٢٤/١٢/٣١ والمقيدة بالبورصة المصرية والتي تعمل في مجال الاتصالات وتكنولوجيا المعلومات.

ويتوافر لدى شركة (XZ) إدارة لمخاطر الأمن السيبراني (تابعة لإدارة المخاطر بصفة عامة) وتقوم بإعداد تقاريرها عن إدارة مخاطر الأمن السيبراني ورفعها لمجلس الإدارة ورئيس لجنة المراجعة. وقد تعرضت الشركة خلال عام ٢٠٢٤ لبعض الهجمات السيبرانية لبياناتها مما ترتب عليه زيادة في التكاليف المتعلقة بالاستجابة لمخاطر الأمن السيبراني وإداراتها؛ كما انخفضت الإيرادات كنتيجة لفقدان جزء كبير من عملائها؛ وقد تم الإفصاح عن ذلك من قبّل إدارة مخاطر الأمن السيبراني في تقريرها المشار إليه.

كما يتوافر لدى شركة (XZ) إدارة للمراجعة الداخلية تتبع المدير التنفيذي (إدارة مراجعة داخلية مستقلة تنظيمية) وتعد تقاريرها له ولرئيس لجنة المراجعة ولا تتضمن تلك التقارير تقرير بالتوكيد على افصاحات مدير إدارة مخاطر الأمن السيبراني بالمرة. كما حصلت الشركة على تقرير مراقب حسابات نظيف عن التقارير والقوائم المالية عن سنة ٢٠٢٤.

١- قائمة المركز المالي في ٢٠٢٤/١٢/٣١:

بيان	الأرقام بالألف
النقدية وما في حكمها	٥٠٠٠٠٠
الأصول الثابتة	٤٣٥٠٠٠
مشروعات تحت التنفيذ	١٢٠٠٠٠
قوائم العملاء	١٠٠٠٠٠
مخزون	٣٠٠٠٠٠
الآلات والمعدات	٢٠٠٠٠٠
يخصم منها: مجمع الإهلاك	(٤٠٠٠٠)
يخصم منها: مجمع خسائر تدهور	(١٠٠)
إجمالي الأصول	**١٥١٤٩٠٠**
رأس المال	٢٠٠٠٠٠
صافي أرباح العام	١٣١٤٩٠٠
أرباح محجوزة	٥٠٠٠٠
الدائنون	١٠٠٠٠
قروض وتسهيلات ائتمانية	٤٠٠٠٠
إجمالي الخصوم	**١٥١٤٩٠٠**

٢- قائمة الدخل المختصرة عن الفترة المنتهية في ٢٠٢٤/١٢/٣١:

بيان	(الأرقام بالألف)
إيراد النشاط	٢١٥٢٦٣٠٠
يخصم: تكلفة النشاط	(١٨٩٥٦٧١٥)
مجمل الربح	**٢٥٦٩٥٨٥**
يخصم: مصروف إدارية وعمومية	(١٢٥٤٦٨٥)
صافي أرباح العام	**١٣١٤٩٠٠**

في ضوء البيانات السابقة؛ يرجي التكرم بالإجابة على الأسئلة التالية:

١- بخصوص الأداء التشغيلي للشركة؛ حققت الشركة معدل عائد على الأصول هذا العام يبلغ (١٢%)؛ ففي رأيك فإنه سوف يزيد كالتالي:

٠	١	٢	٣	٤	٥	٦	٧	٨	٩	١٠

٢- بخصوص مدى صدق القوائم المالية؛ ففي رأيك فإن القوائم المالية للشركة ستكون خالية من التحريفات الجوهرية وذات ثقة ومصداقية كالتالي:

٠	١	٢	٣	٤	٥	٦	٧	٨	٩	١٠

٣- بخصوص مدى الالتزام بالقوانين واللوائح؛ ففي رأيك فإن الشركة سيكون لديها التزام بالقوانين واللوائح ذات الصلة كالتالي:

٠	١	٢	٣	٤	٥	٦	٧	٨	٩	١٠

٤- بخصوص الحصة السوقية للمنشأة؛ إذا كانت الحصة السوقية للمنشأة خلال عام ٢٠٢٤ كانت (٢٠%)؛ ففي رأيك فإنها سوف تزيد في العام القادم كالتالي:

٠	١	٢	٣	٤	٥	٦	٧	٨	٩	١٠

الحالة التجريبية (٢)

(توجد إدارة مراجعة داخلية مع وجود تقرير بالتوكيد على افصاحات إدارة المخاطر السيبرانية)

افترض أنه في الحالة التجريبية (١)؛ أن مدير إدارة المراجعة الداخلية **قد قام بإعداد تقرير بالتوكيد على افصاحات نائب مدير إدارة المخاطر عن إدارة مخاطر الأمن السيبراني موجهاً للمدير التنفيذي ورئيس لجنة المراجعة.**

في ضوء البيانات السابقة؛ يرجي التكرم بالإجابة على الأسئلة التالية:

١- بخصوص الأداء التشغيلي للشركة؛ حققت الشركة معدل عائد على الأصول هذا العام يبلغ (١٢%)؛ ففي رأيك فإنه سوف يزيد كالتالي:

٠	١	٢	٣	٤	٥	٦	٧	٨	٩	١٠

٢- بخصوص مدى صدق القوائم المالية؛ ففي رأيك فإن القوائم المالية للشركة ستكون خالية من التحريفات الجوهرية وذات ثقة ومصداقية كالتالي:

٠	١	٢	٣	٤	٥	٦	٧	٨	٩	١٠

٣- بخصوص مدى الالتزام بالقوانين واللوائح؛ ففي رأيك فإن الشركة سيكون لديها التزام بالقوانين واللوائح ذات الصلة كالتالي:

٠	١	٢	٣	٤	٥	٦	٧	٨	٩	١٠

٤- بخصوص الحصة السوقية للمنشأة؛ إذا كانت الحصة السوقية للمنشأة خلال عام ٢٠٢٤ كانت (٢٠%)؛ ففي رأيك فإنها سوف تزيد في العام القادم كالتالي:

٠	١	٢	٣	٤	٥	٦	٧	٨	٩	١٠

الحالة التجريبية (٣)

(الإسناد الخارجي بالكامل لوظيفة المراجعة الداخلية مع عدم وجود تقرير بالتوكيد على افصاحات إدارة المخاطر السيبرانية)

افترض أنه في الحالة التجريبية (١)؛ **أن الشركة ليس لديها إدارة للمراجعة الداخلية وتقوم بإسناد وظيفة المراجعة الداخلية بالكامل لطرف من خارج الشركة؛** ولم **يقم الطرف الخارجي المسند إليه وظيفة المراجعة الداخلية بإعداد تقريراً عن توكيده على افصاحات نائب مدير إدارة المخاطر عن إدارة مخاطر الأمن السيبراني.**

في ضوء البيانات السابقة؛ يرجي التكرم بالإجابة على الأسئلة التالية:

١- بخصوص الأداء التشغيلي للشركة؛ حققت الشركة معدل عائد على الأصول هذا العام يبلغ (١٢%)؛ ففي رأيك فإنه سوف يزيد كالتالي:

٠	١	٢	٣	٤	٥	٦	٧	٨	٩	١٠

٢- بخصوص مدى صدق القوائم المالية؛ ففي رأيك فإن القوائم المالية للشركة ستكون خالية من التحريفات الجوهرية وذات ثقة ومصداقية كالتالي:

٠	١	٢	٣	٤	٥	٦	٧	٨	٩	١٠

٣- بخصوص مدى الالتزام بالقوانين واللوائح؛ ففي رأيك فإن الشركة سيكون لديها التزام بالقوانين واللوائح ذات الصلة كالتالي:

٠	١	٢	٣	٤	٥	٦	٧	٨	٩	١٠

٤- بخصوص الحصة السوقية للمنشأة؛ إذا كانت الحصة السوقية للمنشأة خلال عام ٢٠٢٤ كانت (٢٠%)؛ ففي رأيك فإنها سوف تزيد في العام القادم كالتالي:

٠	١	٢	٣	٤	٥	٦	٧	٨	٩	١٠

الحالة التجريبية (٤)

(الإسناد الخارجي بالكامل لوظيفة المراجعة الداخلية مع وجود تقرير بالتوكيد على افصاحات إدارة المخاطر السيبرانية)

افترض أنه في الحالة التجريبية (٣)؛ **أن الطرف الخارجي المسند إليه القيام بوظيفة المراجعة الداخلية قد قام بإعداد تقرير بالتوكيد على افصاحات نائب مدير إدارة المخاطر عن إدارة المخاطر الأمن السيبراني.**

في ضوء البيانات السابقة؛ يرجي التكرم بالإجابة على الأسئلة التالية:

١- بخصوص الأداء التشغيلي للشركة؛ حققت الشركة معدل عائد على الأصول هذا العام يبلغ (١٢%)؛ ففي رأيك فإنه سوف يزيد كالتالي:

٠	١	٢	٣	٤	٥	٦	٧	٨	٩	١٠

٢- بخصوص مدى صدق القوائم المالية؛ ففي رأيك فإن القوائم المالية للشركة ستكون خالية من التحريفات الجوهرية وذات ثقة ومصداقية كالتالي:

٠	١	٢	٣	٤	٥	٦	٧	٨	٩	١٠

٣- بخصوص مدى الالتزام بالقوانين واللوائح؛ ففي رأيك فإن الشركة سيكون لديها التزام بالقوانين واللوائح ذات الصلة كالتالي:

٠	١	٢	٣	٤	٥	٦	٧	٨	٩	١٠

٤- بخصوص الحصة السوقية للمنشأة؛ إذا كانت الحصة السوقية للمنشأة خلال عام ٢٠٢٤ كانت (٢٠%)؛ ففي رأيك فإنها سوف تزيد في العام القادم كالتالي:

٠	١	٢	٣	٤	٥	٦	٧	٨	٩	١٠