قياس أثر الملاءة المهنية للمراجع الداخلي على جودة الأمن السيبراني في ضوء الحوكمة الرقمية: دراسة تطبيقية

إعداد

د. وليد أحمد محمد علي

أستاذ المحاسبة المساعد، كلية تكنولوجيا الإدارة ونظم المعلومات، جامعة بورسعيد

dr.walid79@gmail.com

المجلة العلمية للدراسات والبحوث المالية والتجارية

كلية التجارة – جامعة دمياط

المجلد الخامس - العدد الثاني – الجزء الثاني - يوليو ٢٠٢٤

التوثيق المقترح وفقاً لنظام APA:

علي، وليد أحمد محمد (٢٠٢٤). قياس أثر الملاءة المهنية للمراجع الداخلي على جودة الأمن السيبراني في ضوء الحوكمة الرقمية: دراسة تطبيقية، **المجلة العلمية للدراسات والبحوث المالية والتجارية**، كلية التجارة، جامعة دمياط، ٥(٢) ج٢، ٩٩١-١٠٣٣.

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

قياس أثر الملاءة المهنية للمراجع الداخلي على جودة الأمن السيبراني في ضوء الحوكمة الرقمية: دراسة تطبيقية

د. وليد أحمد محمد علي

الملخص:

مما لاشك فيه أن الحوكمة الرقمية أصبحت تمثل أهمية كبيرة على المستوى العالمي، ويتم تطبيق الحوكمة الرقمية بشكل عام من خلال الإجراءات والعمليات التي يتم من خلالها توجيه المنشآت وتوزيع المسئوليات على مختلف الأطراف، وتلعب المراجعة الداخلية دوراً هاماً في التأثر بالحوكمة الرقمية وخاصة فيما يتعلق بجودة الأمن السيبراني، وقد تمثل الهدف الرئيسي للبحث في دراسة أثر الحوكمة الرقمية على العلاقة بين الملاءة المهنية للمراجع الداخلي وجودة الأمن السيبراني، ولتحقيق هذا الهدف قام الباحث بصياغة مجموعة من الفروض لعل أهمها: "لا توجد علاقة ذات دلالة إحصائية بين الحوكمة الرقمية والملاءة المهنية للمراجع الداخلي"، ولاختبار هذه الفروض تم الاستعانة بمجموعة من الأساليب الإحصائية تم استخدامها لخدمة إعداد الدراسة التطبيقية بهدف تحقيق أغراض البحث، وقد أسفرت تلك الدراسة عن مجموعة من النتائج كان أهمها: المهارات التكنولوجية التي يتمتع بها المراجع الداخلي تعزز من ملاءته المهنية بصدد التعامل مع متطلبات ومخاطر الأمن السيبراني بما يدعم جودة الأمن السيبراني، وذلك في ضوء مؤشرات العالم الرقمي الجديد، كما أثبتت نتائج التحليل الإحصائي وجود علاقة ذات دلالة إحصائية بين الحوكمة الرقمية والملاءة المهنية للمراجع الداخلي حيث كانت قيمة معامل التحديد **(0.1782)** وهذه القيمة تشير إلى أن المتغيرات المستقلة في النموذج تفسر ما نسبته **(17.8 %)** من التغير في الملاءة المهنية للمراجع الداخلي حيث كانت إشارة معامل الانحدار موجبة وكانت القيمة الاحتمالية **(Sig = 0.00)** أقل من مستوى المعنوية **(0.05)** وهو ما يثبت عدم صحة الفرض الأول وقبول الفرض البديل، وفي النهاية أوصى الباحث بمجموعة من التوصيات لعل أهمها: أن التأهيل العلمي والعملي لم يعد هو المؤشر الوحيد للملاءة المهنية للمراجع الداخلي، ولكن التكيف والتعامل مع العالم الرقمي والإلمام بالقدرات التكنولوجية يمثل أحد الشروط الهامة لممارسة مهنة المراجعة الداخلية وخاصة فيما يتعلق بالأمن السيبراني.

الكلمات المفتاحية: الحوكمة الرقمية – الملاءة المهنية للمراجع الداخلي – جودة الأمن السيبراني.

مقدمة:

سعت منشآت الأعمال في الآونة الأخيرة إلى ابتكار مجموعة من الأساليب غير التقليدية تتمتع بالكثير من الكفاءة والفعالية بهدف تحسين أدائها مع الحفاظ على حصتها في السوق وتحقيق الميزة التنافسية، وذلك من خلال السعي الدائم والمتواصل نحو إرساء قواعد للنظام الداخلي لتلك المنشآت، يتمتع بالقوة ويعتمد على مجموعة من التقنيات الحديثة التي تهدف إلى دعم عمليات المراجعة الداخلية لإضافة قيمة وتحسين الإجراءات وتعزيز المراجعة الداخلية في ظل أنظمة معلوماتية متطورة، وذلك بهدف الحفاظ على أمن المعلومات داخل هذه المنشآت وهو ما يعرف بالأمن السيبراني، وفي هذا الإطار فقد أشارت منظمة المراجعة الداخلية **(IIA, ٢٠٢١)** إلى ضرورة أن يتفهم المراجعون الداخليون ومعاهد ومنظمات المراجعة الداخلية أهمية الاستفادة من التكنولوجيا، ووفقا للمعايير الدولية لممارسة المراجعة الداخلية بشكل عام، ومعيار IIA ١٢١٠.A٣، بصفة خاصة "يجب على المراجعين الداخلين أن يمتلكوا معرفة كافية بمخاطر وضوابط تكنولوجيا المعلومات الرئيسية وتقنيات المراجعة القائمة على التكنولوجيا المتاحة لأداء العمل المسند إليهم"، بالإضافة إلى إطار كفاءة المراجع الداخلي لمعهد المراجعين الداخليين **(IIA)** والذي يحدد الكفاءات المتعددة القائمة على التكنولوجيا، أو المطلوبة لتخطيط وأداء أعمال المراجعة الداخلية، بما في ذلك المهارات المتعلقة باستخدام أدوات وتقنيات المراجعة القائمة على التكنولوجيا.

والجدير بالذكر أن جميع المتطلبات السابقة التي نادت بها المنشآت المختلفة بشأن تفعيل دور المراجعة الداخلية لا يتأتى إلا من خلال وجود ملاءة مهنية لجميع مهام وأنشطة المراجع الداخلي لتكون بمثابة آليات فاعلة نحو تحقيق جودة الأمن السيبراني وتقليص مخاطره، وفي ذات الوقت ظهرت الحاجة للحوكمة الرقمية، خاصة في ضوء التحولات الرقمية الكبيرة على المستوى المحلي والدولي، والتي يأتي دورها كعنصر مكمل لحوكمة الشركات وكداعم لأعمال المراجعة الداخلية من خلال مجموعة من الضوابط والإجراءات التي تحكم سير العمليات التكنولوجية، وتحكم الرقابة عليها وتعمل أيضاً على تدعيم نظام الرقابة الداخلية والذى يعمل على الحد من مخاطر الأمن السيبراني في ظل نظم المعلومات المحاسبية الإلكترونية الرقمية، مما يترتب عليه زيادة ثقة مستخدمي المعلومات المحاسبية في المنشآت **(Smanidr et al., 2022, Xiaofei,2020).**

ولذا فإن السؤال الذي يتبادر إلى الذهن، هل تؤثر الملاءة المهنية للمراجع الداخلي على تحقيق جودة الأمن السيبراني في ضوء الحوكمة الرقمية؟ هذا ما سوف يجيب عنه البحث الحالي نظرياً وعملياً.

مشكلة البحث:

أدت التطورات الكبيرة في أنظمة تكنولوجيا المعلومات إلى إحداث نقلة نوعية في عالم الأعمال في السنوات الأخيرة – حيث أصبح الحفاظ على سرية وأمن المعلومات والذي يطلق عليه (الأمن السيبراني) من الأمور الهامة التي تمثل تحدياً كبيراً لاستمرارية الأعمال، وعلى الرغم من اهتمام منظمات الأعمال بأساليب الحد من الحوادث والاختراقات المتزايدة لنظم المعلومات إلا أن الأساليب المقترحة من خلال خبراء تكنولوجيا المعلومات أصبحت ليست كافية، وفي هذا الشأن تستطيع المراجعة الداخلية أن تؤدي دوراً فعالاً في تحقيق أهداف الحماية وتقديم خدمات تأكيد أمن أنظمة المعلومات التي تحتوي على معلومات عالية الحساسية **(محروس وصالح، ٢٠٢٢ ,.Lois et al., 2021;** ويشير تقرير **(IIA, 2022)** إلى أن مشكلة الأمن السيبراني تتمثل في تأرجح المساءلة بين عدة أطراف، حيث لا تستطيع المنشأة الحكم على جهة معينة تكون هي المتسببة في حدوث مشاكل الأمن السيبراني.

وفي هذا الشأن فإن المراجعة الداخلية تستطيع من خلال خدمات التأكيد وتقديم المشورة العمل على تحقيق التوازن والمساعدة في تحديد المساءلة بشكل واضح، كما يمكن أن تقدم المراجعة الداخلية رؤيتها بشأن احتمالات زيادة مخاطر انتهاك البيانات والاختراقات الأمنية الناتجة عن تخفيف أو زيادة الضوابط الرقابية، هذا بالإضافة إلى قدرة المراجعة الداخلية على تقييم مدى الوعي بالأمن السيبراني وفعالية البرامج التدريبية للموظفين في ظل بيئة تكنولوجيا المعلومات، بالإضافة إلى مساهمتها البناءة في تحسين قدرة المنظمة على فهم مخاطر الأمن السيبراني وتحديد الإستراتيجيات اللازمة للحد من هذه المخاطر ومدى فعالية إدارة مخاطر الأمن السيبراني **(KPMG, 2020 b)**.

والجدير بالذكر أن عام ٢٠٢٣ قد شهد تطورات كبيرة تتعلق بالأمن السيبراني على المستوى الدولي ومدى تأثيره على جميع أنواع منظمات الأعمال، وسوف يتطلب فهم هذه التطورات وتأثيراتها المتعددة مزيدا من الوقت والجهد، ويأتي في مقدمة هذه التطورات المقترحات التنظيمية الصادرة عن لجنة تداول الأوراق المالية والبورصات الأمريكية **"U.S. Securities and Exchange Commission" (SEC)**، والتي تضمنت مطالبة منظمات الأعمال المدرجة بالسوق الأمريكية بالإفصاح عن سياسات وإجراءات واستراتيجيات الحوكمة ومعرفة مجلس الإدارة وخبراته في مجال الأمن السيبراني. **(IIA, 2022 b)**، وسوف تمثل هذه التطورات مجالا جديدا لوظائف المراجعة الداخلية، والتي يمكن أن تؤدي دورا محوريا في مواجهة مخاطر الأمن السيبراني، ولا شك أن التعامل مع مخاطر الأمن السيبراني لا يتسق معه تطبيق المنهج التقليدي للمراجعة الداخلية، كما أنه يتطلب توافر عدة مقومات جديدة تدعم الملاءة المهنية للمراجع الداخلي بما يتوافق مع بيئة الأعمال المتغيرة وسرعة وتعقيد الهجمات السيبرانية.

وفي سبيل تحقيق ذلك يتعين على المراجع الداخلي إمكانية استخدام تقنيات وبرمجيات تخدم الإدارة وتقدم لها ما يمكنها من الحفاظ على جودة الأنظمة المعلوماتية الإلكترونية في الوقت المناسب والحد من المخاطر التي يمكن أن تواجهها، حيث أن حماية المعلومات الإلكترونية تعتبر جزء أصيل من حماية للمنشأة، وتمثل عملية المراجعة الداخلية للأمن السيبراني عملية فحص أنظمة الرقابة الأمنية المطبقة في كيانات الأعمال للتأكد من توفر المعلومات وسلامتها وحماية سريتها، والجدير بالذكر أن نطاق المراجعة الداخلية للأمن السيبراني يشتمل على كافة أنظمة الرقابة وممارسات الإدارة والحوكمة والمخاطر والالتزام الرقابي المطبق على مستوى كيانات الأعمال **(عبد الرحيم، ٢٠٢٠)** .

وفي سياق متصل فإن الانهيارات التي لحقت بالكثير من المنشآت على المستوى الدولي وما تبعه من ضياع حقوق المساهمين والمستثمرين وأصحاب المصالح الأخرى انعكس على ضياع الثقة في جودة وأمن المعلومات الإلكترونية، وقد ساعد ظهور التقنيات الجديدة إلى تغيير الطريقة التي تدار بها الأنشطة المختلفة داخل الشركات على سبيل المثال في الوقت الحاضر يعرض الأمن السيبراني سمعة المنشآت إلى الخطر وكذلك استقرارها التشغيلي والمالي مما دعا إلى الحاجة إلى حماية متقدمة للبيانات وهذا يخلق عدداً كبيراً من التحديات الجديدة لمهنة المراجعة **(Bresciani et al., 2021)**، لذلك كان لابد من الاهتمام بتطبيق الحوكمة الرقمية (حوكمة تكنولوجيا المعلومات) وذلك حتى يتثنى للمنشأة التأكد من تحقق الأهداف المخطط لها عن طريق تفعيل دور فريق المراجعة الداخلية في الحد من مخاطر الأمن المعلوماتي.

وفي سياق ما تقدم فإن استخدام التكنولوجيا المتطورة يمثل في ذات الوقت تحديا كبيرا للمراجع الداخلي، حيث يرافق استخدامها تهديدات ومخاطر، الأمر الذي يترتب عليه أن يتمتع المراجع الداخلي بالملاءة المهنية المناسبة بأبعادها المختلفة والتي تتمثل في قدرته على الوفاء بالتزاماته ومسئولياته تجاه إدارة المنشأة، وذلك من خلال مجموعة من الآليات والتي تتمثل في وجود فريق عمل متكامل، نظام فعال لرقابة الجودة، نظام للتدريب والتعليم المهني المستمر، وقد حرصت بيئات الأعمال في

الآونة الأخيرة إلى الاستفادة من بيئة تكنولوجيا المعلومات والاتصالات، وتوجه منظمات الأعمال نحو تقنيات التحول الرقمي للاستفادة منها خاصة في مجال المحاسبة والمراجعة كنتيجة للثورة الصناعية الرابعة وتأثيراتها الكبيرة على بيئة الأعمال حيث لم تعد بيئة التحول الرقمي خياراً بل أصبحت ضرورة ملحة للتطور.

وفي ضوء ما تقدم يمكن بلورة مشكلة البحث في التساؤل الرئيسي التالي: ما هو الدور التأثيري للحوكمة الرقمية كمتغير وسيط في العلاقة بين الملاءة المهنية للمراجع الداخلي وجودة الأمن السيبراني؟ ويتفرع من هذا السؤال الأسئلة الفرعية التالية:

١- ما المقصود بالحوكمة الرقمية؟ وما هي أهدافها وأهم متطلباتها وأبعادها؟
٢- ما هي محددات وأبعاد الملاءة المهنية للمراجع الداخلي؟
٣- ما المقصود بالأمن السيبراني؟ وما هي آليات الحد من المخاطر المتعلقة به؟
٤- ما هي العلاقة بين الملاءة المهنية للمراجع الداخلي وجودة الأمن السيبراني في ضوء الحوكمة الرقمية؟
٥- هل يمكن اختبار العلاقة السابقة تطبيقياً على مجموعة من الشركات المقيدة بالبورصة المصرية؟

أهداف البحث:

يهدف هذا البحث إلى تحقيق هدف عام وهو اختبار الدور التأثيري للحوكمة الرقمية كمتغير وسيط في العلاقة بين الملاءة المهنية للمراجع الداخلي وجودة الأمن السيبراني، ويتحقق هذا الهدف العام من خلال مجموعة من الأهداف الفرعية التالية:

١- استعراض مفهوم بالحوكمة الرقمية وأهدافها وأهم متطلباتها وأبعادها.
٢- توضيح محددات وأبعاد الملاءة المهنية للمراجع الداخلي.
٣- تعريف الأمن السيبراني وعرض لأهم آليات الحد من المخاطر المتعلقة به.
٤- دراسة وتحليل العلاقة بين الملاءة المهنية للمراجع الداخلي وجودة الأمن السيبراني في ضوء الحوكمة الرقمية.
٥- اختبار العلاقة السابقة تطبيقياً على مجموعة من الشركات المقيدة بالبورصة المصرية.

أهمية البحث:

تنبع أهمية البحث من تناوله لقضية بحثية حيوية ومعاصرة وهي الدور التأثيري للحوكمة الرقمية كمتغير وسيط في العلاقة بين الملاءة المهنية للمراجع الداخلي وجودة الأمن السيبراني، ومن ثم تتمثل أهمية البحث في:

أولا: الأهمية العلمية:

١- مواكبة التطورات الحديثة في مجال البحوث المحاسبية التي تركز اهتمام الباحثين والأوساط المهنية على أهمية الملاءة المهنية للمراجعة الداخلية ودورها في تحقيق جودة الأمن السيبراني والحد من المخاطر المتعلقة به في ضوء الحوكمة الرقمية.
٢- عدم وجود معيار محاسبي مصري يعكس دور الملاءة المهنية للمراجعة الداخلية في ظل الحوكمة الرقمية يهدف إلى تحقيق جودة الأمن السيبراني في بيئة الأعمال المصرية، وبالتالي تتمثل القيمة العلمية لهذا البحث في ندرة الدراسات المحاسبية في مجال البحث في بيئة الأعمال المصرية. مما يستدعي حاجة المكتبة العلمية العربية لمثل هذا النوع من الدراسات.

ثانيا: الأهمية العملية:

١- تقديم معلومات للقائمين على مهنة المحاسبة والمراجعة تساعدهم في بناء وتطوير المعايير اللازمة لتفعيل الملاءة المهنية للمراجع الداخلي بهدف تحقيق جودة الأمن السيبراني والحد من مخاطره.
٢- سوف تساعد نتيجة البحث على تعميق فهم المسؤولين والشركات المقبلة على تطبيق الحوكمة الرقمية بضرورة مراعاة العوامل المحددة للدور الفعال للملاءة المهنية للمراجع الداخلي في تحقيق جودة الأمن السيبراني والحد من مخاطرة.
٣- توفير دليل تطبيقي على الدور التأثيري للحوكمة الرقمية كمتغير وسيط في العلاقة بين الملاءة المهنية للمراجع الداخلي وجودة الأمن السيبراني.

منهج البحث:

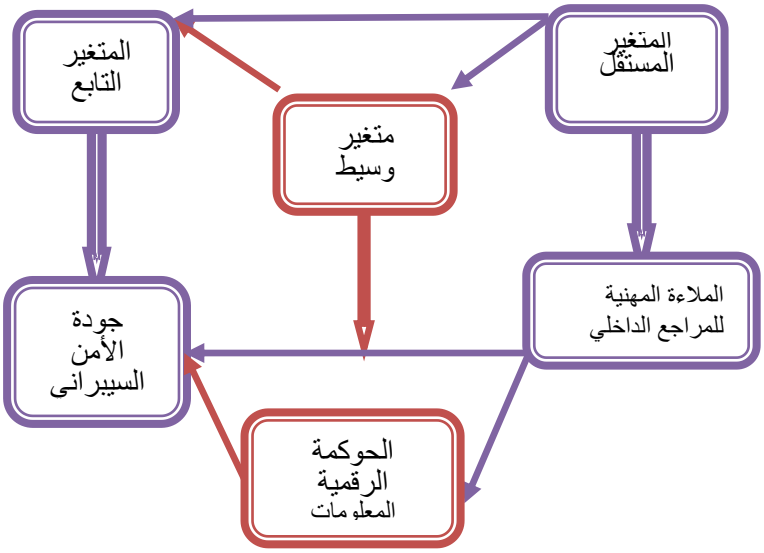
اعتمد الباحث على كل من المنهج الاستقرائي والاستنباطي لتحليل وتقييم الدراسات السابقة في مجال البحث والخروج منها باستنتاجات منطقية تساعد على دراسة وتحليل العلاقة بين الملاءة المهنية للمراجع الداخلي في ظل الحوكمة الرقمية بهدف تحقيق جودة الأمن السيبراني والحد من المخاطر المتعلقة به، مستخدما في ذلك اسلوب الدراسة النظرية المكتبية والدراسة الميدانية على عينة من الخبراء والمختصين في مجالي المراجعة الداخلية وحوكمة تكنولوجيا المعلومات في شركات تكنولوجيا المعلومات بالقرية الذكية، وشركات المساهمة المقيدة أوراقها المالية بالبورصة، ومكاتب المحاسبة والمراجعة الكبرى، والسادة أعضاء هيئة التدريس بالجامعات المصرية، وذلك لمعرفة آرائهم فيما يتعلق بالملاءة المهنية للمراجع الداخلي في ظل الحوكمة الرقمية بهدف تحقيق جودة الأمن السيبراني والحد من المخاطر المتعلقة به.

نموذج البحث:

يهدف نموذج البحث إلى تحديد العلاقة التي تربط المتغيرات بعضها البعض، وتتمثل المتغيرات الأساسية في الملاءة المهنية للمراجع الداخلي **كمتغير مستقل**، وجودة الأمن السيبراني هي **المتغير التابع**، بينما تعتبر الحوكمة الرقمية **متغير وسيط** للعلاقة بين الملاءة المهنية للمراجع الداخلي وجودة الأمن السيبراني، ولإثبات العلاقة السابقة لابد من التأكد من:

١- إن المتغير المستقل (الملاءة المهنية للمراجع الداخلي) يوثر على المتغير التابع (جودة الأمن السيبراني).
٢- إن المتغير المستقل (الملاءة المهنية للمراجع الداخلي) يوثر على المتغير الوسيط (الحوكمة الرقمية).
٣- إن المتغير الوسيط (الحوكمة الرقمية) يوثر على المتغير التابع (جودة الأمن السيبراني).
٤- إن المتغير المستقل (الملاءة المهنية للمراجع الداخلي) يوثر على المتغير التابع (جودة الأمن السيبراني) بوجود المتغير الوسيط (الحوكمة الرقمية)، وتكون الوساطة كلية إذا لم يعد للمتغير المستقل تأثيرا على المتغير التابع بعد تحكم المتغير الوسيط، أما إذا انخفض التأثير المباشر من المتغير المستقل إلى المتغير التابع ولكنه لا يزال مختلفاً عن الصفر عند إدخال المتغير الوسيط تكون الوساطة جزئية.

وانسجاما مع أهداف البحث ومشكلته، فقد تمت صياغة نموذجا يمثل متغيرات البحث من خلال الشكل التالي:



الشكل رقم (١) نموذج البحث
المصدر: إعداد الباحث.

حدود البحث:

تحقيقاً لهدف البحث يقتصر هذا البحث على معرفة دور الملاءة المهنية للمراجع الداخلي في ظل الحوكمة الرقمية لتحقيق جودة الأمن السيبراني، ولذلك لن يتناول البحث الأبعاد الاقتصادية والتنظيمية والقانونية للحوكمة الرقمية لأنها تخرج عن هدف البحث، كما لن يتناول البحث دور لجان المراجعة في تطبيق الحوكمة الرقمية، وكذلك لن يتناول الباحث موضوع الإسناد الخارجي أو التعاقد المشترك لمهام وظائف المراجعة الداخلية، هذا ويخرج عن نطاق البحث أيضا معايير المراجعة الداخلية وميثاق السلوك الأخلاقي إلا بالقدر الذى يخدم البحث.

خطة البحث:

انطلاقا من أهمية البحث وتحقيقا لأهدافه، وفي ضوء مشكلته وحدوده فإن البحث سوف يستكمل - بعد عرض الإطار العام للبحث - على النحو التالي:

المحور الأول: استعراض الدراسات السابقة واشتقاق الفروض.

المحور الثاني: الحوكمة الرقمية (المفهوم – الأهداف – المتطلبات والأبعاد).

المحور الثالث: محددات وأبعاد الملاءة المهنية للمراجع الداخلي.

المحور الرابع: مفهوم الأمن السيبراني وأهم آليات الحد من المخاطر المتعلقة به.

المحور الخامس: العلاقة بين الملاءة المهنية للمراجع الداخلي وجودة الأمن السيبراني في ضوء الحوكمة الرقمية.

المحور السادس: الدراسة التطبيقية (الميدانية).

النتائج والتوصيات والتوجهات البحثية المستقبلية.

المراجع.

المحور الأول: استعراض الدراسات السابقة واشتقاق الفروض.

يتناول هذا الجزء من البحث الأدبيات السابقة والتي تناولت متغيرات البحث المستقلة والتابعة، بهدف الوصول إلى مدى توافر أدلة على العلاقة بينها وبما يمكن من التوصل إلى النماذج البحثية وتطوير فروض الدراسة، ويمكن للباحث استعراض ذلك على النحو التالي:

أشارت دراسة **(Betti & Sarens, 2021)** إلى كيفية الوصول للفهم العميق حول طبيعة تطور وظيفة المراجعة الداخلية في بيئة الأعمال الرقمية، وقد انتهت هذه الدراسة إلى أن بيئة الأعمال الرقمية تُؤَثر على وظيفة المراجعة الداخلية من حيث نطاق هذه المراجعة، حيث إنه من المتوقع أن تُزيد بيئة الأعمال الرقمية من جودة عملية تخطيط المراجعة الداخلية، والمعرفة الرقمية المطلوبة، بالإضافة إلى زيادة الطلب على الأنشطة الاستشارية التي يؤديها المراجعون الداخليون، هذا بالإضافة إلى أن بيئة الأعمال الرقمية تدعم ممارسات العمل للمراجعين الداخليين في مهامهم اليومية.

وفي ذات الإطار فقد استهدفت دراسة **(شحاتة، ٢٠٢٠)** تحليل طبيعة وأهمية المراجعة الداخلية في ظل آليات التحول الرقمي كأحد تطبيقات تكنولوجيا المعلومات، والكشف عن أهم مجالات الفحص التي يجب أن تركز عليها إدارة المراجعة الداخلية ولجان المراجعة للتحقق من كفاءة وفعالية استراتيجيات التحول الرقمي، وتحديد انعكاسات التحول الرقمي على تعزيز المساءلة والشفافية وتحسين الأداء الحكومي بالبيئة المصرية، وقد توصلت الدراسة إلى العديد من النتائج كان أهمها: أن خطة المراجعة الداخلية الشاملة القائمة على المخاطر يجب أن تحمل في طياتها طرق وسبل التعامل مع آليات التحول الرقمي، هذا وقد انتهت الدراسة إلى أن المراجعة الداخلية الناجحة والقائمة على المخاطر لابد أن تتبني مجموعة متنوعة من الأفكار والخبرات لتقييم المخاطر التي تقترن بتنفيذ هذه التقنيات عبر المنصات الرقمية والمواقع الإلكترونية، كما أن المراجعة الداخلية تمارس دور استشاري فعال لقيادة القيمة الرقمية من خلال تحديد المخاطر الخاصة بالمنظمة بشكل استباقي وتقديم المشورة الاستراتيجية وخدمات القيمة المضافة بشأنها.

كما استهدفت دراسة **(Lois et. al, 2020):** تحديد وفحص التقنيات التكنولوجية التي يمكن استخدامها في تنفيذ المراجعة المستمرة من منظور مهنة المراجعة الداخلية في ظل التَحَوُّل الرقمي، والمخاطر، والتحديات التي تواجه تنفيذ مدخل المراجعة المستمرة في ظل التَحَوُّل الرقمي، وقد أسفرت نتائج الدراسة إلى أن التقدم في مجال تكنولوجيا المعلومات يتطلب ضرورة إنشاء نظام مراجعة رقمية بشكل فعال، من خلال التركيز على تحقيق ثلاثة أهداف رئيسة تتمثل في: وجود التدابير أو الإجراءات اللازمة لحماية البيانات الشخصية للعملاء، وتجنب الهجمات الإلكترونية، وتأهيل وتدريب مراجعي الحسابات على العمل في بيئة المراجعة المستمرة من منظور المراجعة الداخلية لضمان أمن وسلامة البيانات، بالإضافة إلى تنفيذ مهام المراجعة الإلكترونية في ظل التَحَوُّل الرقمي على أكمل وجه.

وفي سياق متصل فقد سعت دراسة **(صدقي، ٢٠٢٢)**، إلى تحليل مجموعة التحديات التي تواجه المراجع الداخلي وانعكاساتها على هيكل الرقابة الداخلية في ظل الرقمنة، وقد أوضحت نتائج الدراسة النظرية أن المهارات الرقمية للمراجع الداخلي تجعله قادر على دعم مبادئ الإفصاح والشفافية والمساءلة من خلال ما يقوم به من أعمال الرقابة ومهام المراجعة وما ينتج عنها من معلومات تتاح في الوقت المناسب، وبالشكل الملائم لأصحاب المصالح المختلفة، وأن عدم توافر المهارات والمعرفة والثقافة والخبرة التكنولوجيا لدى المراجعين الداخلين المسئولين عن أداء

عمليات المراجعة الداخلية يمكن أن يؤدى إلى عواقب سلبية، كما تتركز التحديات التي تواجه مهنة المراجعة الداخلية في الفترة الأخيرة في تلك التي نتجت عن التطور الهائل والسريع في تكنولوجيا المعلومات والاتصالات، وأبرزها تلك المتعلقة بالبيانات الضخمة وتحليلاتها وبالحوسبة السحابية، كما نفس الدراسة من خلال نتائج الجزء الميداني إلي، أنه توجد علاقة ارتباط موجبة قوية ذات دلالة إحصائية بين التحديات التي يواجها المراجع الداخلي وهيكل الرقابة الداخلية، كما توجد علاقة ارتباط موجبة قوية ذات دلالة إحصائية بين هيكل الرقابة الداخلية والتحول الرقمي، واخيراً توجد علاقة ارتباط موجبة قوية ذات دلالة إحصائية بين التحديات التي يواجها المراجع الداخلي والتحول الرقمي.

وفي إطار متصل فقد تناولت دراسة **(أبو الخير،٢٠٢٣):** اختبار أثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الاستقرار المالي في البنوك الإلكترونية، واعتمدت الدراسة على مسح ميداني لعينة من مسؤولي المراجعة الداخلية، ومسؤولي تكنولوجيا المعلومات ومسؤولي إدارة المخاطر في البنوك الإلكترونية المقيدة بالبورصة المصرية، وتوصلت الدراسة إلى العديد من النتائج وكان أهمها أن التطور الحادث في المخاطر السيبرانية يحفز المنشآت المالية على البحث المستمر والمكثف نحو اتخاذ إجراءات وقائية من تلك المخاطر، من خلال لوائح تجعل تلك الإجراءات أكثر وضوحاً أمام مجالس إدارات تلك البنوك، الأمر الذي يؤدي إلى دعم الاستقرار المالي في تلك البنوك، كما أوصت الدراسة بضرورة تكثيف التوعية بثقافة الأمن السيبراني لدى المتعاملين بقطاع البنوك بهدف تفهم الضوابط والتعليمات الخاصة بأمن نظم المعلومات والفضاء السيبراني.

وقد استهدفت دراسة **(Kalpesh & Saurabh,2019)** التركيز على العناصر التي يؤثر فيها التحول الرقمي على جودة المراجعة الداخلية، وقد خلصت هذه الدراسة إلى أن المؤسسات الخاصة والعامة تحتاج لمواكبة التغييرات المحيطة للبقاء والاستمرار وتحسين جودة الخدمات المقدمة مع وجود دور فعال لأنشطة المراجعة الداخلية فيما يخص التحول الرقمي، كما أكدت الدراسة على أن وجود الإدارة الرقمية يساعد المراجعة الداخلية على التطور والوصول لأعلى مستويات الكفاءة والفعالية في الأداء من خلال تحسين مستويات الدقة وخفض الخطأ البشري وإدارة المخاطر.

التعليق على الدراسات السابقة واستعراض الفجوة البحثية وصياغة الفروض:

يتضح من تحليل الدراسات السابقة ما يلي: -

١. يحظى موضوع التحول الرقمي بالكثير من اهتمامات الباحثين والجهات التنظيمية في كثير من دول العالم، لما له من تأثير على مجموعة من المتغيرات الداخلية والخارجية لجميع المنشآت، كما لاقى موضوع دور المراجع الداخلي وملاءته المهنية ووضعه في المستوى التنظيمي، ومدى تفعيل هذا الدور في تحقيق جودة الأمن السيبراني الكثير من الاهتمامات سواء على المستوى المحلي أو المستوى الدولي.
٢. أن هناك ندرة في مجموعة الأدبيات المحاسبية ذات الصلة التي بحثت في العلاقة بين الملاءة المهنية للمراجع الداخلي وجودة الأمن السيبراني من خلال الحوكمة الرقمية للمنشآت، الأمر الذي دفع الباحث إلى السعي نحو دراسة العلاقة بين متغيرات الظاهرة البحثية محل الدراسة.

وبناء على استقراء وتحليل الأدبيات السابقة ذات العلاقة وطرح الفجوة البحثية يرى الباحث اشتقاق فروض البحث على النحو التالي:

الفرض الأول: "لا توجد علاقة ذات دلالة إحصائية بين الحوكمة الرقمية والملاءة المهنية للمراجع الداخلي".

الفرض الثاني: " لا توجد علاقة ذات دلالة إحصائية بين الحوكمة الرقمية وجودة الأمن السيبراني".

الفرض الثالث: " لا يوجد تأثير معنوي للحوكمة الرقمية على العلاقة بين الملاءة المهنية للمراجع الداخلي وجودة الأمن السيبراني".

المحور الثاني: الحوكمة الرقمية (المفهوم – الأهداف – المتطلبات والأبعاد).

٢/ ١ المفهوم:

تعبر الحوكمة الرقمية عن مصطلحين الأول منها: **الحوكمة** والذي يمثل مجموعة من القواعد والأنظمة الصادرة التي تسعى بشكل مباشر إلى تنظم العلاقات بين أصحاب المصالح في المنشأة وذلك لضمان حقوق جميع الأطراف وتعزيز الرقابة والإفصاح والشفافية والحد من ممارسات التلاعب والغش، والارتقاء بقيمة المنشأة **(با ناصر والصائغ، ٢٠٢٠)**، بينما يعني لفظ **الرقمية** دمج التكنولوجيا المتقدمة في تحقيق المزيد من الشفافية وإمكانية تتبع سلاسل القيم لخدمة المستفيدين بطريقة أكثر مسؤولية واعمق استدامة، ودعم اتخاذ القرارات التي تستند إلى موضوعية ووفرة البيانات **(Kumar, 2024)**.

وفي هذا السياق فقد أشارت دراسة **(رشوان وأبو رحمة، ٢٠٢٠)** إلى أن الحوكمة الرقمية تتمثل في مجموعة من الضوابط والإجراءات التي تهدف إلى ضبط منظومة بيئة العمل الداخلية والخارجية المتأثرة بالتحول الرقمي، بهدف وضع خارطة طريق لتسهيل الأعمال بشكل يواكب التطور، ويضمن توازناً متناسباً بين أصحاب المصالح لتحقيق الإستراتيجيات والأهداف المرغوبة بشكل متواصل، مع خلق فرص النمو للمنشأة، حيث أن الحوكمة الرقمية تدعم مجالات الاستثمار وتساهم في تحقيق الميزة التنافسية المستهدفة.

وفي إطار متصل فقد تناولت دراسة **(Brous, 2015)** مفهوم الحوكمة الرقمية بأنها نظام قادر على تحديد الأدوار والمسئوليات، ووضع الخطط التنفيذية وكيفية اتخاذ القرار الرقمي للمنشأة، وتشمل هذه الأدوات والمسئوليات الإشراف على تصميم وتطوير الخدمات الرقمية في كافة الأنشطة المتعلقة بالمنشأة، وتقديم أداء هذه الخدمات بقدر عالٍ من الفعالية والكفاءة لتقنية المعلومات والتي تهدف إلى تمكين المنشأة من تحقيق أهدافها، كما أشارت جمعية تحقيق وضبط أنظمة المعلومات **Information Systems Audit and Control Association (ISACA)** لمفهوم الحوكمة الرقمية على أنه إطار عام لتطبيق حوكمة التحول الرقمي في المنشآت، يشتمل على مجموعة من العمليات والمعايير والموارد لتكنولوجيا المعلومات، بحيث يمثل وسيلة لتقديم المساعدة لمستخدمي التكنولوجيا والقائمين على إدارتها لفهم النظم التكنولوجية الرقمية في منظماتهم وإدارة المخاطر المتعلقة بها، وذلك على النحو الذي يسهم في حماية الموارد المالية ويضمن تحقيق الفعالية والشفافية والمسائلة وكفاءة المنشأة **(Kwilinski et al.,2023)**.

وبناء على ما جاء بالتعريفات السابقة يمكن للباحث تعريف الحوكمة الرقمية بأنها استخدام الإمكانات والوسائل التي توفرها تكنولوجيا المعلومات والاتصالات الحديثة في تطبيق مبادئ الحوكمة من أجل تحقيق أهدافها، فالحوكمة الرقمية تعمل على ضبط أعمال المنشآت، وترفع من مستوى أدائها وتضمن المشاركة والشفافية والمساءلة مما يحسن من مستوي أنشطة تلك المنشآت.

كما يؤكد الباحث على أنه في ضوء المفاهيم المتعددة للحوكمة الرقمية فإنها تمثل جزء أصيل من مهام وأهداف الرقابة الداخلية في المنشأة، والتي تعد المراجعة الداخلية جزءاً منها لذلك فإن الحوكمة الرقمية وما تشتمل عليه من بعد حوكمي وبعد رقمي وآخر متعلق بضبط المخاطر فإن تلك الأبعاد السابقة تمثل ركائز أساسية من رفع الأداء المهني والملاءة المهنية للمراجع الداخلي.

٢/٢ الأهداف:

تتعدد الأهداف من وراء استخدام الحوكمة الرقمية حيث أنها تعمل بشكل كبير على خفض حدة البيروقراطية في أداء الأعمال، والعمل على تجميع كافة الخدمات والمعلومات ذات الأهمية لأصحاب المصالح بما يمكن من الاستفادة منها بطريقة سهلة، وتتمثل أهم الأهداف التي تسعى الحوكمة الرقمية إلى تحقيقها في الآتي: **(Manoharan et al.,2022; Tiwari,2022, Hanisch, M et al., 2023)**

٢/٢/١ تقديم الخدمات لأصحاب المصالح بطريقة سريعة ومنخفضة التكاليف.

٢/٢/٢ توفير المعلومات عن كافة التعاملات بين المنشأة وعملائها على شبكة الإنترنت.

٢/٢/٣ تحديد متطلبات الحصول على الخدمات والنماذج المطلوبة بما يمكن من استكمالها قبل الذهاب لمكان أداء الخدمة، ومن ثم تخفيض الوقت والجهد اللازم لأداء الخدمة.

٢/٢/٤ الارتقاء بثقافة ووعي العاملين في الإدارات المختلفة للمنشأة من خلال تشجيعهم على استخدام وسائل التكنولوجيا الحديثة.

٢/٢/٥ توفير مناخ ملائم للاستثمار بما يحد من المعوقات والإجراءات التي تحول دون جذب المستثمرين، وبما يوفر عامل جذب للمنشآت العاملة في مجال التكنولوجيا.

٢/٢/٦ رفع كفاءة أداء المؤسسات والإعداد للاندماج في النظام العالمي لمواكبة نظم المعلومات الحديثة المتبعة.

٢/٢/٧ تحقيق الشفافية من خلال إتاحة المعلومات بصورة متكافئة لكافة المتعاملين.

وفي ضوء ما تقدم يرى الباحث أن الحوكمة الرقمية تساهم بشكل كبير في تحقيق الكفاءة والفعالية في تقديم الخدمات للمستفيدين والاستغلال الأمثل للموارد، والعمل على ضمان تدفق المعلومات بدقة وكفاية وتوقيت ملائم وجاهزية مستمرة، هذا علاوة على خلق البيئة والمناخ التنظيمي الملائم للبحث والتطوير الإداري المتواصل، هذا بالإضافة إلى خلق بيئة تعليمية تعتمد بشكل كبير على النظم الإلكترونية المتقدمة بما يضمن تقديم آليات فعالة وداعمة لاتخاذ القرارات.

٢/٣ المتطلبات والأبعاد:

أكدت دراسة كل من **(Fatima et al.,2021 ;Idzi &Gornes,2022)** على أن أهم متطلبات الحوكمة الرقمية يمكن تلخيصها في الآتي:

٢/٣/١ **الامتثال للتنظيمات والقوانين:** حيث يجب على كل المنشآت الالتزام بالقوانين واللوائح الخاصة بالحوكمة الرقمية وضمان أن تكون جميع الأنشطة الرقمية مطابقة للمعايير الأخلاقية والقانونية.

٢/٣/٢ توفير الخصوصية: حيث يجب حماية خصوصية المستخدمين والعملاء والعاملين من استغلال بياناتهم الشخصية واستخدامها بطريقة غير مشروعة أو غير مرغوب فيها وذلك عن طريق تنظيم جمع البيانات واستخداماتها وتخزينها وحذفها ومشاركتها.

٢/٣/٣ توفير الشفافية: حيث يجب على المنشآت الالتزام بالشفافية في جميع العمليات الرقمية وذلك عن طريق الكشف عن المعلومات المتعلقة بالبيانات المستخدمة ومصادرها وطرق جمعها واستخدامها ومنح الوصول إليها.

٢/٣/٤ توفير الأمان: حيث يجب حماية الأنظمة والتطبيقات والبيانات الرقمية من الهجمات السيبرانية والاختراقات والقرصنة والتشويش وذلك عن طريق تبني التدابير الأمنية اللازمة وإدارة المخاطر بشكل فعال.

كما يمكن استعراض أبعاد الحوكمة الرقمية وذلك في ضوء ما تناولته دراسة كل من **(Hanisch et al.,2023; Shang et al. ,2023; Bezerra et al.,2023)** على النحو التالي:

- **المشاركة الرقمية:** والتي تتمثل في إتاحة الفرصة أمام جميع المشاركين والطراف ذات الصلة للمشاركة في اتخاذ القرارات وإتاحة الفرصة لهم بإبداء آرائهم وأفكارهم وذلك من خلال تسهيل وصولهم إلى المعلومات باستخدام تكنولوجيا المعلومات والاتصالات لتقديم آرائهم ومقترحاتهم.
- **الشفافية الرقمية:** حيث تتمثل في الوضوح بعيداً عن الغموض والسماح لأصحاب المصالح بمعرفة الحقيقة دون إخفاء أو تضليل، والإفصاح عنها بوضوح من خلال وسائل تكنولوجيا المعلومات والاتصالات.
- **المساءلة الرقمية:** والتي تعبر عن الوسيلة التي من خلالها تحمل الأفراد مسؤولية أعمالهم مما يؤدي إلى اطمئنان أصحاب العلاقة بأن الأمور تجري للصالح العام.
- **المراجعة الرقمية:** حيث أنه يمثل النشاط المستخدم للتأكد من أن عمليات المنشأة تسير وفق المعايير المحددة والمراجعة الفعالة بأسرع وقت وأقل جهد وتكلفة.

وفي نهاية هذا المحور يؤكد الباحث على أن الحوكمة الرقمية من خلال استثمار تكنولوجيا المعلومات تمثل مضافة للمنشآت، فهي تعزز مكانتها وتكسبها ثقة أصحاب العلاقة وتزيد من قدراتها التنافسية من خلال المشاركة الفعالة والشفافية في تقديم المعلومات والمساءلة، كما أنها تزيد من كفاءة الإدارة والتزامها بالقوانين، علاوة على كونها تمثل أداة فعالة للرقابة على أداء المنشآت بما يدعم تطوير أدائها ويزيد من جودة خدماتها، وهذا بالطبع يتطلب من إدارة المنشأة أن تسعى بشكل كبير إلى دعم الملاءة المهنية للمراجعين الداخليين بصفتهم المعنيين بأمور كثيرة من مبادئ وأهداف الحوكمة الرقمية، وهذا ما سوف يسعى الباحث إلى تناوله في المحور القادم من هذا البحث.

المحور الثالث: محددات وأبعاد الملاءة المهنية للمراجع الداخلي.

أدت التطورات السريعة والمتلاحقة في بيئة الأعمال إلى تطور مفهوم وأهداف وظيفة المراجعة الداخلية، حيث تحولت تلك الوظيفة من الأدوار التقليدية التي كانت تشتمل على حماية أصول المنشاة، التأكد من تدفق المعلومات بكفاءة وفعالية، تقييم نظام الرقابة الداخلية والتأكد من مدى الالتزام بالسياسات الإدارية الموضوعة، إلى أدوار جديدة تعتمد على تقييم وإدارة المخاطر، تقييم مدى الالتزام بأبعاد ومحددات الحوكمة، وكذلك تقديم الخدمات الاستشارية للمستويات الإدارية المختلفة دعماً لتطوير وتحسين الأداء والعمل على إضافة قيمة للمنشأة.

والجدير بالذكر أن التحول في تلك الأدوار السابقة أصبح يعتمد على مجموعة من المقومات التي تستهدف تعزيز الملاءة المهنية للمراجع الداخلي حتى يتمكن من مباشرة وإتمام مهامه بنجاح في ظل تلك التحولات، وبالشكل الذي يتوافق مع التطورات والتنافسية في بيئة الأعمال، لذلك شهدت الفترة الأخيرة تطوراً تدريجياً واضحاً في أنشطة المراجعة الداخلية نظراً لمكانتها الهامة في نظام الرقابة الداخلية، حيث أنها أصبحت شريكاً إستراتيجياً يدعم قيمة المنشأة ويحد من المخاطر المرتبطة بكافة أنشطة تلك المنشأة وخاصة فيما يتعلق بأنشطة الأمن السيبراني.

وفي هذا الإطار فقد أكدت الكثير من الدراسات على تعدد مقومات تعزيز الملاءة المهنية للمراجع الداخلي والتي تتمثل في: وجود فرق عمل تتوافر لديها المهارات والمعرفة الأساسية اللازمة والتي تساهم بشكل كبير في دعم جودة مهام المراجعة الداخلية، وجود نظام متكامل للرقابة على الجودة، هذا بالإضافة إلى توافر مجموعة من مقومات التدريب والتعليم المهني المستمر، حيث أن توافر تلك المقومات يساهم بشكل كبير في دعم الملاءة المهنية لوظيفة المراجعة الداخلية **(أحمد، ٢٠٢١)**، وفي ذات الإطار فإن مفهوم الملاءة المهنية لوظيفة المراجعة الداخلية يعتمد بشكل أساسي على قدرة أعضاء فريق المراجعة الداخلية على الوفاء بالتزاماتهم تجاه المنشأة وأيضاً تجاه الأطراف المستفيدة، وذلك من خلال الالتزام بالمعايير المهنية، قواعد وآداب السلوك المهني والذي ينتج عنه تأدية تشكيلة خدماتها بمستويات مرتفعة من الجودة، خاصة في ظل مجموعة التحديات التي أفرزتها بيئة الأعمال الحديثة **(Chang et al., 2019).**

ولقد أكدت دراسة **(شحاتة وآخرون، ٢٠٢٣)** على أن مصطلح الملاءة المهنية في مصر ظهر مؤخراً مع بداية ظهور الاهتمام بمفاهيم الرقابة على منشآت المحاسبة والمراجعة، حيث قامت الهيئة العامة للرقابة المالية باتخاذ بعض الخطوات والتدابير والتي من شأنها تحسين الرقابة على أداء الشركات المقيدة بالبورصة المصرية، كما قامت الهيئة بعمل برامج تدريبية توعوية لمديري الأصول والأعضاء المنتدبين وإدارة المخاطر والرقابة الداخلية والمراجعة الداخلية ومكافحة غسيل الأموال تهدف إلى دعم الملاءة المهنية لتلك الأطراف المشاركة.

وفي ذات السياق فإن ضرورة وجود فريق عمل جماعي كأحد مقومات الملاءة المهنية للمراجعة الداخلية يعد من الأمور الهامة والأساسية في تحقيق هذا الهدف، ولقد أكدت دراسة كل من **(Cameran et al., 2018)** على أن العمل بشكل جماعي وتقسيم العمل بين أعضاء فريق المراجعة الداخلية يؤدي إلى مستويات دقة أعلى، والعمل والتفاعل بروح الفريق يترتب عليه جودة القرارات والتصرفات التي تصدر من هذا الفريق.

وفيما يتعلق بنظام رقابة الجودة والذي يعد مكون أساسي للملاءة المهنية لوظيفة المراجعة الداخلية، فقد تناول المعيار الدولي للمراجعة الداخلية **رقم ١٣٠٠** والخاص ببرامج توكيد وتحسين الجودة على أنه يجب على مدير المراجعة التنفيذي أن يقوم بإعداد برنامج يتعلق بتوكيد وتحسين الجودة، على أن يكون هذا البرنامج مصمم لتقييم أنشطة المراجعة الداخلية وفقاً للمعايير المهنية لتلك الأنشطة، مع مراعاة أن يشتمل كل جزء في هذا البرنامج على إضافة القيمة وتحسين أداء المنشأة **(Jiin et al.,2022)** .

واستكمالا لما سبق فقد تناولت دراسة **(Chen et al., 2020)** مجموعة من التوصيات والتي تؤكد في مجملها على أن التدريب المتخصص يمثل أهمية كبيرة نحو اكتساب المهارات المطلوبة في تفعيل أداء أنشطة المراجعة الداخلية مما يؤدي إلى إضافة قيمة للمنشأة، كما أوصت نفس الدراسة على أن البرامج التدريبية ذات الصلة بأنشطة المراجعة الداخلية يجب ان تشتمل على تنمية مجموعة من المهارات والقدرات لتلك الأنشطة لعل أهمها: مهارات خاصة بوضع الرؤية الاستراتيجية للمراجعة الداخلية، مهارات خاصة بالتحليل والتفكير الابتكاري، مهارات الاتصالات مع مجلس الإدارة ولجنة المراجعة، مهارات إدارة المخاطر وإضافة القيمة، ومهارات توصيل قيمة المراجعة الداخلية إلى المستخدمين.

هذا ويرى الباحث أن توافر تلك المقومات السابقة من شأنه ان يدعم بقوة قيمة المنشأة والتي تعد ركيزة نجاح اساسية نحو نجاح المنشآت واستمراريتها في ظل تداعيات التطورات السريعة والمتلاحقة، وخاصة في ظل تأكيد المعيار الدولي رقم **1200A** المتعلق بالمراجعة الداخلية على أنه في ظل ممارسة العناية المهنية الواجبة، فإنه يجب على المراجع الداخلي أن يأخذ في الاعتبار استخدام التكنولوجيا وأدوات تحليل البيانات.

المحور الرابع: مفهوم الأمن السيبراني وأهم آليات الحد من المخاطر المتعلقة به.

٤/١ مفهوم الأمن السيبراني:

أدى استخدام تقنيات وأدوات تكنولوجية جديدة في معظم المنشآت إلى ظهور مفهوم الأمن السيبراني، والذي يتمثل في حماية الأصول المعلوماتية من خلال معالجة التهديدات التي تتعرض لها هذه المعلومات التي يتم معالجتها وتخزينها ونقلها بواسطة أنظمة المعلومات المتداخلة بين الشبكات **(ISACA, 2017; أميرهم، ٢٠٢٢)**.

كما أكدت دراسة **(البغدادي , ٢٠٢١)** على أن مفهوم الأمن السيبراني يمثل ذلك النشاط الذي يعمل بشكل متواصل من أجل حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن الحد من الخسائر والأضرار الناتجة عن حدوث المخاطر المترتبة على الأمن السيبراني، بما يضمن تصحيح الأوضاع بشكل سريع حتى لا تتحول الأضرار إلى خسائر دائمة.

كما أشارت دراسة كل من **(Mendhurwar et al., 2021; Maleh, et ah 2021; Yusif,2021, Lois et al., 2021)** إلى أن الأمن السيبراني يمثل مجموعة الإجراءات والتقنيات المصممة لحماية أنظمة المعلومات والشبكات الإلكترونية من الهجمات السيبرانية والتهديدات الإلكترونية، بهدف حماية سرية المعلومات، وسلامتها، وسلامة الأنظمة والشبكات من الاختراقات، والتجسس، والتلاعب، والتدمير، والانقطاع عن الخدمة، وغيرها من الهجمات الإلكترونية.

وفي هذا الإطار يرى الباحث أن الأمن السيبراني هو مجموعة من الإجراءات والسياسات والتقنيات التي تهدف إلى حماية أنظمة المعلومات والشبكات الرقمية من الاختراقات والتهديدات الإلكترونية، بهدف الحماية من الاختراقات الإلكترونية والبرمجيات الخبيثة والاعتداءات السيبرانية الأخرى، وكذلك ضمان سرية المعلومات وسلامتها وتوفير استجابة فعالة في حالة حدوث أي اختراق، كما يؤكد الباحث على أن مفهوم الأمن السيبراني يمتد ليشمل عملية حماية مواقع تخزين البيانات والتقنيات المستخدمة لتأمينها، كما يتضمن حماية تكنولوجيا المعلومات والاتصالات والأجهزة والبرمجيات.

٤/٢ مخاطر الأمن السيبراني:

تتنوع مخاطر الأمن السيبراني بشكل كبير وتتضمن مجموعة واسعة من التهديدات التي قد تؤثر على الأفراد والمنشآت على حد سواء، هذا وقد أشارت دراسة كل من **(Slapnicar et al., 2022, Alic,2021; عطية، ٢٠٢١، الرشيدي وعباس ٢٠١٩)** إلى أن هناك مجموعة من تلك المخاطر يمكن عرض أهمها في الآتي:

٤/٢/١ **البرمجيات الخبيثة:** والتي تشمل الفيروسات وأحصنة طروادة وبرامج التجسس وغيرها، والتي تهدف إلى سرقة المعلومات أو تعطيل الأنظمة.

٤/٢/٢ **اختراق البيانات:** والتي تتمثل في الوصول إلى البيانات بشكل غير مصرح به، مما يؤدي إلى سرقتها أو تسريبها، وهو يشكل تهديدا كبيرا للخصوصية والأمان.

٤/٢/٣ **اختراق الهوية:** حيث يتم استخدام معلومات الهوية الشخصية للقيام بأنشطة غير مصرح بها، مثل فتح حسابات بنكية مزيفة أو التجسس على الأفراد.

٤/٢/٤ **اختراق امن الشبكات:** والتي تتضمن اختراق الأجهزة الشبكية والبنية التحتية للشبكات، مما يؤدي إلى سرقة البيانات أو التلاعب بها.

٤/٢/٥ **الاحتيال الإلكتروني:** وهي تعد محاولة احتيالية لاستدراج الأفراد للكشف عن معلوماتهم الشخصية أو المالية، عادة من خلال رسائل البريد الإلكتروني المزيفة أو مواقع الويب الزائفة.

٤/٢/٦ **التهديدات الداخلية:** والتي تشمل التهديدات الناتجة عن موظفين أو أشخاص داخل المنشأة الذين يستخدمون وصولهم المصرح به بطرق غير قانونية للوصول إلى المعلومات أو التسبب في الأضرار.

٤/٢/٧ **البرمجيات الضارة لإنترنت الأشياء:** حيث تمثل التهديدات التي تستهدف الأجهزة المتصلة بالإنترنت مثل الأجهزة المنزلية الذكية والأجهزة الطبية، مما يمكن أن يؤدي إلى استغلال الجهاز أو السيطرة عليه.

٤/٢/٨ **الضغط النفسي على موظفي الأمان:** استغلال الضغط النفسي على موظفي الأمان للحصول على معلومات حساسة أو للوصول إلى معلومات عن البنية التحتية.

٤/٣ آليات الحد من مخاطر الأمن السيبراني:

تنولت دراسة كل من **(Morin, 2020; SEC, 2022a; Yang et al. 2020)** مجموعة من التدابير المختلفة التي يمكن اتخاذها للحد من مخاطر الأمن السيبراني والتي كان من أهمها الآتي:

٤/٣/١ **تحديد وتقييم المخاطر:** حيث ينطوي ذلك على تحديد المخاطر المحتملة للأمن السيبراني وتقييمها بالنسبة للمنشأة، ويتم ذلك من خلال تحليل الأصول الرقمية وتحديد التهديدات المحتملة وتقييم الثغرات.

٤/٣/٢ **تطبيق سياسات الأمان:** حيث يتضمن ذلك وضع سياسات وإجراءات أمان صارمة، تغطي جوانب مختلفة مثل إدارة الوصول، تشفير البيانات، التحقق من الهوية، والنشر الآمن للتطبيقات.

٤/٣/٣ **تدريب وتوعية الموظفين:** حيث يعتبر التدريب والتوعية للموظفين حول مخاطر الأمن السيبراني وممارسات الأمان الجيدة جوهر عملية الحد من هذا النوع من المخاطر، ويتضمن ذلك تعزيز الوعي بشأن التهديدات السيبرانية المحتملة، وكيفية التعامل معها بما في ذلك التصيد الاحتيالي **(Phishing)** والبريد الإلكتروني المزيف وغيرها من الهجمات السيبرانية الشائعة.

٤/٣/٤ **تطبيق تقنيات الأمان الفعالية:** ويشتمل ذلك على استخدام التقنيات الحديثة للحماية مثل جدران الحماية، أنظمة الكشف عن الاختراقات، برامج مكافحة الفيروسات، والتحديث الدوري للبرامج والأنظمة لضمان سلامتها من الثغرات الأمنية المعتادة.

٤/٣/٥ **التحليل المستمر للتهديدات والاستجابة السريعة:** حيث يجب على المنشآت إجراء تحليل مستمر للتهديدات السيبرانية، والاستجابة بشكل سريع للتهديدات الجديدة أو الحالات الطارئة.

٤/٣/٦ **تنفيذ خطط الطوارئ والتعافي:** حيث يجب وضع خطط استجابة للطوارئ تتضمن إجراءات للتعامل مع الهجمات السيبرانية واستعادة البيانات والأنظمة المتأثرة بشكل سريع وفعال.

ويرى الباحث أن إدارة مخاطر الأمن السيبراني تتطلب مجموعة من الخطوات التي تتخذ بشكل دوري لمواجهة التهديدات الإلكترونية ومعالجتها من خلال رصدها وتحديدها وتقييمها، ومن أجل إدارتها بفاعلية، الأمر الذي ينبثق من خلال وجود نظرة شاملة لهذه المخاطر وتعاون من كافة الأفراد داخل المنشأة، **كما يؤكد الباحث** على أن إدارة مخاطر الأمن السيبراني تعتمد على وجود إستراتيجيات تعمل على تعزيز ترتيب أولويات المخاطر المطلوب معالجتها، لرصد التهديدات الأكثر ضررًا والمطلوب مواجهتها بشكل فوري.

المحور الخامس: العلاقة بين الملاءة المهنية للمراجع الداخلي وجودة الأمن السيبراني في ضوء الحوكمة الرقمية.

تمتد المخاطر السيبرانية إلى أبعد من اختراق البيانات، حيث قد تصل إلى اضطراب عمليات المنشآت بأكملها، والتي قد تتسبب في أن تتكبد تلك المنشآت مبالغ طائلة في سبيل السيطرة على ذلك، وفي هذا السياق فقد أكدت دراسة **(Miskiewicz & Affordable, 2022)** على أن ٧٩٪ من المنشآت التي شملتها الدراسة صنفت المخاطر السيبرانية كواحدة من أكبر خمسة مخاطر تتعرض لها تلك المنشآت.

والجدير بالذكر أن نشاط المراجعة الداخلية يلعب دوراً هاماً وبارزاً في مساعدة تلك المنشآت على إدارة هذه المخاطر من خلال تقديم ضمان موضوعي ومستقل للضوابط الرقابية الحالية والمطلوبة، وكذلك مساعدة الإدارة العليا ومجلس الإدارة على تفهم المخاطر المرتبطة بالعالم الرقمي الجديد، كما أشار نموذج معهد المراجعين الداخليين **(IIA, 2022)** إلى أن هناك ثلاثة خطوط للدفاع عن اختراقات أنظمة الأمن السيبراني حيث يمثل خط الدفاع الأول الرقابة الإدارية، بينما يمثل مراقبة المخاطر وأدوار الرقابة التي وضعتها الإدارة خط الدفاع الثاني، وجاء التوكيد المستقل ليمثل خط الدفاع الثالث.

وعند استعراض متطلبات خط الدفاع الأول نجد أنه يتمثل في ملاك العمليات التجارية ويركز على تقنية المعلومات (**IT**) المسئولة عن الأنظمة والعمليات والبنية التحتية للبيانات والمخاطر المتعلقة بها، أما خط الدفاع الثاني فيتمثل في وظيفة أمن المعلومات والتي تكون دائماً تحت إشراف مسئولي أمن المعلومات وتمتد مسئوليتهم لعمليات إدارة المخاطر، بناء الضوابط الرقابية اللازمة ورصد فعالية هذه الضوابط واتخاذ الإجراءات التصحيحية عند الحاجة، كما أنهم مسئولون عن تصميم سياسات وإجراءات الأمن السيبراني ورصد المؤشرات الرئيسية للمخاطر، بينما يأتي خط الدفاع الثالث والذي يتمثل في التأكيد المستقل لجهود الأمن السيبراني من خلال المراجع الداخلي، حيث يتحمل المراجع الداخلي مسئولية ضمان تنفيذ الخطوات اللازمة لتحقيق متطلبات خط الدفاع الأول والثاني، وذلك نظراً لأن المراجع الداخلي يقوم بدوراً هاماً في تقييم وتحديد طرق تحسين الأمن السيبراني للمنشأة وإبلاغ نتائج المراجعة إلى لجنة المراجعة ومجلس الإدارة، كما يقوم المراجع الداخلي بتقييم أصول تقنية المعلومات في عهدة المستخدمين مع التأكيد على عدم وجود أي برامج مشبوهة وهذا ما أكدت عليه دراسة المعهد القانوني للمراجعين الداخليين **(CIIA, 2021).**

ويرى الباحث أن هذا الأمر يتطلب مجموعة من المهارات التي لابد أن تتوافر لدى المراجع الداخلي بما يعزز من ملاءته المهنية بصدد التعامل مع متطلبات ومخاطر الأمن السيبراني بما يدعم جودة الأمن السيبراني وذلك في ضوء مؤشرات العالم الرقمي الجديد، ويمكن استعراض ذلك إستناداً إلى ما جاء بمجموعة من نتائج الدراسات ذات الصلة بهاذ الشأن على النحو التالي:

٥/١ المهارات المطلوبة من المراجعين الداخليين لدعم جودة الأمن السيبراني في ضوء الحوكمة الرقمية:

أكدت دراسة كل من **(Badawy, 2021; Florakis et al.٢٠٢٠)** على أن المراجعة الداخلية لكي تؤدي دورها في إجراء التقييمات اللازمة لجهود الأمن السيبراني فأنها سوف تحتاج إلى تعزيز مهاراتها في هذا المجال، ودعم الملاءة المهنية للمراجع الداخلي، ومع ذلك فقد يكون من الصعب في بعض الحالات التوصل إلى الكفاءة المهنية الصحيحة للمراجع الداخلي المصحوبة بالمهارات الفنية

المناسبة، لذلك قد يكون البحث عن مزودي خدمة خارجيين حلاً ضرورياً لتوسيع قاعدة مهارات المراجعة الداخلية ودعم ملاءتها، وسواء اختارت المراجعة الداخلية تطوير مهاراتها في مجال الأمن السيبراني أو البحث عن كفاءات خارجية، فإن ذلك يتطلب تطوير خبراتها في ثلاث مجالات رئيسية تضم:

٥/١/١ إدارة النظم: حيث يتطلب ذلك إلمام المراجع الداخلي بقواعد البيانات والخوادم والتطبيقات التي يمكن أن تتعرض للهجمات السيبرانية لأنه بدون هذا الفهم، سيكون من الصعب مراجعة تلك الأنظمة والتعامل معها.

٥/١/٢ تصميم الشبكات وتكوين النظام: حيث يتطلب ذلك أن يكون المراجع الداخلي بحاجة للوصول إلى كفاءات ذو معرفة بشبكات متنوعة جدران الحماية **(Firewalls)**، وقوائم التحكم في الوصول **(Access Control Lists)**، والتحكم في الوصول إلى الشبكة **(Network Access Control).**

٥/١/٣ تطوير البرمجيات: حيث يتطلب ذلك من المراجع الداخلي أن يكون ذو معرفة وملماً بتطوير البرمجيات ولغة البرمجة.

هذا وقد أكدت دراسة **(IIARF,٢٠١٨)** على أن الدور الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني وتحسين جودته يعتمد في الأساس على مدى قدرة إدارة المراجعة الداخلية بتقديم النصح لمجلس الإدارة فيما يتعلق بتحديد وتوصيف وقياس مخاطر الأمن السيبراني وتفادي آثارها وكيفية مواجهتها ودعم جودة الأمن السيبراني ببيئة عمل المنشأة الرقمية، بما يدعم تحقيق المنشأة لأهدافها المرجوة، هذا ويتم ذلك عن طريق القيام بالتحديث والمتابعة الدورية المختلف لمخاطر الأمن السيبراني، وتحديد كيفية تطوير وتنمية الاستراتيجيات المتبعة لإدارة مخاطر الأمن السيبراني.

وفي هذا الشأن فقد أكدت دراسة **(حامد، ٢٠١٩)** على أن الدور التوكيدي للمراجع الداخلي في دعم جودة الأمن السيبراني يرتكز في الأساس على قيام مدير إدارة المراجعة الداخلية بتقديم تقرير باستنتاج بشأن مدى صدق التقارير المعدة من قبل المسئولين عن إدارة مخاطر الأمن السيبراني وطرق دعم جودة الأمن السيبراني، وذلك من خلال قيان المراجع الداخلي بتقديم تقرير حول مدى فاعلية تصميم وتشغيل عميلة إدارة مخاطر الأمن السيبراني وطرق تحقيق جودته، كذلك التقرير عن مدى تنفيذ الاستراتيجيات الموضوعة بشأن جودة الأمن السيبراني في ظل بيئة التحول الرقمي.

ووفقاً لما أكدت عليه دراسة كل من **(Shahimi&Mahzan,2018;Li & Wang., 2019)** بشأن متطلبات الدور الفاعل للمراجع الداخلي نحو زيادة جودة الأمن السيبراني وإدارة مخاطره بما يدعم الملاءة المهنية لهذا الدور فلقد تم عرضها طبقاً لما جاء بهذه الدراسات على النحو التالي:

أ- ارتقاء إدارات الشركات بثقافة النظر للمراجعة الداخلية كوظيفة مضيفة للقيمة:

وذلك من خلال توفير الاستقلال التنظيمي لها، وتحديد حقوق وواجبات ومسئوليات المراجعين الداخليين بالشركات، الأمر الذي قد ينعكس على تدنية مستوى فجوة التوقعات في المراجعة الداخلية، وتحديد الأدوار والمسئوليات الحالية والمستحدثة في ظل بيئة التحول الرقمي للشركات.

ب- تنظيم مهنة المراجعة الداخلية

من خلال تنمية القدرات العلمية والعملية للمراجع الداخلي خاصة في مجال تكنولوجيا المعلومات والتطورات المتلاحقة ببيئة الأعمال الحالية، على أن يشترط ذلك التنظيم حصول المراجعين الداخليين على رخصة معتمدة منه وضع وتنفيذ ومتابعة برامج التنمية المهنية للمراجعين الداخليين، تأخذ في الاعتبار متغيرات بيئة تكنولوجيا المعلومات.

ج- تطوير نظام التعليم المحاسبي

وذلك من خلال إعادة النظر في برامج التعليم المحاسبي الرقمي وكذلك برامج التعليم المهني المستمر، وتدعيمها بمقررات ملائمة ذات صلة بالأدوار والمسئوليات الحالية والمستحدثة التي تقع على عاتق المراجعين الداخليين في ظل بيئة التحول الرقمي.

ويرى الباحث أنه على المراجع الداخلي وهو بصدد تحقيق جودة الأمن السيبراني والحد من مخاطره، عليه استخدام تقنيات وبرمجيات تخدم الإدارة وتقدم لها كل الأدوات التي تمكنها من الاستفادة من جودة المعلومات المحاسبية الإلكترونية في الوقت المناسب، هذا فضلاً عن تطوير أنظمة الرقابة للمراجعة الداخلية لكي تتلاءم مع أهداف وسياسات المنشأة بما يساهم في تحقيق جودة الأمن السيبراني في ضوء البيئة الرقمية، والعمل بشكل مستمر على وضع مجموعة من الممارسات والسياسات والإجراءات التي تساعد على رفع الملاءة المهنية للمراجع الداخلي، كما يؤكد الباحث على ضرورة تبني المراجع الداخلي لثقافة التعامل مع الجهود السيبرانية مع الحفاظ على خطوط اتصال مفتوحة وواضحة مع كافة الإدارات لكي تكون أحد محفزات العمل الوقائي ضد الهجمات السيبرانية مع ضرورة التأكيد على قدرة المنشأة على تقييم قوة الضوابط المتعلقة بالأمن السيبراني.

المحور السادس ـ الدراسة التطبيقية:

٦/١ منهجية البحث وبناء النماذج التطبيقية:

هدف البحث إلى قياس أثر الحوكمة الرقمية على العلاقة بين الملاءة المهنية للمراجع الداخلي وجودة الأمن السيبراني، ولتحقيق ذلك الهدف اعتمد الباحث على **أسلوب تحليل المحتوى (Content Analysis)** حيث تم تحليل البيانات الواردة بالقوائم المالية، بالإضافة إلى الإيضاحات المتممة لها وذلك لمجموعة من الشركات المصرية المسجلة ضمن مؤشر **EGX100** خلال الفترة من عام (٢٠١٨ حتى عام ٢٠٢٣) .

٦/١/١ توصيف وقياس متغيرات الدراسة:

في ضوء مشكلة البحث وأهدافه وفروضه تم تحديد متغيرات الدراسة وتوصيفها وكيفية قياسها على النحو التالي:

٦/١/١/١ قياس المتغيرات التابعة:

تتمثل المتغيرات التابعة فيما يلي

٦/١/١/١/١ الملاءة المهنية للمراجع الداخلي (IAR):

اعتمد الباحث في قياس الملاءة المهنية للمراجع الداخلي على جودة تقرير المراجعة الداخلية الذي يقوم بإعداده مدير إدارة المراجعة الداخلية ورفعه إلى مجلس إدارة الشركة.

٦/١/١/١/٢ جودة الأمن السيبراني(QCS):

في ضوء مراجعة الأدبيات السابقة اختار الباحث مقياس عدد الحوادث السيبرانية في الشركة خلال العام لقياس جودة الأمن السيبراني.

٦/١/١/٢ قياس المتغير المستقل: الحوكمة الرقمية (DG):

قام الباحث بقياس الحوكمة الرقمية من خلال عدد المشاريع الرقمية الناجحة في الشركة خلال العام .

٦/١/١/٣ قياس المتغيرات الرقابية Control Variables.

اعتمد الباحث على نتائج العديد من الدراسات السابقة التي أشارت إلى بعض العوامل أو المتغيرات الرقابية التي يجب السيطرة عليها نظراً لقدرتها على التأثير في العلاقة بين متغيرات الدراسة، وقد تم إدراج تلك المتغيرات ضمن النماذج التطبيقية علماً بأن تلك المتغيرات لا تدخل في نطاق الدراسة محل البحث وتم إضافتها بهدف ضبط العلاقة في نموذج الانحدار ومن أهم هذه المتغيرات حجم الشركة، معدل العائد على حق الملكية، نوع النشاط .

في ضوء ما جاء بالدراسات السابقة يمكن للباحث توضيح طريقة قياس متغيرات نماذج الدراسة من خلال الجدول التالي:

جدول رقم (١)
طريقة قياس متغيرات الدراسة

المتغيرات		طريقة القياس	مصادر البيانات
رمز المتغير	اسم المتغير		
أولا المتغير المستقل			القوائم المالية السنوية والإيضاحات المتممة لها بالإضافة إلى تقارير المراجعة الداخلية
IAR	الملاءة المهنية للمراجع الداخلي	تقرير المراجعة الداخلية	
ثانياً المتغير التابع			
QCS	جودة الأمن السيبراني	عدد الحوادث السيبرانية خلال العام	
ثالثاً المتغير الوسيط			
DG	الحوكمة الرقمية	عدد المشاريع الرقمية الناجحة	
رابعاً: المتغيرات الرقابية			
F SIZE	حجم الشركة	اللوغاريتم الطبيعي لإجمالي قيمة الأصول (**Rouf, 2011; Lobo et al., 2013 ;Alsadoun & Aljabr, 2014; Ji et al., 2017**)	
ROE	معدل العائد على حقوق الملكية	قسمة صافي الربح السنوي على القيمة الدفترية لحقوق الملكية قياساً على دراسة (**Alfaraih & Alanezi, 2012**)	
TA	نوع النشاط	متغير وهمي يأخذ القيمة (١) اذا كانت المنظمة تمارس نشاط صناعي أو القيمة (صفر) بخلاف ذلك.	

٦/٢ صيغة النماذج الإحصائية اللازمة لاختبار فروض الدراسة:

بناء على ما سبق ومن خلال مشكلة الدراسة وأهدافها وفروضها قام الباحث بإعداد ثلاثة نماذج أساسية لقياس أثر الحوكمة الرقمية كمتغير مستقل على العلاقة بين الملاءة المهنية للمراجع الداخلي وجودة الأمن السيبراني كمتغيرات تابعة، هذا بالإضافة إلى استخدام بعض المتغيرات الرقابية التي تم الإشارة إليها من قبل.

وفي ضوء ما سبق يمكن للباحث صياغة نماذج الدراسة في شكل نماذج انحدار وذلك على النحو التالي:

النموذج الأول: أثر تطبيق الحوكمة الرقمية على الملاءة المهنية للمراجع الداخلي

$$IAR_{it} = \beta_0 + \beta_1 (DG) + \beta_2 F\ SIZE + \beta_3 (ROE) + \beta_4 (TA) + £_{it}$$

النموذج الثاني: أثر الملاءة المهنية للمراجع الداخلي على جودة الأمن السيبراني .

$$QCS_{it} = \beta_0 + \beta 1\ (DG) + \beta 2\ (\ F\ SIZE\ ) + \beta 3\ (\ ROE\ ) + \beta 4\ (\ TA\ )$$

النموذج الثالث: أثر تطبيق الحوكمة الرقمية على نموذج العلاقة بين الملاءة المهنية للمراجع الداخلي وجودة الأمن السيبراني

$$QCS_{it} = \beta_0 + \beta_1 (IAR) + \beta_2 (DG*IAR) + \beta_3 (F\ SIZE) + \beta_4 (R$$

حيث أن:

(DG_{it}): الحوكمة الرقمية

(IAR): الملاءة المهنية للمراجع الداخلي

(QCS_{it}): جودة الأمن السيبراني

(F SIZE): حجم الشركة

(ROE): معدل العائد على حقوق الملكية

(TA): نوع النشاط

($\beta_3 - \beta_5$): معاملات الانحدار لمتغيرات الرقابة

($£_{it}$): بند الخطأ العشوائي

(β_0): قيمة الثابت في معادلة الانحدار

(DG * IAR): متغير يعكس التفاعل بين الحوكمة الرقمية والملاءة المهنية للمراجع الداخلي

٦/٣ تصميم الدراسة التطبيقية

تم تصميم الدراسة التطبيقية من خلال الآتي:

٦/٣/١ مجتمع وعينة الدراسة:

يتمثل مجتمع الدراسة في جميع الشركات المقيدة ببورصة الأوراق المالية المصرية والمدرجة بمؤشر **(EGX 100)** وذلك لاعتبار الشركات التي تندرج تحت هذه المؤشر من أكثر الشركات نشاطاً في البورصة المصرية، كذلك تم تحديد عينة الدراسة من خلال عينة حكمية في ذات

المؤشر السابق بحيث تشتمل على بيانات قطاعات مختلفة خلال مجموعة من السنوات (٢٠١٨ حتى ٢٠٢٣) وهي بيانات تمثل سلاسل زمنية **Time Series Data** لمجموعة من الشركات التي يبلغ عددها (٤٥) شركة تمثل (١١) قطاع، على أن يتم ذلك طبقاً للضوابط التالي:

١- أن تكون الشركات المختارة من الشركات النشطة خلال فترة الدراسة ومدرجة ضمن مؤشر **(EGX 100)** .

٢- أن تتوافر التقارير المالية السنوية عن الشركات بانتظام، وأن تتوافر فيها بيانات كافية لحساب متغيرات الدراسة.

٣- ألا تكون قد تعرضت هذه الشركات للشطب أو الاندماج أو التوقف خلال فترة الدراسة.

٤- تم استبعاد المؤسسات المالية والتي تضم (البنوك - شركات التأمين - شركات الخدمات المالية) وذلك للطبيعة الخاصة التي تتمتع بها تلك الشركات.

ويوضح الجدول التالي رقم (٢) عدد الشركات في كل قطاع ونسبة كل قطاع في عينة الدراسة:

جدول رقم (٢)

التوزيع القطاعي للشركات ونسبة كل قطاع في عينة الدراسة

م	القطاع	عدد الشركات	نسبة شركات العينة مصنفة قطاعياً (%)
١	الأغذية والمشروبات	١٢	٪٢٦,٧
٢	التشييد ومواد البناء	٥	٪١١,٢
٣	الاتصالات	٣	٪٦,٧
٤	الغاز والبترول	٤	٪٨,٩
٥	الرعايا الصحية	١	٪٢,٢
٦	السياحة والترفيه	٢	٪٤,٤
٧	الكيماويات	٤	٪٨,٩
٨	المنتجات المنزلية	٢	٪٤,٤
٩	الموارد الأساسية	٢	٪٤,٤
١٠	العقارات	٦	٪١٣,٤
١١	الخدمات والمنتجات الصناعية والسيارات	٤	٪٨,٩
إجمالي عدد الشركات		**٤٥**	٪١٠٠
إجمالي عدد المشاهدات		**٣١٣**	٪١٠٠

٦/٣/٢ أداة جمع البيانات

اعتمد الباحث في جمع بيانات الدراسة على التقارير المالية والإيضاحات المتممة لشركات العينة المنشورة في مواقعها الإلكترونية الرسمية، بالإضافة لكتاب الإفصاح السنوي الصادر عن بورصتي القاهرة والإسكندرية للشركات، هذا بالإضافة إلى موقع شركة مصر لنشر المعلومات (www.egidegypt.com) للحصول على القوائم المالية السنوية الكاملة لعينة الشركات، وكذلك بعض المواقع الإلكترونية مثل موقع معلومات مباشر (www.mubasher.info)

٦/٣/٣ الأساليب الإحصائية المستخدمة في تحليل بيانات الدراسة:

قام الباحث بإجراء عمليات الترميز لكافة متغيرات الدراسة ثم إدخال وتشغيل البيانات على الحاسب الآلي باستخدام برنامج الحزم الإحصائية للعلوم الاجتماعية **(SPSS)** الإصدار (٢٤) وأيضاً تم الاعتماد على برنامج التحليل القياسي **E-Views** الإصدار (١٠)، وذلك بهدف إجراء التحليل الإحصائي لبيانات الدراسة التطبيقية في ضوء الاعتماد على بعض الأساليب الإحصائية لأغراض اختبار فروض الدراسة والتي اشتملت على:

- التحليل الإحصائي الوصفي **Descriptive Statistics:** ويستخدم هذ التحليل بهدف الحصول على معلومات خاصة عن خصائص البيانات المستخدمة في التحليل مثل (أقل قيمة، أعلى قيمة، الوسط الحسابي، الانحراف المعياري، المدي)
- اختبار **Kolmogorov – Smirnov Test** واختبار **Jarque – Bera**: وذلك للتحقق من مدى اقتراب بيانات الدراسة التطبيقية من التوزيع الطبيعي **Normal Distribution**
- اختبار الارتباط الذاتي **Autocorrelation Test**: وذلك لفحص والتأكد من وجود مشكلة الارتباط الذاتي في نماذج الدراسة من عدمه بالاستعانة باختبار **(Durbin Watson Test)**
- اختبار معامل تضخم التباين **Variance Inflation Factor (VIF)**: حيث يستخدم هذا الاختبار للتأكد من عدم وجود مشكلة الازدواج الخطي بين متغيرات الدراسة .
- مقياس استقرار السلاسل الزمنية: والذي يتم من خلال اختبار جذر الوحدة **Unit Root Test** لفحص استقرار أو سكون المتغيرات المكونة للسلاسل الزمنية وتحديد درجة التكامل بينها، وذلك تفادياً لمشكلة الاستدلال القياسي .
- اختبار تكامل السلاسل الزمنية **Co-Integration Test**: بهدف التحقق من التوازن بين متغيرات الدراسة.
- نموذج الانحدار الخطي المتعدد بطريقة المربعات الصغرى (LS) **Least Squares**: وذلك بهدف تقدير العلاقات بين متغيرات الدراسة .

٦/٤ تحليل نتائج الدراسة التطبيقية واختبار فروض البحث

٦/٤/١ اختبار صلاحية البيانات للتحليل الإحصائي

٦/٤/١/١ اختبار التوزيع الطبيعي (Normal Distribution Test)

استخدم الباحث اختبار **(Kolmogorov – Smirnov)** ضمن حزمة البرنامج الإحصائي **(SPSS)** واختبار **(Jarque – Bera)** ضمن برنامج **(E- Views)** وذلك للتحقق من التوزيع الطبيعي للبيانات، وذلك بالنسبة لمتغيرات الدراسة الكمية المتصلة المتمثلة في جودة الأمن السيبراني والملاءة المهنية للمراجع الداخلي وحجم الشركة ومعدل العائد على حقوق الملكية، ويمكن الحكم على توافر التوزيع الطبيعي للبيانات إذا كانت درجة معنوية (Sig) كلا الاختبارين أكبر من (0.05)، ويتضح ذلك من خلال الجدول التالي:

جدول رقم (٣)

نتائج اختبار التوزيع الطبيعي (Normal Distribution)

Jarque-Bera Test		Kolmogorov-Smirnov		عدد المشاهدات	المتغيرات الكمية المتصلة
Sig.	J - B	Sig.	Statistic		
.000	113227.44	.000	.254	313	(جودة الأمن السيبراني) QCS
.000	2817.909	.000	.209	313	(الملاءة المهنية للمراجع الداخلي) IAR
.000	.777٧405	.200	.046	313	(حجم الشركة) F.SIZE
.000	76844.55	.000	.366	313	(معدل العائد على حقوق الملكية) ROE

وبنا على ما جاء بالجدول السابق يتضح للباحث أن درجة المعنوية (.Sig) أقل من **(0.05)** لكافة المتغيرات مما يعني عدم توافر التوزيع الطبيعي للبيانات فيما عدا حجم الشركة **(F.SIZE)** طبقاً لاختبار **(Kolmogorov- Smirnov)** ويتفق اختبار **(Jarque – Bera)** مع هذه النتيجة، ولعلاج هذه المشكلة يتم استخدام دالة اللوغاريتم الطبيعي Natural Log لهذه المتغيرات بحيث تقترب من التوزيع الطبيعي، وطبقاً لنظرية النهاية المركزية **(Central Limit Theory)** والتي تنص على أنه من الممكن افتراض تحقق شرط التوزيع الطبيعي للعينات الكبيرة **(n > 30)** بصرف النظر عن توزيع المجتمع الأصلي، وبما أن حجم العينة في هذه الدراسة **(n=313)** فلن تكون مشكلة عدم توزيع البيانات توزيعاً طبيعياً ذات تأثير على صحة النماذج، أما بقية المتغيرات فهي متغيرات وهمية ذات قيمة ثنائية لا تخضع لشروط التوزيع الطبيعي.

٦/٤/١/2 اختبار التداخل الخطي المتعدد Multicollinearity Test

حيث أنه للتحقق من وجود مشكلة التداخل الخطي المتعدد التي تساهم في ضعف قدرة نموذج الدراسة في تفسير أثر المتغير المستقل على المتغير التابع تم استخدام مقياس **(Collinearity Diagnostics)** من خلال احتساب معامل (Tolerance) لكل متغير من المتغيرات المستقلة والرقابية في علاقة الانحدار مع المتغير التابع، ومن ثم إيجاد معامل **(VIF) Variance Inflation Factor**حيث يعد بمثابة مقياساً لتأثير الارتباط بين المتغيرات المستقلة، ويظهر ذلك بوضوح من خلال الجدول التالي رقم (٤)

جدول رقم (٤)

نتائج اختبار التداخل الخطي Multicollinearity Test

Collinearity Statistics				
(جودة الأمن السيبراني) QCS		(الملاءة المهنية للمراجع الداخلي) IAR		المتغيرات التابعة
VIF	Tolerance	VIF	Tolerance	المتغيرات المستقلة والرقابية
1.679	.556	-	-	(الملاءة المهنية للمراجع الداخلي) IAR
1.555	.645	1.006	.997	(الجوكمة الرقمية) DG
1.620	.615	-	-	(المتغير التفاعلي) (DG*IAR)
2.093	.479	1.950	.515	(حجم الشركة) FSIZE
1.016	.986	1.004	.992	(معدل العائد على حقوق الملكية) ROE
1.061	.944	1.043	.956	(نوع النشاط) TA

وفي ضوء ما سبق يتضح من الجدول رقم **(٤)** أن قيمة **(VIF)** لكافة متغيرات الدراسة لم تتجاوز (١٠)، وقد أظهرت النتائج أن جميع قيم **(VIF)** للمتغيرات المستقلة تشير إلى عدم وجود تداخل خطي متعدد في نموذج الدراسة، مما يدل على قوة النموذج المستخدم في تفسير تأثير المتغيرات المستقلة على المتغير التابع

٦/٤/٢ قياس استقرار السلاسل الزمنية Time Series Stationarity

في معظم نتائج التحاليل الإحصائية نجد أنه هناك عدم استقرار للسلاسل الزمنية للمتغيرات تتصف بخاصية عدم الاستقرار، ومن ثم لا يمكن تعميم نتائج سلوك هذه السلاسل على الفترات الزمنية المستقبلية وللتحقق من استقرار السلاسل الزمنية يتم استخدام اختبار جذر الوحدة **(Unit Root Test)** وذلك بهدف احتساب الفروق اللازمة لتحويل السلاسل الزمنية المتغيرة إلى سلاسل زمنية مستقرة، ويوضح الجدول التالي رقم (٥) نتائج اختبارات الاستقرار لمتغيرات الدراسة:

جدول رقم (٥)

نتائج اختبار استقرار متغيرات نماذج الدراسة للتأكد من سكون السلاسل الزمنية باستخدام الاختبارات المختلفة لجذر الوحدة Unit Root Test للفترة (٢٠١٨ – ٢٠٢٣)

الفروق اللازمة لسكون المتغير (I)	الفرق الأول First Difference		المستوى الأصلي The Level		الاختبارات	المتغيرات
	Prob.	Statistic	Prob.	Statistic		
I (0)***	0.00	-7.3030	0.00**	-8.313	Levin Lin & Chu t	QCS
I (0)	0.0002	142.33	0.01*	116.47	ADF – Fisher Chi – square	
I (0)	0.000	277.47	0.00**	176.65	PP-Fisher Chi – Square	
I (0)	0.00	-12.117	0.00**	-9.1777	Levin Lin & Chu t	IAR
I (0)	0.001	128.68	0.002**	126.63	ADF – Fisher Chi – square	
I (0)	0.00	271.55	0.00**	205.16	PP-Fisher Chi – Square	
I(1)***	0.00**	-137.92	0.00	-236.82	Levin Lin & Chu t	FSIZE
I(1)	0.0004**	136.07	0.1540	96.191	ADF – Fisher Chi – square	
I(1)	0.00**	247.88	0.0001	143.42	PP-Fisher Chi – Square	
I(1)	0.00**	-5.6714	0.00	-35.431	Levin Lin & Chu t	ROE
I(1)	0.044*	108.33	0.106	100.42	ADF – Fisher Chi – square	
I(1)	0.00**	233.88	0.0278	112.39	PP-Fisher Chi – Square	

المصدر: إعداد الباحث إعتماداً على مخرجات البرنامج الإحصائي (E-Views)

* تشير إلى الدلالة الإحصائية عند مستوى معنوية أقل من 0.05

** تشير إلى الدلالة الإحصائية عند مستوى معنوية أقل من 0.01

*** تشير I (0) إلى أن المتغير ساكن عن المستوى الأصلي و I (1) إلى أن المتغير ساكن عند الفرق الأول

وقد أشارت نتائج اختبار جذر الوحدة **(Unit Root)** إلى أن متغيرات النموذج جميعها غير مستقرة عند المستوى الأصلي **(Level)** عند مستوى معنوية **(0.05)** باستثناء متغير جودة الأمن السيبراني **(QCS)**، الملاءة المهنية للمراجع الداخلي **(IAR)**، حجم الشركة **(F SIZE)** وفقاً للاختبارات المختلفة لجذر الوحدة كما أكدت نتائج اختبار جذر الوحدة أن كافة متغيرات نماذج الدراسة يتحقق لها الاستقرار (سكون السلسلة الزمنية) بعد إجراء الفرق الأول **(First Difference)** وذلك عند مستوى معنوية (0.01) فيما عدا متغير معدل العائد على حقوق الملكية **(ROE)** .

٦/٤/٣ اختبار تكامل السلاسل الزمنية (Co- Integration Test)

في ضوء اختبار جذر الوحدة السابق اتضح أن هناك متغيرات ساكنة أو متكاملة عند مستوياتها الأولى **I(0)**، أي أنها غير ساكنة في المستوى الأصلي وبالتالي لابد من اختبار البواقي الناتجة من تقدير العلاقة الخطية بينها بحيث تكون متكاملة من الرتبة **U = I (0)**، ومن ثم يتحقق التوازن في الأجل الطويل والحصول على معلمات انحدار حقيقية للتأكد من سكون البواقي لانحدار التكامل المشترك الخاصة بنماذج الدراسة، ويظهر ذلك بالصورة الكاملة في الجدول التالي رقم (٦):

جدول رقم (٦)

نتائج اختبار جذر الوحدة Unit Root لاختبار سكون البواقي باستخدام اختباري (ADF) و (LLC)

المتغيرات	نوع الاختبار	المستوى The Level				درجة التكامل
		Constant		Constant & Trend		
		Statistic	Prob.	Statistic	Prob.	
البواقي U	(ADF)	-2.8624	0.003٦**	-2.22784	0.0135*	I (0)
	(LLC)	-12.٣٧٥٤	0.000**	-12.2254	0.000**	I (0)

وفي إطار ما تقدم وبالنظر إلى الجدول السابق نجد أن بواقي معادلة الانحدار تتميز بالسكون أي أنها متكاملة من الدرجة صفر **I (0)**، ولتحديد مدى وجود ظاهرة التكامل المشترك بين متغيرات النموذج من عدمه فإنه يتم الكشف عن التكامل المشترك من خلال اختبار جوهانسون، حيث أنه إذا كانت متغيرات السلسلة الزمنية غير مستقرة بمستوياتها فإن ذلك يعني أنها متكاملة ويدل على وجود تكامل مشترك وعلاقة توازنية طويلة الأجل بين المتغيرات البحثية لنماذج الدراسة وعندها يمكن إجراء اختبارات **(Trace Test – Max – Elgen value Test)** وذلك طبقاً لنتائج الجدول التالي رقم (٧):

جدول رقم (٧)

نتائج اختبار جوهانسون للتكامل المشترك (Co – integration Test)

Max- Elgen value Test			Trace Test			عدد علاقات التكامل بين المتغيرات
Prob.	0.01 critical value	Max Eigen statistic	Prob.	0.01 critical value	Trace statistic	
0.0001	44.87900	218.0766	0.0001	103.9617	714.4494	R= 0
0.0000	37.37017	149.6415	0.0001	75.81888	494.3746	R ≤ 1
0.0000	30.71521	133.8854	0.0001	53.68152	341.7432	R ≤ 2
0.0001	24.86128	110.6955	0.0001	33.45816	203.8562	R ≤ 3
0.0000	17.52007	72.16994	0.0000	18.93713	90.16120	R ≤ 4
0.0000	5.634895	16.99128	0.0000	6.634899	17.99119	R ≤ 5

حيث تشير نتائج اختبار جوهانسون الواردة في الجدول السابق رقم (٧) إلى رفض وجود أي علاقة تكامل مشترك بين متغيرات النماذج عند مستوى معنوية **(0.01)** وفقاً للاختبارين، حيث ينطوي النموذج على ستة من علاقات التكامل المشترك بين متغيراته وهذا يعني وجود علاقات تحقق التوازن بين متغيرات النماذج في الأمد الطويل.

٦/٥ التحليل الوصفي لمتغيرات الدراسة:

٦/٥/١ التحليل الوصفي للمتغيرات الكمية المتصلة

بعد أن قام الباحث بالتأكد من صلاحية بيانات الدراسة للتحليل الإحصائي يُظهر الجدول رقم (٨) وصف لمتغيرات الدراسة الكمية المتصلة (جودة الأمن السيبراني **QCS**) الملاءة المهنية للمراجع الداخلي **(IAR)** حجم الشركة **(F SIZE)** معدل العائد على حقوق الملكية **(ROE)**.

جدول رقم (٨)

نتائج الإحصاء الوصفي لمتغيرات الدراسة المتصلة

Range	Minimum range	Maximum	S deviation	Mean	Variable	Year
3554	-246	3.305	.663056	1.21٥55	QCS	2018
3.984	088	4.072	.807677	1.29162	IAR	
1.753	-037	1.714	.263887	.11146	F SIZE	
2.347	-094	2.256	350584	.15966	ROE	
4.114	-908	30205	693626	1.00366	QCS	2019
6.058	.047	6.106	1.046624	1.07935	IAR	
2.700	-040	2.661	.555025	.16612	F SIZE	
52112	-1832	5.0277	.9285044	.262952	ROE	
4.716	-915	3.797	776515	1.12578	QCS	2020
4.704	110	4.813	989896	1.24603	IAR	
2.667	-132	2.537	395337	.09083	F SIZE	
3.5856	-3285	3.2572	5182372	.105737	ROE	
5.233	288	5.517	1.055542	1.28783	QCS	2021
8.317	-945	7.372	1.556845	1.39434	IAR	
2.405	-235	2.167	337078	.09995	F SIZE	
2.7095	-1487	2.5606	4946832	.188212	ROE	
5.413	.335	5.747	1.142327	1.64066	QCS	2022
9.426	-2408	7.019	1.690485	1.52946	IAR	
2.065	-100	1.965	306267	.09696	F SIZE	
2.4426	-1534	2.2894	.4681207	.177542	ROE	
1365	008	1371	286363	.36866	TA	
6.893	306	70197	1.217754	1.87179	QCS	2023
5.33٢	-1.56٢	3077٢	1.01025٥	1.٦٣٠٦٦	IAR	
1.24٤	-179	1.06٤	.174773	.0720٧	F SIZE	
1.307٧	-0814	1.226٤	.2019283	.11992٦	ROE	

ويتضح طبقاً لما جاء بهذا الجدول الآتي:

١- في ظل التحليل الوصفي لجودة الأمن السيبراني **(QCS)** يلاحظ أن هناك انخفاض في مستوى جودة الأمن السيبراني في الشركات الممثلة في عينة البحث حيث بلغ مستواه **(1.215)** خلال عام **(٢٠١٨)**، وانخفض في عام **(٢٠١٩)** إلى **(1.003)**، وقد اتضح أيضاً أن هناك تحسن في متوسط وجودة الأمن السيبراني **(QCS)** في عام **(٢٠٢٠)** حيث بلغ **(1.125)** وعام **(٢٠٢١)** إلى **(1.287)** كما بدأ تحسن مستوى جودة الأمن السيبراني بشكل ملحوظ بداية من عام **(٢٠٢٢)** حيث بلغ متوسط مستواه **(1.640)** كما بلغ عام **(٢٠٢٣)** إلى **(1.871).**

٢- في ظل التحليل الوصفي الملاءة المهنية للمراجع الداخلي **(IAR)** يلاحظ أن هناك ارتفاع درجة الملاءة المهنية للمراجع الداخلي والتي تظهر في تقرير المراجعة الداخلية للشركات الممثلة في عينة البحث خلال نطاق فترة الدراسة حيث بلغ أعلى متوسط للملاءة المهنية للمراجع الداخلي **(1.630)** في عام **(٢٠٢٣)**، بينما كان أقل متوسط للملاءة المهنية للمراجع الداخلي قدره **(1.07)** في عام **(٢٠١٩)** وهذا يدل على أن شركات العينة المدرجة ضمن المؤشر المصري **(EGX 100)** تسعى جاهدة نحو دعم سياسة الملاءة المهنية للمراجع الداخلي.

٣- التحليل الوصفي للمتغيرات الرقابية للدراسة فيما يتعلق بمعدل العائد على حقوق الملكية **(ROE)** يلاحظ أن أعلى قيمة للعائد على حقوق الملكية **(5.028)** بمتوسط حسابي **(0.263)** في عام **(٢٠١٩)** بينما كانت أقل قيمة **(-.081)** بمتوسط حسابي **(0.119)** في عام **(٢٠٢٣)**، وبالنسبة لحجم منشأة عميل المراجعة **(F.SIZE)** يلاحظ أن متوسط اللوغاريتم الطبيعي لحجم الشركة بلغ (8.984) في عام **(٢٠١٨)** وهو ما يعادل **(3.371)** مليار جنيه و **(8.992)** في عام **(٢٠١٩)** وهو ما يعادل **(3.384)** مليار جنيه ثم أخذ في الارتفاع ليصل إلى **(9.138)** في عام **(٢٠٢٣)** وهو ما يعادل **(6.840)** مليار جنيه

٦/٥/٢ التحليل الوصفي للمتغيرات الوصفية المنفصلة:

يظهر الجدول رقم (٩) وصفاً للمتغيرات الوصفية المنفصلة والتي تتمثل في المتغيرات الوهمية **(Dummy Variables)** التي يتم التعبير عنها بالقيمتين (١) أو (صفر) وهي الحوكمة الرقمية ونوع النشاط، وهذا ما يوضحه الجدول التالي رقم (٩):

جدول رقم (٩)

نتائج التحليل الوصفي للمتغيرات المنفصلة

Binomial Test					
Sig.	مشاهدات غير متحققة (٠)		مشاهدات متحققة (١)		المتغيرات
	النسبة	العدد	النسبة	العدد	
.000	63%	196	37%	117	DG
.414	60%	187	40%	126	TA

وبالاطلاع على بيانات الجدول السابق رقم (٩) يلاحظ انخفاض عدد مشاهدات الشركات التي تطبق الحوكمة الرقمية خلال فترة الدراسة **(١١٧)** مشاهدة بنسبة **(٣٧٪)** بالمقارنة **(١٩٦)** مشاهدة في شركات لا تطبق الحوكمة الرقمية، ويفسر ذلك الباحث بارتفاع تكاليف تطبيق تلك السياسة، كما بلغ عدد مشاهدات، وبلغت نسبة مشاهدة الشركات التي تنتمي للقطاع الصناعي خلال فترة الدراسة **(١٢٦)** مشاهدة بنسبة **(٤٠٪)** بالمقارنة **(١٨٧)** مشاهدة لشركات لا تنتمي إلى القطاع الصناعي.

٦/٦ نتائج اختبار فروض الدراسة:

لاختبار صحة فروض الدراسة تم إجراء تحليل الانحدار الخطي المتعدد وذلك لتوضيح العلاقة بين المتغير المستقل (الحوكمة الرقمية) والمتغيرات التابعة (الملاءة المهنية للمراجع الداخلية وجودة الأمن السيبراني) باستخدام برنامج الحزم الإحصائية للعلوم الاجتماعية **(SPSS)** الإصدار **(٢٤)** وبرنامج التحليل القياسي **E- Views** الإصدار **(١٠)** على النحو التالي:

٦/٦/١ نتائج اختبار الفرض الأول

ينص الفرض الأول على أنه "لا توجد علاقة ذات دلالة إحصائية بين الحوكمة الرقمية والملاءة المهنية للمراجع الداخلي"

حيث قام الباحث بتطوير هذا الفرض من خلال صياغة نموذج الانحدار الخطي المتعدد بهدف التعرف على العلاقة بين متغيرات الفرض السابق وذلك بعد إضافة بعض المتغيرات الرقابية، ويوضح الجدول التالي رقم (١٠) نتيجة الاختبار الإحصائي لنموذج الفرض الأول:

جدول رقم (١٠)

نموذج الانحدار الخطي المتعدد لنموذج الفرض الأول

المتغيرات المستقلة	المعاملات	الخطأ المعياري	إحصائية T	مستوى الدلالة
C	-114.72٨7	53.1540٩	-2.15843٧	0.031٧
DG	0.0741٧4	0.01862٨	3.981306	0.0001
DROE	1.072855	0.334933	3.203188	0.0017
DFSIZE	0.189815	0.406425	0.46748٨	0.6405
TA	0.093016	0.107508	0.86490٧	0.387٥
R-squared	0.206477	Mean dependent var		0.058433
Adjusted R-squared	0.1٧8298	S.D. dependent var		0.099699٢
S.E.of regression	0.895599	Akaike info criterion		2.64730٣
Sum squared resid	226.7792	Schwarz criterion		2.78159٥
Log likelihood	-378.0064	Hassan- Quinn criter		2.69947٨
F-statistic	8.150723	Durbin – Watson stat		2.27367٨
Prob (F statistic)	0.000			

١- وفي ضوء ما جاء بالجدول السابق يتضح للباحث أن قيمة مستوى الدلالة الخاص باختبار معنوية الحوكمة الرقمية **(DG)** مع الملاءة المهنية للمراجع الداخلي **(IAR)** أقل من قيمة مستوى المعنوية **(0.05)**، وهذا يعني وجود علاقة معنوية ذات دلالة إحصائية بين الحوكمة الرقمية (المتغير المستقل) والملاءة المهنية للمراجع الداخلي (المتغير التابع)

٢- أن قيمة مستوى الدلالة الخاص بكل من الحد الثابت **(C)** ومعدل العائد على حقوق الملكية **(ROE)** أقل من قيمة مستوى المعنوية **(0.05)** وهذا يعني وجود تأثير معنوي بين الملاءة المهنية للمراجع الداخلي **(IAR)** للشركة **(i)** في الفترة الزمنية **(T)** ومعدل العائد على حقوق الملكية، واتضح أيضا عدم وجود تأثير معنوي لكل من حجم الشركة **(FSIZE)** ونوع النشاط **(TA)** حيث أن قيمة مستوى المعنوية أكبر من **(0.05)** .

٦/٦/٢ نتائج اختبار الفرض الثاني

ينص الفرض الثاني على أنه "لا توجد علاقة ذات دلالة إحصائية بين الحوكمة الرقمية وجودة الأمن السيبراني"

قام الباحث بتطوير هذا الفرض من خلال صياغة نموذج الانحدار الخطي المتعدد وذلك للتعرف على العلاقة بين متغيرات الفرض السابق وذلك بعد إضافة المتغيرات الرقابية، ويوضح الجدول التالي رقم (١١) نتيجة الاختبار الإحصائي لنموذج الفرض الثاني:

جدول رقم (١١)
نموذج الانحدار الخطي المتعدد لنموذج الفرض الثاني

المتغيرات المستقلة	المعاملات	الخطأ المعياري	إحصائية T	مستوى الدلالة
C	-٦١,٩٠٦٩٣	26.84307	-2.306036	0.0216
DDG	0.٤٨٤٩٨٧	0.027924	16.66915	0.0000
DROE	1.0٥٠٨٥٧	0.090518	-5.464497	0.0000
DFSIZE	-2.214463	0.205074	-10.90317	0.0000
TA	0.012548	0.053725	0.227692	0.8186
R-squared	0.918322	Mean dependent var		0109287
Adjusted R-squared	0.820668	S.D. dependent var		1.524182
S.E.of regression	0.445545	Akaike info criterion		1.265337
Sum squared resid	56.89388	Schwarz criterion		١,٣٧٨٦٢٤
Log likelihood	-175.9105	Hannan- Quinn criter		1.315511
F-statistic	٣45.6449	Durbin – Watson stat		1.527246
Prob (F statistic)	0.000			

١- وفي ضوء ما جاء بالجدول السابق يتضح للباحث أن قيمة مستوى الدلالة الخاص باختبار معنوية الحوكمة الرقمية (DG) مع جودة الأمن السيبراني (QCS) أقل من قيمة مستوى المعنوية (0.05) وهذا يعني وجود علاقة معنوية ذات دلالة إحصائية بين الملاءة المهنية للمراجع الداخلي (المتغير المستقل) جودة الأمن السيبراني (المتغير التابع) .

٢- قيمة مستوى الدلالة الخاص بكل من الحد الثابت (C)، ومعدل العائد على الأصول (ROA)، وحجم منشأة عميل المراجعة (FSIZE) أقل من قيمة مستوى المعنوية (0.05) وهذا يعني وجود تأثير معنوي بين هذه المتغيرات وقيمة الشركة، واتضح أيضا عدم وجود تأثير معنوي لنوع النشاط (TA) حيث أن قيمة مستوى المعنوية أكبر من (0.05)

٦/٦/٣ نتائج اختبار الفرض الثالث

ينص الفرض الثالث على أنه "لا يوجد تأثير معنوي للحوكمة الرقمية على العلاقة بين الملاءة المهنية للمراجع الداخلي وجودة الأمن السيبراني"

قام الباحث بتطوير هذا الفرض للتحقق مما إذا كانت الحوكمة الرقمية تؤثر على العلاقة بين الملاءة المهنية للمراجع الداخلي وجودة الأمن السيبراني، ولاختبار ذلك الفرض تم صياغة نموذج الانحدار الخطي المتعدد، ويوضح الجدول رقم (١٢) نتيجة الاختبار الإحصائي للفرض الثالث من خلال مقارنة نتائج النموذج البحثي الثالث بالنتائج التي تم التوصل إليها في النموذج البحثي الثاني:

جدول رقم (١٢)

نموذج الانحدار الخطي المتعدد لنموذج الفرض الثالث

متغيرات النماذج Variable	العلاقة بين الملاءة المهنية للمراجع الداخلية وجودة الأمن السيبراني			
	متغيرات النموذج الثاني (قبل إدخال الحوكمة الرقمية)		متغيرات النموذج الثالث (بعد إدخال الحوكمة الرقمية)	
	Coefficient	Prob.	Coefficient	Prob.
C	-61.90693	0.0216	-72.20819	0.0066
DDG	0.484879	0.0000	0.537182	0.0000
(DG*IAR)	--	--	0.273662	0.0001
DROE	1.050857	0.0000	-0.524145	0.0000
DFSIZE	-2.214463	0.0000	-2.234768	0.0000
TA	0.012548	0.8186	0.030700	0.0.5575
R-squared	0.918322		0.920782	
Adjusted R-squared	0.820668		0.918579	
F- Statistic	345.6449		328.4942	
Prob (F-Statistic)	0.000		0.000	
Durbin-Watson stat	1.538247		1.589742	

١- وفي ضوء ما جاء بالجدول السابق فقد أسفرت نتائج الانحدار المتعدد بطريقة (LS) إلى أن إضافة متغير الحوكمة الرقمية في نموذج قياس العلاقة بين الملاءة المهنية للمراجع الداخلي وجودة الأمن السيبراني أدى إلى تحسين القدرة التفسيرية للنموذج من (0.9163) إلى (0.9206)، وأيضاً ارتفعت قيمة معامل الملاءة المهنية للمراجع الداخلي من)٠,٤٨٢٩) إلى (0.5391)، مما يدل على الأثر الإيجابي لإدخال الحوكمة الرقمية في نموذج العلاقة.

٢- بلغت قيمة مستوى الدلالة الخاص باختبار المعنوية (٠,٠٠٠١) للمتغير الذي يعكس التفاعل بين الحوكمة الرقمية والملاءة المهنية للمراجع الداخلي (DG*IAR) وهو أقل من قيمة مستوى

المعنوية (٠,٠٥)، مما يشير إلى وجود تأثير معنوي لإدخال الحوكمة الرقمية على العلاقة بين الملاءة المهنية للمراجع الداخلي وجودة الأمن السيبراني.

٣- مستوى الدلالة الخاص بكل من الحد الثابت (C)، والمتغيرات الرقابية الآتية: معدل العائد على الأصول (ROA)، وحجم منشأة عميل المراجعة (FSIZE) أقل من قيمة مستوى المعنوية (0.05) وهذا يعني وجود تأثير معنوي بين هذه المتغيرات وجودة الأمن السيبراني (QCS)، واتضح أيضا عدم وجود تأثير معنوي لنوع النشاط (TA) حيث أن قيمة مستوى المعنوية أكبر من (0.05) .

النتائج والتوصيات والتوجهات المستقبلية للبحث:

أولاً – النتائج:

في ضوء النتائج النظرية وما انتهت إليه الدراسات التطبيقية يمكن تقسيم النتائج إلى الآتي:

- **النتائج النظرية:**

١- تساهم الحوكمة الرقمية بشكل كبير في تحقيق الكفاءة والفعالية في تقديم الخدمات للمستفيدين والاستغلال الأمثل للموارد، والعمل على ضمان تدفق المعلومات بدقة وكفاية وتوقيت ملائم وجاهزية مستمرة، هذا بالإضافة إلى خلق البيئة والمناخ التنظيمي الملائم للبحث والتطوير الإداري المتواصل، علاوة على خلق بيئة تعليمية تعتمد بشكل كبير على النظم الإلكترونية المتقدمة بما يضمن تقديم آليات فعالة وداعمة لاتخاذ القرارات.

٢- توافر مقومات الحوكمة الرقمية السابق ذكرها من شأنه ان يدعم بقوة قيمة المنشأة والتي تعد ركيزة نجاح اساسية نحو نجاح المنشآت واستمراريتها في ظل تداعيات التطورات السريعة والمتلاحقة، وخاصة في ظل تأكيد المعيار الدولي رقم **1200A** المتعلق بالمراجعة الداخلية على أنه في ظل ممارسة العناية المهنية الواجبة، فإنه يجب على المراجع الداخلي أن يأخذ في الاعتبار استخدام التكنولوجيا وأدوات تحليل البيانات.

٣- الأمن السيبراني هو مجموعة من الإجراءات والسياسات والتقنيات التي تهدف إلى حماية أنظمة المعلومات والشبكات الرقمية من الاختراقات والتهديدات الإلكترونية، بهدف الحماية من الاختراقات الإلكترونية والبرمجيات الخبيثة والاعتداءات السيبرانية الأخرى، وكذلك ضمان سرية المعلومات وسلامتها وتوفير استجابة فعالة في حالة حدوث أي اختراق، كما يؤكد الباحث على أن مفهوم الأمن السيبراني يمتد ليشمل عملية حماية مواقع تخزين البيانات والتقنيات المستخدمة لتأمينها، كما يتضمن حماية تكنولوجيا المعلومات والاتصالات والأجهزة والبرمجيات .

٤- إدارة مخاطر الأمن السيبراني تتطلب مجموعة من الخطوات التي تتخذ بشكل دوري لمواجهة التهديدات الإلكترونية ومعالجتها من خلال رصدها وتحديدها وتقييمها، ومن أجل إدارتها بفاعلية، الأمر الذي ينبثق من خلال وجود نظرة شاملة لهذه المخاطر وتعاون من كافة الأفراد داخل المنشأة .

٥- إدارة مخاطر الأمن السيبراني تعتمد على وجود إستراتيجيات تعمل على تعزيز ترتيب أولويات المخاطر المطلوب معالجتها، لرصد التهديدات الأكثر ضررًا والمطلوب مواجهتها بشكل فوري.

٦- المهارات التكنولوجية التي يتمتع بها المراجع الداخلي تعزز من ملاءته المهنية بصدد التعامل مع متطلبات ومخاطر الأمن السيبراني بما يدعم جودة الأمن السيبراني وذلك في ضوء مؤشرات العالم الرقمي الجديد .

٧- المراجع الداخلي وهو بصدد تحقيق جودة الأمن السيبراني والحد من مخاطره عليه استخدام تقنيات وبرمجيات تخدم الإدارة وتقدم لها كل الأدوات التي تمكنها من الاستفادة من جودة المعلومات المحاسبية الإلكترونية في الوقت المناسب، هذا فضلاً عن تطوير أنظمة الرقابة للمراجعة الداخلية لكي تتلاءم مع أهداف وسياسات المنشأة بما يساهم في تحقيق جودة الأمن السيبراني في ضوء البيئة الرقمية، والعمل بشكل مستمر على وضع مجموعة من الممارسات والسياسات والإجراءات التي تساعد على رفع الملاءة المهنية للمراجع الداخلي .

النتائج على المستوى التطبيقي:

في ضوء نتاج الدراسة التطبيقية يمكن للباحث عرض الآتي:

١- أثبتت نتائج التحليل الإحصائي وجود علاقة ذات دلالة إحصائية بين الحوكمة الرقمية والملاءة المهنية للمراجع الداخلي حيث كانت قيمة معامل التحديد (٠.١٧٨٢) وهذه القيمة تشير إلى أن المتغيرات المستقلة في النموذج تفسر ما نسبته (17.8 %) من التغير في الملاءة المهنية للمراجع الداخلي حيث كانت إشارة معامل الانحدار موجبة وكانت القيمة الاحتمالية (Sig = 0.00) أقل من مستوى المعنوية (0.05) وهو ما يثبت عدم صحة الفرض الأول وقبول الفرض البديل .

٢- أثبتت نتائج التحليل الإحصائي وجود علاقة ارتباط قوية ذات دلالة إحصائية بين الحوكمة الرقمية وجودة الأمن السيبراني، حيث أدى تفعيل الملاءة المهنية للمراجع الداخلية إلى زيادة جودة الأمن السيبراني، حيث كانت قيمة معامل التحديد (0.820) وهذه القيمة تشير إلى أن المتغيرات المستقلة في النموذج تفسر ما نسبته (٨٢%) من التغير في جودة الأمن السيبراني حيث كانت إشارة معامل الانحدار موجبة وكانت القيمة الاحتمالية (Sig = 0.00) أقل من مستوى المعنوية (0.05) وهو ما يثبت عدم صحة الفرض الثاني وقبول الفرض البديل .

٣- أثبتت نتائج التحليل الإحصائي وجود علاقة تفاعلية بين الحوكمة الرقمية والملاءة المهنية للمراجع الداخلي ومدى تأثير هذه العلاقة على جودة الأمن السيبراني حيث كانت قيمة معامل التحديد (0.918) وهذه القيمة تشير إلى أن المتغيرات المستقلة في النموذج تفسر ما نسبته (91.8%) من التغير في جودة الأمن السيبراني حيث كانت إشارة معامل الانحدار موجبة وكانت القيمة الاحتمالية (Sig = 0.00) أقل من مستوى المعنوية (0.05) وهو ما يثبت عدم صحة الفرض الثالث وقبول الفرض البديل.

ثانياً – التوصيات:

في ضوء النتائج النظرية والعملية التي كشفت عنها الدراسة يوصي الباحث بالآتي:

١- ضرورة التعريف بمفاهيم حوكمة التحول الرقمي والعمل على تطبيقها وتعميمها على جميع الشركات بمختلف انتماءاتها.

٢- ضرورة توافر إدارة واعية لإنشاء بنية تحتية تعمل على تأسيس الاتصالات الرقمية وحماية الأمن السيبراني.

٣- ضرورة وجود قوانين وقواعد منظمة لآلية التحول الرقمي في مجال الأمن السيبراني، ورفع الملاءة المهنية لإدارة المراجعة الداخلية في هذا الشأن.

٤- أن التأهيل العلمي والعملي لم يعد هو المؤشر الوحيد للملاءة المهنية للمراجع الداخلي، ولكن التكيف والتعامل مع العالم الرقمي والإلمام بالقدرات التكنولوجية يمثل أحد الشروط الهامة لممارسة مهنة المراجعة الداخلية وخاصة فيما يتعلق بالأمن السيبراني.

٥- العمل على دعم وتعزيز المهارات الرقمية للموارد البشرية بالشركات بشكل عام وللمراجعين الداخليين بشكل خاص لضمان تطبيق الرقمنة والاستفادة منها في الحد من مخاطر الأمن السيبراني .

٦- توجيه الفكر المحاسبي لدعم المزيد من البحوث التي يمكن أن تقدم تفسيراً إضافياً حول دور التحول الرقمي في دعم الملاءة المهنية للمراجع الداخلي ودلالة انعكاس ذلك على حماية الأمن المعلوماتي بها .

ثالثاً – التوجهات المستقبلية للبحث:

في ضوء أهداف ومشكلة هذا البحث وما انتهى إليه من نتائج وتوصيات يمكن للباحث عرض أهم مجالات البحث المقترحة على النحو التالي:

١- انعكاسات حوكمة التحول الرقمي على العلاقة بين جودة التقارير المالية وقرارات المستثمرين .

٢- أثر حوكمة التحول الرقمي على العلاقة بين جودة تقرير المراجع الداخلي والكفاءة الاستثمارية.

٣- أثر التحول الرقمي على تفعيل دور المراجعة الداخلية لدعم قواعد الاستدامة .

٤- أثر دور المهارات الرقمية للمراجع الداخلي على العلاقة بين الحد من مخاطر الأمن السيبراني وقرارات المستثمرين .

قائمة المراجع:

أولاً – المراجع العربية:

١- أبو الخير، محمد حارس محمد، (٢٠٢٣)، "أثر جودة المراجعة الداخلية في الحد من من المخاطر السيبرانية بهدف دعم الاستقرار المالي في البنوك الإلكترونية – دراسة ميدانية"، المجلة العلمية للدراسات والبحوث المالية والإدارية، المجلد الخامس عشر، العدد الأول.

٢- أحمد، محمد عزام عبد المجيد، (٢٠٢١)، "_جودة المراجعة الداخلية ودورها في الحد من عدم تماثل المعلومات"، مجلة البحوث المالية والتجارية، كلية التجارة – جامعة بورسعيد، المجلد ٢٢، العدد ٣ .

٣- أميرهم، جيهان عادل ناجي، (٢٠٢٢)، " اثر جودة المراجعة الداخلية في الحد من مخاطر الامن السيبرانى و انعكاساته على ترشيد قرارات المستثمرين (دارسة ميدانية)"، مجلة البحوث المالية والتجارية، كلية التجارة – جامعة بورسعيد، المجلد ٢٣، العدد ٣.

٤- باناصر، لميس جميل، والصائغ، مها فيصل، (٢٠٢٠)، دور الآليات المحاسبية لحوكمة الشركات في الحد من ممارسات المحاسبة الإبداعية في شركات قطاع الاتصالات بمدينة الرياض: دراسة ميدانية، مجلة العلوم الإقتصادية والإدارية والقانونية، مجلد ٤، عدد١٥ .

٥- البغدادي، مروه فتحي السيد، (٢٠٢١)، "اقتصاديات الأمن السيبراني في القطاع المصرفي"، مجلة البحوث القانونية والإقتصادية، جامعة المنصورة، العدد ٧٦ .

٦- حامد، سحر سعيد، (٢٠١٩)، أثر الإسناد والتوقيت والوضع الوظيفي للمراجعة الداخلية على قرار المراجع الخارجي بشأن مدى اعتماده على وظيفة المراجعة الداخلية - دراسة تجريبية. رسالة دكتوراة، قسم المحاسبة والمراجعة، كلية التجارة جامعة دمهنور .

٧- رشوان، عبد الرحمن، وأبو رحمة، محمد، (٢٠٢٠)، التحول الرقمي وانعكاساته على ممارسة مهنة المحاسبة والتدقيق، المؤتمر الدولي الأول في تكنولوجيا المعلومات والأعمال .

٨- الرشيدي، طارق عبد العظيم، وعباس، داليا عادل، (٢٠١٩)، أثر الإفصاح عن مخاطر الأمن السيبراني في التقارير المالية على أسعار الأسهم وأحجام التداول دراسة مقارنة في قطاع تكنولوجيا المعلومات، مجلة المحاسبة والمراجعة (٢) .

٩- شحاتة، شحاتة السيد، على، عبدالوهاب نصر، والسيد، محمود محمد، (٢٠٢٣)، " أثر درجة الملاءة المهنية لمنشأة مراقب الحسابات على جودة أحكامه المهنية بشأن أمور المراجعة الأساسية: دليل من مصر- دراسة تجريبية"، مجلة البحوث المحاسبية، كلية التجارة – جامعة الإسكندرية، المجلد ٧، العدد ١ .

١٠-شحاتة، محمد موسى علي، (٢٠٢٠)، قياس أثر تفعيل أنشطة المراجعة الداخلية لآليات التَحَوُّل الرقمي على تعزيز المساءلة والشفافية وتحسين الأداء الحكومي مع دليل ميداني بالبيئة المصرية . المجلة العلمية للدراسات المحاسبية. ٢(العدد الأول الجزء الثاني) .

١١-صدقي، محمد عماد، (٢٠٢٢)، التحديات التي تواجه المراجع الداخلي وانعكاساتها على هيكل الرقابة الداخلية في ظل الرقمنة، المجلة العلمية للدراسات المحاسبية، المجلد ٤، العدد ٣.

١٢-عبد الرحيم، محمود محمد، (٢٠٢٠)، الدور التأثيرى لحوكمة تكنولوجيا المعلومات كمتغير وسيط في العلاقة بين المراجعة الداخلية كنشاط مضيف للقيمة والحد من مخاطر نظم المعلومات المحاسبية الإلكترونية: دراسة ميدانية، مجلة الدراسات والبحوث المحاسبية – قسم المحاسبة - كلية التجارة - جامعة بنها - العدد الثاني

١٣-عطية، أحمد صلاح، **(٢٠٢١)**، التحول الرقمي في مصر هل يلقي بمسؤوليات جديدة على المراجع؟، مجلة البحوث التجارية، كلية التجارة، جامعة الزقازيق، ٤٣ (١).
١٤-محروس، رمضان عارف رمضان، 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، المجلد (٢٣)- العدد الثالث.

ثانياً – المراجعة الأجنبية:

1- Alfaraih, M. And Alanezi, F.. **(2012)**. The Effectiveness of joint auditor requirements in promoting corporate disclosure quality. Arab Journal of Administrative Sciences, 19(2).
2- Alic, D. **(2021)**. The Role of Data Protection and Cybersecurity Regulations in Artificial Intelligence Global Governance: A Comparative Analysis of the European Union, the United States, and China Regulatory Framework.
3- Alsadoun, N. and Aljabr, Y. **(2014)**. Joint Audit and Cost of Equity Capital: Evidence from Saudi Arabia. Available at: www.fac.ksu.edu.sa/
4- Badawy, H., **(2021)** , The Impact of Assurance Quality and Level on Cybersecurity Risk Management Program on NonProfessional Egyptian Investors' Decisions: An Experimental Study, Alexandria Journal of Accounting Research, 3 (5) .
5- Betti, N. and Sarens, G. **(2021)**, "Understanding the internal audit function in a digitalised business environment", Journal of Accounting & Organizational Change,17 (2).
6- Bezerra Sales Sarlet, G., and Piñeiro Rodriguez, D. **(2023)**. Alternatives for an adequate structuring of the national data protection authority (ANPD) in its independent profile: proposals to overcome the technological challenges in the age of digital governance. International Cybersecurity Law Review, 4(2).
7- Bresciani , S., Ferraris, A., Romano, M., and Santoro, G. **(2021)**. Digital Transformation management for agile organizations: A compass to sail the digital world. Emerald Group Publishing.
8- Brous, P., Janssen, M., **(2015)**, Advancing e-government using the internet of things: a systematic review of benefits. In: Tambouris, E., et al. (eds.) EGOV 2015. LNCS. vol. 9248,. Springer, Cham , https://doi.org/10.1007/978-3-319- 22479-4 12.
9- Cameran, M., Ditillo, A. , and Pettinicchio, A. , **(2018)**. Audit Team Attributes Matter: How Diversity Affects Audit Quality, European Accounting Review, Vol.27, Issue 4.

10- Chang, Yu-Tzu,Chen, Hanchung,K. Cheng,Rainbow, and Chi,Wuchun., **(2019)** . The impact of internal audit attributes on the effectiveness of internal control over operations and compliance, Journal of Contemporary Accounting & Economics ,Vol.15,Issue 1,April .
11- Chen, H., D.Yang, X. Zhang and N. Zhou. **(2020)** . The Moderating Role of Internal Control in Tax Avoidance: Evidence from a COSO-Based Internal Control Index in China. The Journal of the American Taxation Association, Vol .42,No 1 .
12- Fatima , Samar , Desouza , Kevin C, Denford , James S. , Dawson, Gregory S, **(2021)**, What explains governments interest in artificial intelligence? A signaling theory approach, Economic Analysis and Policy, Vol. 71 .
13- Florakis C.C. Louca R. Michaely and M Weber, **(2020)** ,Cybersecurity Risk, Available at http://ssrn.com .
14- Hanisch, M., Goldsby, C. M., Fabian, N. E., and Oehmichen, J. **(2023)**. Digital governance: A conceptual framework and research agenda. Journal of Business Research, 162.
15- Idzi, Francis. M. and, Gornes, Ricardo, (2022), Digital governance: government strategies that impact public services, GPPG 2.
16- Institute of Internal Auditors, (IIA), **(2021)** .
17- Institute of Internal Auditors, (IIA), **(2022)** .
18- Ismanidar, N., Maksum, A., Gultom, P., and Meutia, R. **(2022)**. The effect of auditor competence and remote audit support on audit quality through digital-based governance with information technology as moderating variable in state financial audit. International Journal of Business and Technology Management, 4(2) .
19- Ji, X., Lu, W. and Qu, W., **(2017)**, Voluntary disclosure of internal control weakness and earnings quality: evidence from China, The International Journal of Accounting, 52 (1).
20- Jiin-Feng Chen and Wan – Ying Lin , **(2022)**, Measuring Internal Auditing Value, www.thilea.org, The IIA Global Internal Audit Survey.
21- Kalpesh, M. and Saurabh, B. **(2019)**. Impact of Digital on the future of internal audit. ExlService Holdings, Inc. Available at: www.exlservice.com/legal-disclaimer.
22- KPMG. (2020a). COVID-19 Role of Internal Audit Leaders. Available at: www.hpmg.com

23- Kumar, Dadabada Pradeep, **(2024)**, The Impact of Digital Technologies on E-Governance: A Comprehensive Analysis, Indian Institute of Managament Shillong 793018 Meghalaya. Indin
24- Kwilinski, Aleksy, Lyulyov, Oleksii and Pimonenko, Tetyana, **(2023)**, The Coupling and Coordination Degree of Digital Business and Digital Governance in the Context of Sustainable Development , Academic Editor: Luis Borges Gouveia .
25- Li H. W.G.No and T. Wang , **(2019)** ,SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors International Journal of Accounting Information Systems, 30.
26- Lobo. G., Paugam, L., Zhang, L., and Casta, J. **(2017)**. The Effect of Joint Auditor Pair Composition on Audit Quality: Evidence from Impairment Tests. Contemporary Accounting Research. 34 (1).
27- Lois, P., Drogalas, G., Karagiorgos, A. and Tsikalakis, K. **(2020)**. "Internal audits in the digital era: opportunities risks and challenges", EuroMed Journal of Business. 15(2).
28- Lois, P., Drogalas, G., Karagiorgos, A., Thrassou, A., and Vrontis, D. **(2021)**. Internal auditing and cyber security: audit role and procedural contribution. International Journal of Managerial and Financial Accounting, 13(1).
29- Maleh, Y., Sahid, A., and Belaissaoui, M. **(2021)**. A maturity framework for cybersecurity governance in organizations. EDPACS, 63(6) .
30- Manoharan, A. P., Melitski, J., and Holzer, M. **(2023)**. Digital governance: An assessment of performance and best practices. Public Organization Review, 23(1) .
31- Mendhurwar, S., and Mishra, R. **(2021)**. Integration of social and IoT technologies: architectural framework for digital transformation and cyber security challenges. Enterprise Information Systems, 15(4) .
32- Miskiewicz, R. Clean and Affordable Energy, **(2022)**, within Sustainable Development Goals: The Role of Governance Digitalization: Energies, 15
33- Morin, P. **(2020)**. NIST Cybersecurity Framework- Assessing the Maturity of your Cybersecurity Program.
34- of Cybersecurity in Internal Audit. Available at: www.iiarf.org.
35- Rouf, A. **(2011)**. The Corporate Social Responsibility Disclosure: A Study of Listed Companies in Bangladesh. Business and Economics Research Journal 2(3).

36- Shahimi S. and N. Mahzan, **(2018)** ,Building a research model and hypotheses development and findings of Exploratory Interviews International Journal of Management Excellence 10 (2).
37- Shang, X., He, Y., and Niu, H. **(2023)**. Research Status and Challenges of Global Digital Governance Based on Knowledge Graph Analysis. Scientific and Social Research, 5(5) .
38- Slapnicar, S., Vuko, T., Cular, M., and Drascek, M. **(2022)**. Effectiveness of cybersecurity audit. International Journal of Accounting Information Systems, 44 .
39- The Certified International Investment Analyst (CIIA), **(2021)** .
40- The Institute of Internal Auditors Research Foundation (IIARF). **(2018)**. The Future
41- Tiwari, S. P. **(2022)**. Organizational Competitiveness and Digital Governance Challenges. Archives of Business Research, 10(3).
42- U.S. Securities and Exchange Commission "SEC" **(2022a)**. "SEC Proposes Cybersecurity Risk Management Rules and Amendments for Registered Investment Advisers and Funds," press release, February 9. https://www.sec.gov/news/press-release/2022-20
43- Xiaofei, X., **(2020).** Internal audit strategies for dealing with digital risk in the digital economy. In 2nd International Scientific and Practical Conference on Digital Economy (ISCDE 2020) ,. Atlantis Press.
44- Yang, L., Lau, L., and Gan, H. **(2020)**. Investors' perceptions of the cybersecurity risk management reporting framework. International Journal of Accounting and Information Management, Vol. 28 (1) .
45- Yusif, S., and Hafeez-Baig, A. **(2021)**. A conceptual model for cybersecurity governance. Journal of applied security research, 16(4) .

Measuring the impact of the internal auditor's professional solvency on the quality of cybersecurity in light of digital governance

Abstract:

There is no doubt that digital governance has become of great importance at the global level, and digital governance is generally applied through procedures and processes through which organizations are directed and responsibilities are distributed to various parties, and internal audit plays an important role in being affected by digital governance, especially with regard to the quality of security. The main goal of the research was to study the impact of digital governance on the relationship between the professional solvency of the internal auditor and the quality of cyber security. To achieve this goal, the researcher formulated a set of hypotheses, perhaps the most important of which is: "There is no statistically significant relationship between digital governance and the professional solvency of the internal auditor." To test these hypotheses, a set of statistical methods were used to prepare the applied study with the aim of achieving the research objectives. This study resulted in a set of results, the most important of which were: The technological skills possessed by the internal auditor enhance his professional suitability in dealing with cyber security requirements and risks. In order to support the quality of cyber security in light of the indicators of the new digital world, the results of the statistical analysis also demonstrated the existence of a statistically significant relationship between digital governance and the professional competence of the internal auditor, as the value of the coefficient of determination was (17820.) and this value indicates that the independent variables in the model explain what (17.8%) of the change in the professional solvency of the internal auditor, where the sign of the regression coefficient was positive and the probability value (Sig = 0.00) was less than the level of significance (0.05), which proves the invalidity of the first hypothesis and the acceptance of the alternative hypothesis. In the end, the researcher recommended a set of Perhaps the most important recommendations are: Scientific and practical qualification is no longer the only indicator of the professional competence of the internal auditor, but adaptation and dealing with the digital world and familiarity with technological capabilities represent one of the important conditions for practicing the internal audit profession, especially with regard to cyber security.

Key Words: Digital Governance - The Professional Solvency of the Internal Auditor - The Quality of Cyber Security.