أثر توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى على قرار الاستثمار بالأسهم – دراسة تجريبية

The Impact of the Auditor's Assurance on Management's Assertions of Electronic Security Risks Management on Investment Decision in Stocks - an Experimental Study

د. هانى خليل فرج([1])

ملخص البحث:

استهدف البحث دراسة واختبار العلاقة بين توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى(الأمن السيبرانى cyber security) وقرار الاستثمار بالأسهم. وكذلك اختبار أثر تأهيل وخبرة المستثمرين على العلاقة محل الاختبار. ولقد اعتمد الباحث على إجراء دراسة تجريبية، على عينة من 65 من المستثمرين المؤسسيين والذين يتمثلون فى أمناء الاستثمار فى البنوك التجارية المصرية.

وتوصلت الدراسة إلى وجود تأثير لتوكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى إيجاباً ومعنوياً على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية. وتم استخدام متغيرات معدلة هى؛ مستوى التأهيل العلمى للمستثمر، ومستوى خبرة المستثمر. وخلصت الدراسة إلى عدم وجود تأثير معنوى لمتغيرى التأهيل والخبرة، كل على حده، على قرار الاستثمار بالأسهم، وكذلك عدم وجود تأثير معنوى لمتغيرى التأهيل والخبرة معاً على قرار الاستثمار بالأسهم.

الكلمات المفتاحية: مخاطر الأمن الإلكترونى، قرار الاستثمار بالأسهم، توكيد مراقب الحسابات، مزاعم الإدارة.

[1] **أستاذ مساعد بقسم المحاسبة ـ كلية التجارة – جامعة الاسكندرية .hany_khalil2007@yahoo.com**

Abstract:

The Research aimed to Study and Test the Relationship between the Auditor's Assurances on Management's Assertions of Electronic Security Risks Management (cyber security) on Investment Decision in Stocks. As well as Testing the Impact of the Qualification and Experience of Investors on the Relationship under Test. The Researcher Relied on conducting an Experimental Study on a Sample of 65 Institutional Investors who are Investment Trustees in Egyptian Commercial Banks.

The Study concluded that there is a Positive and Significant Impact of the Auditor's Assurances on Management's Assertions of Electronic Security Risks Management on Investment Decision in Stocks of Companies Listed on the Egyptian Stock Exchange. Modified Variables Were Used: The Level of Educational Qualification of the Investor, and the Level of Experience of the Investor. The Study concluded that there is no Significant Effect of the Qualification and Experience Variables Separately on the Decision to Invest in Stocks, as well as the Absence of a Significant Effect of the Qualification and Experience Variables together on the Decision to Invest in Stocks.

KeyWords: Electronic Security Risks, Investment Decision, Auditor Assurance, Management's Assertions.

1- المقدمــة:

أدت هجمات الأمن الإلكترونى على مستوى البيانات الهامة للشركات الكبرى والحكومات إلى لفت إنتباه الشركات إلى الآثار التجارية التى تمثل خرقاً كبيراً فى الشركة يمكن أن تسبب، بما فى ذلك؛ الإضرار بالسمعة، وفقدان الملكية الفكرية، وتعطيل العمليات التجارية الرئيسية، والغرامات والعقوبات التى تفرضها الحكومات، وتكاليف التقاضى، والاستبعاد من الأسواق الاستراتيجية.

كما أدى خطر حدوث مثل هذه الآثار إلى إهتمام كبير بشأن الأمن الإلكترونى وإدارته من قبل المستثمرين والعملاء وشركاء الأعمال والمنظمين، ونتيجة لذلك أصبحت إدارة مخاطر الأمن الإلكترونى من الأمور الرئيسية فى مجال الأعمال التى تواجه الإدارة العليا ومجالس إدارات معظم الشركات(Rosati et al.,2017).

وتعتبر إدارة هذه المشكلة التجارية تحدياً خاصاً لأنه حتى الشركات ذات المستوى المرتفع من النضج سيكون لديها إدارة مخاطر أمن إلكترونى متبقية تتمثل فى مخاطر الأمن الإلكترونى المادى، ويمكن أن يحدث الخرق ولا يتم اكتشافه فى الوقت المناسب. علاوة على ذلك ، أن مخاطر الأمن الإلكترونى من غير المرجح أن تتغير فى المستقبل بسبب مجموعة من العوامل، منها إعتماد الشركات على تكنولوجيا المعلومات، وتعقيد شبكات تكنولوجيا المعلومات، والاعتماد الواسع على البشر، والحاجة المستمرة إلى المعلومات لدفع عملية صنع القرار (Navarro, P. & S. Steve, 2021).

وبسبب أهمية مخاطر الأمن الإلكترونى اهتمت إدارات الشركات وأصحاب المصلحة بالحصول على معلومات مفيدة عنها لتمكينهم من إتخاذ القرارات الرشيدة. مثال: برنامج إدارة مخاطر الأمن الإلكترونى، وأدوات إدارية لمساعدتهم على الوفاء بمسئولياتهم الرقابية. كما أنهم يرغبون فى الحصول على معلومات من جهة مستقلة لتقييم فعالية الإدارة فى إدارة مخاطر الأمن الإلكترونى.

وقد يستفيد المستثمرون من التوكيد على المعلومات حول الأمن الإلكترونى للشركة وبرنامج إدارة المخاطر، وتهدف هذه المعلومات إلى مساعدتهم على فهم مخاطر الأمن الإلكترونى التى يمكن أن تهدد تحقيق هدف الشركة التشغيلى، وإعداد التقارير بصورة سليمة. وبالتالى ، يكون لها تأثير سلبى على قيمة الأعمال وسعر السهم. كما قد يستفيد شركاء العمل من المعلومات حول إدارة مخاطر الأمن الإلكترونى للشركة كجزء من التقييم الشامل للمخاطر. كما تهدف هذه المعلومات إلى مساعدة الأعمال فى أن يحدد الشركاء بعض الأمور مثل: ما إذا كان هناك حاجة لموردين متعددين لسلعة أو خدمة ومدى اختيارهم لمنح الإئتمان للشركة، وقد يستفيد بعض منظمى الصناعة من المعلومات حول مخاطر الأمن الإلكترونى للشركة لدعم دورهم الرقابى. تبعاً لذلك، بدأت الإدارة وكبار مديرى الشركات فى طلب تقارير توكيد عن فعالية إدارة مخاطر الأمن الإلكترونى الخاصة بهم من مراقبى الحسابات(AICPA,2018b).

2- مشكلة البحث:

يعد الأمن الإلكترونى أحد المجالات الهامة فى الوقت الحاضر، نظراً لما تواجهه منظمات الأعمال من تهديدات إلكترونية، حيث يوفر الأمن الإلكترونى حماية ضد الهجمات الإلكترونية وحماية معلوماتها وضمان إستمرار خدماتها وسلامة التقارير المالية. كما تعرض العديد من مجالس إدارات الشركات فى الأونة الأخيرة للعديد من الدعاوى القضائية نتيجة حدوث إختراقات إلكترونية لأنظمتها، ترتب عليها فقدان سمعة الشركات وتعطيل العمليات الرئيسية. لذلك تولى العديد من الشركات فى الوقت الحاضر الاهتمام بالتوكيد المهنى على مزاعم الادارة عن إدارة مخاطر الأمن الإلكترونى من مراقب حسابات لتوفير مزيد من الثقة للمتعاملين مع الشركة وخاصة المستثمرين، لتحسين قدراتهم على تقييم إدارة مخاطر الأمن الإلكترونى والتى تؤثر بالتبعية على قرارات الاستثمار فى الأسهم(Kamiya et al., 2021).

ويمكن التعبير عن مشكلة البحث فى كيفية الإجابة تجريبياً على التساؤلين التاليين؛

ماهو شكل واتجاه العلاقة بين توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى على قرار الاستثمار بالأسهم؟، وهل تختلف هذه العلاقة بإختلاف مستوى التأهيل والخبرة للمستثمر المؤسسى؟.

3- هدف البحث:

يهدف البحث إلى دراسة واختبار العلاقة بين توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى وقرار الاستثمار بالأسهم. وكذلك اختبار أثر تأهيل وخبرة المستثمرين على العلاقة محل الاختبار، وذلك من خلال دراسة تجريبية.

4- أهمية ودوافع البحث:

تكمن **الأهمية الأكاديمية** للبحث فى كونه يركز على قضية هامة وهى تسليط الضوء على أثر توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى على قرار الاستثمار بالأسهم، وهى قضية تتسم بندرة الأبحاث المصرية بشأنها.

كما تتمثل **الأهمية العملية** للبحث فى مردوده على ترشيد قرارات أصحاب المصالح، خاصة قرار الاستثمار فى الأسهم، نتيجة توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى.

ورغم كثرة **دوافع البحث** إلا أن أهمها ندرة البحوث المحاسبية فى مصر، خاصة تلك التى تهتم بدراسة واختبار الآثار المترتبة على توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى تجريبياً على قرار الاستثمار بالأسهم.

5- حدود البحث:

وفقاً لهدف البحث ومشكلته سوف يقتصر البحث على دراسة واختبار العلاقة بين توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى وقرار الاستثمار بالأسهم. وكذلك اختبار أثر تأهيل وخبرة المستثمرين على العلاقة محل الاختبار، وذلك من خلال دراسة تجريبية.

ويخرج عن نطاق البحث القرارات الأخرى بخلاف قرار الاستثمار (مثل: تنبؤات المحللين الماليين)، كما يخرج عن نطاق البحث أيضاً، المتغيرات المعدلة الأخرى ماعدا مستوى التأهيل والخبرة للمستثمرين(مثل: حجم مكتب المحاسبة وتخصصه الصناعى)، وتأثيرها على العلاقة محل الاختبار. وسوف تقتصر المعالجات التجريبية على المتغير المستقل فى حالة عدم وجود توكيد لمراقب الحسابات أو مع وجوده. وأخيراً، فإن قابلية تعميم نتائج البحث تتوقف على منهجية الدراسة التجريبية بمحدداتها، خاصة محددات اختيار عينة البحث.

6- فروض البحث:

سوف يتم اشتقاق فروض البحث نظرياً لاحقاً، على النحو الأتى:

H_1: يؤثر توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى إيجاباً ومعنوياً على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية.

H_2: يختلف التأثير الإيجابى المعنوى لتوكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية باختلاف مستوى التأهيل العلمى للمستثمر.

H_3: يختلف التأثير الإيجابى المعنوى لتوكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية باختلاف مستوى خبرة المستثمر.

7- خطـة البحـث:

إنطلاقاً من مشكلة البحث ولتحقيق هدفه واختبار فروضه فى ضوء حدوده، فسوف يستكمل البحث على النحو التالى:

1/7- إدارة مخاطر الأمن الإلكترونى من منظور مهنى.

2/7- توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى: المفهوم والمتطلبات والمردود المهنى.

3/7- تحليل العلاقة محل الدراسة واشتقاق فروض البحث.

4/7 - نموذج ومنهجية البحث.

5/7- النتائج والتوصيات ومجالات البحث المقترحة.

1/7- إدارة مخاطر الأمن الإلكترونى من منظور مهنى:

يعرف الأمن الإلكترونى([2]) بأنه مجموعة الأدوات التى تعمل على الحد من مخاطر الهجمات الإلكترونية على البرامج والأنظمة والشبكات. وتشمل هذه الأدوات السياسات والضوابط والأنظمة مثل: الحوائط النارية، وبرامج مكافحة الفيروسات، وأنظمة كشف الإختراق، والتشفير (Amoroso,2007). ويعرف المعهد الوطنى للمعايير والتكنولوجيا NIST ([3]) الأمن الإلكترونى على أنه عملية لحماية المعلومات عن طريق منع الهجمات واكتشافها والرد عليها(NIST,2013a). كما يعرفه Kissel(2013) على أنه النشاط الذى بموجبه يتم حماية أنظمة المعلومات والإتصالات والدفاع ضد الضرر أو الاستخدام غير المصرح به أو الاستغلال من خلال الانتهاكات.

ويعرفه ماجد (2016) على أنه مجموعة من الأدوات والعمليات التكنولوجية المصممة لحماية الأنظمة والبرامج من الإختراقات الإلكترونية، كما أنه نشاط يعمل على حماية الموارد المالية والبشرية ومحاولة الحد من الأضرار الناتجة عن مخاطر الأمن الإلكترونى. وتعرفه هيئة الإتصالات وتقنية المعلومات السعودية بأنه أمن المعلومات على الحاسب الآلى بغرض حماية المعلومات من أى هجوم خارجى من خلال إستخدام مجموعة وسائل فنية تكنولوجية تعمل على حماية تلك الأنظمة، ويعد هو المجال الخامس للحروب الحديثة(الهيئة الوطنية للأمن السيبرانى، السعودية، 2017).

وتعرفه السمحان(2020) على أنه الوسيلة لحماية الفضاء الإلكترونى([4]) من الإختراقات الإلكترونية ومنع الوصول غير المصرح به للمعلومات الإلكترونية بهدف الحفاظ على الأنظمة المعلوماتية. وعرفته وزارة الدفاع الأمريكية على أنه كل الإجراءات اللازمة لحماية المعلومات من

([2]) يعرف بالأمن السيبرانى المأخوذة من كلمة Cyber وهى صفة لأى مجال مرتبط بالحاسبات وتكنولوجيا المعلومات أو فضاء الإنترنت.

(3) National Institute of Standards and Technology (NIST)

([4])الفضاء الإلكترونى: هو البيئة الرقمية المكونة من مجموعة أنظمة وشبكات وأجهزة وبرامج ومستخدمين.

الجرائم الإلكترونية، كما إعتبرالإتحاد الأوروبى الأمن الإلكترونى بأنه قدرة الأنظمة المعلوماتية على الحماية ضد جرائم الإختراق التى تحدث للبيانات(encyclopedia.org,2020).

ويعرفه(Santhosh & Thiyagu (2021 على أنه فرع من فروع تكنولوجيا المعلومات يعمل على حماية الأنظمة والبرامج والشبكات ضد الهجمات الرقمية على المعلومات الهامة أو تغييرها أو تخريبها أو تعطيل الأعمال التجارية أو ابتزاز مستخدمى هذه الأنظمة للحصول على الأموال، وهو مايسمى بالجرائم الإلكترونية. وبحسب تعريف الموقع الرسمى لوزارة الإتصالات وتكنولوجيا المعلومات فى مصر عام 2021 ، فإن الأمن الإلكترونى هو مجموعة الوسائل التى يتم من خلالها منع الاستخدام غير المصرح به للمعلومات الإلكترونية.

وتقوم إدارة الشركات بتبنى برامج لإدارة مخاطر الأمن الإلكترونى، والتى تعرف على أنها مجموعة من السياسات والعمليات والضوابط الرقابية التى من شأنها حماية المعلومات والأنظمة من الهجمات الإلكترونية التى قد تضر تحقيق الشركة لأهدافها واكتشافها فى الوقت المناسب ومعالجتها(AICPA,2021).

ويعتبر مصطلح أمن المعلومات والأمن الإلكترونى مصطلحان متشابهان بشكل كبير، حيث توجد بعض الفروق بينهما، ويعتبر أمن المعلومات أشمل من الأمن الإلكترونى، فالأمن الإلكترونى مجال من مجالات أمن المعلومات، حيث يهتم أمن المعلومات بتوفير حماية للأنظمة من خلال الوسائل المختصة بالتعرف المسبق على التهديدات والتصدى لها، وهو بذلك يشمل تأمين كافة البيانات والمعلومات المتداولة عبر جميع الشبكات والتى يتم تخزينها بالوسائل الإلكترونية المتعددة، وكذلك المعلومات الورقية. بينما يركز الأمن الإلكترونى على أنظمة الدفاع عن الشبكات والأنظمة دون التركيز على الوسائل التأسيسية مثل وسائل التشفير(AICPA,2021).

ويرى الباحث أن أهمية الأمن الإلكترونى تنبع على المستوى الفردى من خلال فقدان معلومات هامة للفرد، وعلى المستوى المجتمعى من خلال الضرر الحادث للبنية الأساسية فى المجتمع، وهو ما يتطلب الحفاظ عليها ضد الإختراقات الإلكترونية.

ويوفر الأمن الإلكترونى ثلاثة عناصر هامة فى المعلومات وهى السرية، والسلامة، والجاهزية(الإتاحة). ويوفر الأمن الإلكترونى حماية للمعلومات والأجهزة والشبكات وتحديد نقاط الضعف الجوهرية فى الأنظمة مع توفير بيئة آمنة للعمل بها عبر شبكة الإنترنت، مما يعزز من ثقة المساهمين وأصحاب المصالح بالشركة. ويهدف وجود الأمن الإلكترونى إلى التصدى للهجمات الإلكترونية، مع بقاء البنية التحتية الإلكترونية صالحة للعمل وتوفير المتطلبات اللازمة للحد من مخاطر هذه الهجمات، والتعرف على نقاط الضعف الموجودة بالأنظمة، وإتخاذ كافة الإجراءات اللازمة لحماية المجتمع من أضرار هذه الهجمات، وتوفير آليات لمواجهة هذه الهجمات بأقل أضرار ممكنة (السمحان، 2020).

ويذكر داود(2000) أن الجرائم الإلكترونية صعبة الاكتشاف مع وجود سرعة وغياب الدليل، وتوفر خبرة كبيرة للقائم بها مع ضعف وسائل الاكتشاف لها.

ويمثل الإحتيال عبر الإنترنت حالياً تحدياً خطيراً للمجتمع، فقد أصبح هذا الموضوع من أهم خمسة تهديدات تواجه العالم الآن والإقتصاد العالمى، وتهدد مستقبل الشركات، وتفقد أصحاب المصالح بالشركات الثقة فى التعامل مع الشركات التى يحدث بها اختراقات إلكترونية (Santhosh& Thiyagu, 2021).

ويرى البعض (Demetz& Bachlechner, 2013; Lawrence et al., 2015) أن الحفاظ على الأمن الإلكترونى أمر بالغ الأهمية بالنسبة للشركات للحفاظ على إستمرارية خدماتها وسلامة تقاريرها وحماية معلوماتها الإستراتيجية. وبناء على ذلك تقوم الشركات فى الوقت الحالى بإستثمارات كبيرة فى مختلف الأنشطة المتعلقة بالأمن الإلكترونى، هذه الإستثمارات تمثل نواحى قوة فى الشركات حيث تساعد على التخصيص الفعال للموارد داخل الشركات، إلا أن هناك العديد من العقبات وراء ذلك الاستثمار منها؛ صعوبة تحديد المردود من هذه الإستثمارات من حيث وفورات التكاليف التى تترتب على هذا الإنفاق والتى تتمثل فى تخفيض الإختراقات الأمنية، والتى تمثل الفرق بين تكاليف الإختراقات الأمنية قبل الإنفاق الإستثمارى فى الأمن الإلكترونى والتكاليف اللاحقة المرتبطة بالإختراقات الفعلية للأمن الإلكترونى بعد الإنفاق الإستثمارى. وهى تمثل وفورات

يصعب ملاحظتها بشكل ملموس، لذلك تميل الشركات إلى تأجيل الاستثمار فى الأمن الإلكترونى طالما لم يحدث لها إختراق إلكترونى، ممايعنى إستخدامهم لنهج تفاعلى وليس إستباقى فى موضوع الاستثمار فى الأمن الإلكترونى. ولقد دعا ذلك إلى المطالبة بالمشاركة فى تبادل المعلومات بين الشركات بخصوص الأمن الإلكترونى والإختراقات التى تحدث للشركات مما يقلل من تهديدات هذه الإختراقات بناء على تجارب الشركات، والذى قد يقلل من الإستثمارات الموجهة من الشركات نحو الأمن الإلكترونى.

كما تذكر الدراسات (Cavusoglu et al.,2004; Ghosh & Li, 2013)أن تبادل المعلومات بين الشركات له قيود قانونية محتملة للمشاركة بالمعلومات المتعلقة بالأمن الإلكترونى، كما قد يكون له تأثير على القدرة التنافسية للشركات فى سوق العمل. ومن المتوقع أن تصل تكاليف الإختراقات الإلكترونية إلى ستة تريليون دولار عام 2025. ويمكن تصنيف تكاليف الإختراقات الإلكترونية إلى مجموعتين؛ **المجموعة الأولى: تكاليف مؤقتة** (قصيرة الأجل) وهى التى يتم تحملها فقط خلال الفترة التى حدث فيها الإختراق، وتشمل خسارة الأعمال، وإنخفاض الإنتاجية نتيجة عدم توفر الموارد، وتكاليف الإصلاح للموارد المخترقة، وتكاليف جمع الأدلة عن القائم بالإختراق، والتكاليف المتعلقة بتوفير معلومات للعملاء وأصحاب المصالح المتعلقة بوسائل الإعلام المختلفة للإفصاح عن الإختراق. **والمجموعة الثانية: تكاليف دائمة** (طويلة الأجل) وهى التى تؤثر على عدة فترات محاسبية. وهى ترتبط بضياع التدفقات النقدية المستقبلية للشركة وفقد العملاء وتحولهم إلى المنافسين، وعدم القدرة على جذب عملاء جدد بسبب ضعف المنظومة الأمنية الإلكترونية، وفقد ثقة المستثمرين، وزيادة تكاليف التأمين على الشركة، وزيادة تكلفة رأس المال.

كما يمكن تقسيم هذه التكاليف إلى نوعين؛ **تكاليف ملموسة** مثل: تكاليف المبيعات أوالخدمات المفقودة، وتكاليف المواد الخام والعمالة والتأمين. **وتكاليف غير ملموسة** تتمثل فى ضياع الثقة لدى الأطراف المتعددة المرتبطة بالشركة.

كما تذكر دراسة (Gordon et al.,(2006 وجود أثار إيجابية للإفصاح عن إدارة مخاطر الأمن الإلكترونى فى الشركات، كما زادت نسب الإفصاح الإختيارى بعد تطبيق مرسوم SOX مما زاد من الإفصاح عن إدارة مخاطر الأمن الإلكترونى بالتبعية، على الرغم من عدم وجود إشارة صريحة فى المرسوم عن الإفصاح عن إدارة مخاطر الأمن الإلكترونى إلا أن مطالبة الإدارة تقديم تقرير عن تقييم هيكل الرقابة الداخلية يعنى ضمناً مسئوليتها عن الإفصاح عن المخاطر الإلكترونية ضمن هذا التقرير، خاصة وأن ضوابط أمن المعلومات فى الشركة هى جزء من هيكل الرقابة الداخلية(ICS) وتؤثر على درجة الثقة فى تقارير الإدارة المنشورة.

وتشير الدراسات (Jeong et al., 2018; Janvrin & Wang, 2019; Kelton & Pennington,2019) إلى وجود تأثير سلبى على الشركات نتيجة الإفصاح عن الإختراقات الإلكترونية التى تحدث لها ويمتد هذا التأثير للصناعة كلها بما يعرف (بتأثير العدوى)، حيث وجدت الدراسة أن إحتمالات الاستثمار فى شركة غير مخترقة تكون أقل عندما تواجه شركة فى نفس الصناعة إختراق إلكترونى، كما أن الإفصاح عن الإختراقات الإلكترونية التى تحدث لشركة ما فى صناعة معينة قد يفيد فعلياً الشركات المناظرة لها فى نفس الصناعة نتيجة وجود مردود إيجابى غير عادى فى الشركة المنافسة غير المخترقة لأنها تكون فى مركز تنافسى أقوى من الشركة المخترقة لفترة معينة(تأثير المنافسة). كما أن هناك تأثير أخر على سلوك إدارة الشركة بعد اكتشاف حدوث إختراق للأمن الإلكترونى، حيث وجد أن هناك إدارة للأرباح بواسطة الإدارة عندما يكون الإختراق لمعلومات مالية لأنهم يتوقعون الإستغناء عنهم بعد حدوث الإختراق.

وتتفق بعض الدراسات (Gal-Or&Ghose, 2005; Biener et al., 2015; Amir et al., 2018; Lawrence et al., 2018)على أن الشركات أصبحت تشعر بقلق أكبر إزاء الإختراقات الإلكترونية المحتملة والفعلية للعملاء، مع وجود حقيقة عدم إمكانها القضاء على مخاطر الأمن الإلكترونى بدرجة 100%. كما أن تدابير الأمن الإلكترونى تصبح فى مرحلة ما أكثر تكلفة من منفعتها، لذلك يحتاج المسئولون عن منع الإختراقات الإلكترونية داخل الشركات وكذلك مراقبى الحسابات الذين يقدمون خدمات توكيدية بشأن إدارة مخاطر الأمن الإلكترونى إلى إشراك شركات

التأمين فى هذه المخاطر أملاً فى نقل بعض من هذه المخاطر المتوقعة مستقبلاً على شركات التأمين. وفى الحقيقة فإن هذه الوسيلة تمثل أداة فعالة فى تقليل مخاطر الأمن الإلكترونى ويجب وضعها كخطوة أولى فى سياق برامج إدارة مخاطر الأمن الإلكترونى.

ومن ناحية أخرى، نجد أن شركات التأمين متحفظة للغاية فى تسعير أقساط التأمين الإلكترونى بسبب الخوف من حدوث (الإعصار الإلكترونى)، والذى قد يحدث عندما تغمر المطالبات بسبب المخاطر لشركات التأمين. إلا أن وجود سوق تأمين إلكترونى فعال من شأنه تشجيع الشركات على زيادة إستثماراتها فى أنشطة الأمن الإلكترونى ويعد ألية هامة لتحسين المستوى العام للحماية من مخاطر الأمن الإلكترونى فى الشركات(Lawrence et al., 2018) .

لذلك أصدرت لجنة البورصة الأمريكية SEC فى 2018 دليل إرشادات الأمن الإلكترونى الخاص بمتطلبات الإفصاح عن الأمن الإلكترونى بواسطة إدارات الشركات ويتضمن قسمين:

القسم الأول: تضمن طبيعة الأمن الإلكترونى وإرشادات الأمن الإلكترونى منذ 2011 وتطوير إرشادات عام 2018 بغرض التوسع فى متطلبات الإفصاح عن إرشادات عام 2011.

القسم الثانى: تضمن مجموعتين؛

المجموعة الأولى: مراجعة قواعد الإفصاح عن مشاكل الأمن الإلكترونى وتشمل:

- **الأهمية النسبية:** يركز على توجيه الإهتمام نحو مخاطر وحوادث الأمن الإلكترونى عند إعداد تقارير الإدارة السنوية، وخاصة الحوادث الهامة من وجهة نظر المستثمرين والأضرار الناتجة عنها، كما يجب أن يستوفى الإفصاح خاصيتى الملاءمة والإكتمال عند الإفصاح عن إدارة مخاطر الأمن الإلكترونى.
- **عوامل المخاطرة:** يجب الإفصاح عن حوادث الأمن الإلكترونى الفعلية والمتوقعة والتى تمثل مخاطر خاصة على الشركة فى سياق الإفصاح عن إدارة مخاطر الأمن الإلكترونى للمستثمرين.
- **المركز المالى ونتائج الأعمال:** يجب الإفصاح عن أى حوادث أمن إلكترونى يكون لها تأثير جوهرى على المركز المالى ونتائج الأعمال.
- **وصف طبيعة الأنشطة:** يجب الإفصاح عن أى حوادث أمن إلكترونى يكون لها تأثير جوهرى على

طبيعة نشاط الشركة والعلاقات مع الموردين أوالعملاء أو أى أطراف خارجية أخرى.

- **الإجراءات القانونية:** يجب الإفصاح عن أى قضايا متعلقة بإدارة مخاطر الأمن الإلكترونى.
- **سياسات الإفصاح فى القوائم المالية:** قد تؤثر حوادث الأمن الإلكترونى على عناصر القوائم المالية من إيرادات أو مصروفات أو تدفقات نقدية، وبالتالى لابد من الإفصاح عن هذه الأثار ضمن الإيضاحات المتممة للقوائم المالية.
- **دور مجلس الإدارة:** يجب الإفصاح عن دور مجلس الإدارة بخصوص برنامج إدارة مخاطر الأمن الإلكترونى والذى يؤثر إيجاباً على المستثمرين.

المجموعة الثانية: السياسات والإجراءات الخاصة بالرقابة على الإفصاح عن إدارة مخاطر الأمن الإلكترونى وتشمل:

- **إجراءات الرقابة:** يجب التأكد من وجود تصميم جيد لضوابط وإجراءات الرقابة على برنامج إدارة مخاطر الأمن الإلكترونى المطبق بالشركة فهى جزء من أعمال لجنة المخاطر بالشركة.
- **المعلومات الداخلية:** يجب أن لايستغل الأطراف الداخلية معرفتهم بأحداث جوهرية حول مخاطر الأمن الإلكترونى فى التعامل على الأوراق المالية.
- **الإفصاح الإنتقائى:** يجب عدم الإفصاح عن المعلومات المتعلقة بإدارة مخاطر الأمن الإلكترونى بشكل إنتقائى وهى المعلومات غير المعلنة للمستثمرين(SEC, 2018).

وتذكر الدراسات (AICPA, 2018a; AICPA,2018b; Frank et al.,2021) أن هناك إرتفاع كبير فى الدعاوى القضائية المرفوعة ضد مجالس إدارات الشركات الحادث بها إختراقات إلكترونية، مما يعنى زيادة المسئوليات على الإدارة بعد حدوث هذه الإختراقات، خاصة وأن هذه الإختراقات يترتب عليها الإضرار بسمعة الشركة، وفقدان الملكية الفكرية، وتعطيل العمليات الرئيسية، ووجود غرامات وعقوبات بالإضافة لتكاليف التقاضى. لذلك تحتاج الإدارة لأدوات تساعدها على مواجهة هذه المخاطر الجديدة لمساعدتها على الوفاء بمسئولياتها. وفى نفس الوقت يحتاج أصحاب المصالح إلى معلومات مفيدة فى الوقت الملائم حول جهود الإدارة لتفادى مخاطر الأمن الإلكترونى بالشركة.

وفى نفس السياق، قدمت مجموعة من الدراسات المسحية (Gordon & Loeb, 2006; Agrafiotis et al., 2018; Curtis et al., 2018; Haapamäki& Sihvonen, 2019) العديد من الإرشادات حول دور الإدارة عن تفادى مخاطر الأمن الإلكترونى والتى تتضمن ضرورة:

- تبادل المعلومات عن الإختراقات الأمنية لزيادة مستوى أمان المعلومات.
- تنفيذ برامج أمن إلكترونى وتطويرة بإستمرار.
- تقييم تكاليف ومنافع الاستثمار فى برامج الأمن الإلكترونى.
- الحفاظ على كفاءة برامج الأمن الإلكترونى لحماية إستراتيجية الشركة.
- تحسين هياكل الرقابة الداخلية لتحسين مستوى برامج الأمن الإلكترونى.
- وجود تعاون فعال بين إدارتى المراجعة الداخلية ونظم المعلومات بشأن إدارة مخاطر الأمن الإلكترونى.
- إفصاح الإدارة عن إدارة مخاطر الأمن الإلكترونى لتقليل الإختراقات فى المستقبل.
- وضع مسئول نظم المعلومات ضمن فريق الإدارة العليا لزيادة آليات الحوكمة ضد مخاطر الأمن الإلكترونى.

ولقد قام AICPA عام 2017 بوضع مجموعتين من المعايير، المجموعة الأولى: **معايير الوصف** لكى تستخدمها الإدارة عند تنفيذ برامج إدارة مخاطر الأمن الإلكترونى، وإعداد تقرير الإدارة عن إدارة مخاطر الأمن الإلكترونى. والمجموعة الثانية: **معايير الرقابة** وهى التى يستخدمها مراقب الحسابات لتقييم فاعلية تصميم وتشغيل الضوابط داخل برنامج إدارة مخاطر الأمن الإلكترونى، ويلخص ملحق رقم (1) معايير الوصف اللازمة للإدارة، ومعايير الرقابة للتوكيد على تكنولوجيا المعلومات ومخاطر الأمن الإلكترونى. (AICPA, 2017).

أما بشأن الجهود المصرية فى دعم والتصدى لمخاطر الأمن الإلكترونى، فقد نص الدستور المصرى عام 2014 (م31) على أن *"أمن الفضاء المعلوماتى هو جزء أساسى من منظومة الإقتصاد والأمن القومى، وتلتزم الدولة بإتخاذ التدابير اللازمة للحفاظ عليه على النحو الذى ينظمه القانون"*. ثم صدر قرار رئيس الوزراء رقم 2259 لسنة 2014 بإنشاء المجلس الأعلى للأمن

السيبرانى بغرض وضع إستراتيجية وطنية لمواجهة الأخطار والهجمات السيبرانية والإشراف على تنفيذها وتحديثها. ثم صدر قرار رئيس الوزراء رقم 1631 لسنة 2016 بتحديد مهام المجلس الأعلى للأمن السيبرانى وتشكيل المكتب التنفيذى للمجلس، وتشكيل الأمانة الفنية للمجلس وتحديد مهامهم. ثم صدر قرار رئيس مجلس الوزراء رقم 994 لسنة 2017 بإلزام كافة الجهات الحكومية بتنفيذ قرارات المجلس الأعلى للأمن السيبرانى بشأن تأمين البنية التحتية للإتصالات وتكنولوجيا المعلومات.

تلى ذلك إصدار الإستراتيجية الوطنية للأمن السيبرانى (2017- 2021) والتى تضمنت أهم التحديات والأخطار السيبرانية، وأهم القطاعات الحيوية المستهدفة، وعناصر التهديدات السيبرانية، وركائز التوجه الإستراتيجى للخطر السيبرانى، وآلية تنفيذ الإستراتيجية، وأهم البرامج الإستراتيجية التى سيتم تنفيذها. وهدفت إلى مواجهة المخاطر السيبرانية وتعزيز الثقة فى البنية التحتية للإتصالات والمعلومات وتطبيقاتها وخدماتها من أجل التنمية الشاملة وتأمينها من أجل تحقيق بيئة رقمية أمنة وموثقة للمجتمع المصرى.

ثم صدر القانون رقم 175 لسنة 2018 فى شأن مكافحة جرائم تقنية المعلومات، لدعم منظومة مواجهة مخاطر الأمن السيبرانى، ثم صدر قرار رئيس الوزراء رقم 276 سنة 2020 الخاص بتعيين رئيس المكتب التنفيذى للمجلس الأعلى للأمن السيبرانى ورئيس الأمانة الفنية.

ويرى الباحث أن إصدار قانون ملزم للشركات المقيدة بالبورصة للإفصاح عن إدارة مخاطر الأمن الإلكترونى وبرامج إدارة مخاطر الأمن الإلكترونى أصبحت ضرورة ملحة فى الوقت الراهن خاصة وأن مصر تتعرض لهجمات إلكترونية مرتفعة فى الوقت الحالى. كما يرى الباحث أن إدارة مخاطر الأمن الالكترونى مهنياً تخلق طلباً على خدمات مراقب الحسابات بخلاف المراجعة بشأن تصميم نظام إدارة المخاطر وخدمات توكيدية مجالها مزاعم الإدارة كما تظهر بإفصاح الشركة عن إدارة مخاطر الأمن الالكترونى.

2/7- توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى: المفهوم والمتطلبات والمردود المهنى:

تعد المراجعة المالية التاريخية هى النموذج التقليدى لخدمات التوكيد لأنها خدمة تصديقية توفر توكيداً إيجابياً، ولقد ظهرت الخدمات التوكيدية نتيجة وجود طلب على مراجعة المعلومات غير المالية، إذ تركز المراجعة التاريخية على مراجعة المعلومات المالية فقط. وتعد الخدمات التوكيدية خدمات مهنية تهدف إلى تحسين جودة المعلومات لخدمة أصحاب المصالح فى الشركة. ويقوم بها عادة مراقبى الحسابات بغرض الوصول إلى استنتاج حول موضوع التكليف. وتنقسم الخدمات التوكيدية إلى نوعين؛ الأولى: خدمات تصديقية (ومنها خدمة التوكيد على الأنظمة الإلكترونية للشركات)، والثانية: خدمات غير تصديقية ثنائية الأطراف لاتنتهى بإعطاء توكيد.

وبالتالى فإن خدمة التوكيد على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى تعد خدمة تصديقية تهدف لإبداء استنتاج فنى محايد بشأن مزاعم الإدارة المكتوبة عن إدارة مخاطر الأمن الإلكترونى، بناء على المعايير الصادرة فى هذا الشأن وتوصيل منتج هذا التوكيد إلى أصحاب المصالح فى الشركة وخاصة المستثمرين بالأسهم(موسى، 2018).

وقد عرفت هيئة توكيد المعلومات(**CESG**) ([5]) خدمة التوكيد المهنى على أنها وسيلة لزيادة الثقة المستقلة فى أن الضوابط الأمنية تؤدى الوظائف المتوقعة منها(CESG,2012). ووفقاً للمعهد الوطنى للمعايير والتكنولوجياNIST تعرف خدمة التوكيد على أنها أساس الثقة فى تحقيق الأهداف الأمنية الأربعة (النزاهة، والإتاحة، والسرية، والثقة) ويتم الوفاء بها بشكل كاف من قبل الإدارة (NIST,2013a).

ويوجد حاليا آليات رئيسية تركز على توفير معايير لخدمة التوكيد على إدارة مخاطر الأمن الإلكترونى وهى:

([5])The UK Government's National Technical Authority for Information Assurance (CESG)

COBIT ([6]): هو إطار تم إنشائه بواسطةISACA والذى يمكن الإدارة من سد الفجوة بين متطلبات الرقابة ومخاطر الأمن الإلكترونى.

ISO ([7]): طورت سلسلة معايير رقم 27000 والتى تمكن الشركات من تنفيذ الضوابط التى تدعم مبادئ أمن المعلومات.

AICPA: قام بتقديم إطار تقرير الإدارة عن إدارة مخاطر الأمن الإلكترونى لمساعدة الشركات على تحديد فعالية برامج إدارة مخاطر الأمن الإلكترونى. وقد أصدرت مجموعتين من المعايير هى؛ معايير الوصف، ومعايير الرقابة (ملحق رقم 1).

NIST: أصدرت الإصدار الأول للبنية التحتية للأمن الإلكترونى عام 2014 ويستند الإصدار إلى المعايير والمبادئ التوجيهية والممارسات لتوجيه الشركات لتقليل الأثار المحتملة للمخاطر الإلكترونية (Kahyaoglu & Caliyurt, 2018) .

ويذكر Hancock (2017) أن هناك العديد من الآليات الموجودة حالياً لدعم خدمات التوكيد على إدارة مخاطر الأمن الإلكترونى، إلا أنه يجب تعديل إطار نموذج المراجعة الحالى ليتوافق مع تطور خدمات التوكيد فى الوقت الحالى وخاصة ما يتعلق بالمراجعة المستمرة والأمن الإلكترونى. ولقد حددت هيئة توكيد المعلومات **CESG** نموذج للتوكيد على إدارة مخاطر الأمن الإلكترونى يتضمن أربعة عناصر وهى(CESG ,2012):

- **توكيد جوهرى:** هو أى نشاط يوفر الثقة فى العملية التى تقوم بها الشركة أثناء تطوير المنتج أو الخدمة أو النظام.
- **توكيد خارجى:** هو أى نشاط مستقل عن بيئة التطوير التى توفر الثقة فى المنتج أو الخدمة أو النظام، وبالتالى يوفر تقييم مستقل للتطوير.
- **توكيد تنفيذى:** هو أى نشاط مستقل يوفر الثقة فى أن تطوير المنتج أو الخدمة أو النظام قد تم تنفيذه بشكل صحيح.
- **توكيد تشغيلى:** هو أى نشاط لازم للحفاظ على سلامة التطوير عند دخوله الاستخدام التشغيلى من خلال توفير أنظمة رقابية للرقابة على النظام وأمنه بإستمرار.

([6])COBIT: Control Objective for Information Technologies
([7]) International Organization for Standardization.

ويكون التوكيد الجوهرى دور الإدارة المسئولة عن التطوير، والتوكيد الخارجى والتنفيذى هو دور مراقبى الحسابات، أما التوكيد التشغيلى فهو دور إدارة المراجعة الداخلية كتوكيد مستمر (CESG ,2012) .

وتولى الشركات الحديثة المزيد من الإهتمام بقضية التوكيد على إدارة مخاطر الأمن الإلكترونى ومع ذلك تزداد فجوة التوكيد فى مجال الأمن الإلكترونى، حيث إتضح أنه على الرغم من تنفيذ جميع متطلبات الحماية من مخاطر الأمن الإلكترونى، إلا أن نسبة المخاطر ما زالت مرتفعة. حيث يظهر من تقرير CISCO (2017) السنوى والذى تم إعتماداً على بحث مسحى فى 13 دولة مع أكثر من 2900 مشارك من 130 شركة فى مختلف المجالات، أن أكثر من ثلث الشركات المتضررة من الهجوم الإلكترونى فقدوا مالا يقل عن 20 % من الدخل، رغم تطبيق الاجراءات المضادة للتهديدات (Illiashenko, et al.,2018) .

لذلك تحاول الشركات تقديم أنواع مختلفة من التوكيد الإلكترونى على مواقعها على شبكة الإنترنت والتى تنقسم إلى مجموعتين؛

الأولى: تأكيدات إلكترونية داخلية، والتى تعنى الإهتمام بخصائص الموقع الإلكترونية وتوفير إفصاح كامل على الموقع لكسب ثقة المتعاملين مع الشركة.

الثانية: تأكيدات إلكترونية خارجية، والتى يقدمها طرف خارجى مستقل بعد إجراء تقييم مستقل لموقع الشركة والإفصاحات التى يشملها والتهديدات الموجودة على نظام الشركة.

مما يوفر مزيد من الثقة للمتعاملين مع الشركة، مما يشير إلى أهمية التوكيد على ماتفصح عنه الإدارة بشأن إدارة مخاطر الأمن الإلكترونى (Bahmanziari, et al.,2009).

وبشأن أهمية خدمات التوكيد؛ فقد أيدت دراسة كل من(Vekez, 2019; Goldstein, 2021) فوائد إفصاح الإدارة عن إدارة مخاطر الأمن الإلكترونى، وتحسن قدرة المستثمرين على تقييم هذه المخاطر بعد الإطلاع على تقرير التوكيد الخاص بها. حيث وجد أن التوكيد الاختيارى للشركة على تقارير إدارة مخاطر الأمن الإلكترونى يزيد من قيمة الشركة ومصداقيتها، ومع تزايد عدد التهديدات الأمنية أصبح من الضرورى تضمين خطة المراجعة للشركة التهديدات الأمنية، وبالتالى

على مراقبى الحسابات مراجعة عمليات وأدوات وسياسات الأمن الإلكترونى لتوفير استنتاج حول درجة مصداقية تقارير الإدارة عن إدارة مخاطر الأمن الإلكترونى. ومن الطرق المستخدمة لمراجعة الأمن الإلكترونى فى الشركات:

- مراجعة سياسات أمن البيانات قبل بداية المراجعة من حيث السرية والسلامة والإتاحة.
- تصنيف البيانات وتحديد مستويات الأمان اللازم لحمايتها وتفاصيل هيكل الشبكة.
- تجميع سياسات الأمن الإلكترونى ومتطلباتها فى وثيقة واحدة للحصول على فهم شامل لممارسات أمن تكنولوجيا المعلومات لتحديد نقاط الضعف الموجودة بها.
- مراجعة معايير مخاطر الأمن الإلكترونى للشركة(معايير الوصف).
- إنشاء قائمة بأفراد الأمن الإلكترونى ومسئولياتهم.

كما تذكر الدراسات (No & Vasarhelyi, 2017; Haapamäki& Sihvonen,2019; Rosati, 2019; Aldorisio, 2020) أن نموذج التوكيد على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى لابد أن يراعى ثلاثة عناصر أساسية هى:

- **طبيعة توقيت التقرير:** حيث أن تهديدات الأمن الإلكترونى مرتبطة بفترة زمنية وتستند على متغيرات متعددة مثل: الخصائص التنظيمية، وطبيعة العمليات المعرضة للخطر خلال فترة معينة، فلايجب أن يكون استنتاج مراقب الحسابات معبراً عن نقطة زمنية معينة وإنما يكون تقريره عن فترة زمنية ممتدة على حسب التغطية.
- **طبيعة الاستنتاج:** تقدم تقارير المراجعة التقليدية الرأى حول مدى عدالة تعبير التقارير المالية عن المركز المالى ونتائج الأعمال (عادلة/ غير عادلة) وهو مالاينطبق على حالة التوكيد على إدارة مخاطر الأمن الإلكترونى، فهى عملية مستمرة متغيرة لاتأخذ حكماً واحداً على طول الوقت، وإنما من الأنسب وجود مراجعة فورية مستمرة لحالة درجة الأمن الإلكترونى والتعبير عن الحالة فى أوقات متتالية مستمرة.
- **الأهمية النسبية:** عادة تنص معايير المراجعة المقبولة على مفهوم الأهمية النسبية للعناصر، والذى يفسر عادة كنسبة من الدخل أو من إجمالى الأصول، وهو مالايصلح مع التوكيد على إدارة

مخاطر الأمن الإلكترونى، فهناك عناصر لايمكن قياسها نقداً مثل؛ الإستدامة، وسلاسل التوريد، والعلامات التجارية، وإدراك المخاطر، وبالتالى لايصلح مفهوم الأهمية النسبية فى هذه الحالة.

إلا أنه يثور التساؤل حول مبررات الطلب على مراقب الحسابات للقيام بمهمة التوكيد على الافصاح عن إدارة مخاطر الأمن الإلكترونى للشركة، حيث تذكر الدراسات (Eaton et al.,2019; AICPA, 2021) أن خبرة مراقب الحسابات تمثل أحد أسباب اللجوء له للقيام بخدمة التوكيد على إدارة مخاطر الأمن الإلكترونى، ومعرفته بالرقابة الداخلية والتقارير المالية وتقييم المخاطر وتحديد حجم التهديدات، كما لديه من المؤهلات العلمية والتدريب والمعرفة بأنظمة تكنولوجيا المعلومات وأنظمة التشغيل وتقييم الأنظمة الرقابية وتقديم الخدمات الإستشارية وتصميم البرامج مايبرر زيادة الطلب على خدماته.

وتذكر دراسة(2019) Rosati أن هناك أسباب تجعل مراقبى الحسابات هم الأولى بالقيام بهذه المهمة ومنها؛ أنهم المسئولين عن تقييم العميل، والتعرف على أثار الهجمات الإلكترونية على المركز المالى له، ومقدار الخسائر التى تسببت فيها، كما أنهم الأقدر على تقييم هيكل الرقابة الداخلية بما فيه نظم تكنولوجيا المعلومات وتحديد أوجه الضعف الجوهرية به، وأسباب الفشل فى الرد على الهجمات الإلكترونية. كما أن هناك ضغوط من الهيئات المهنية على مراقبى الحسابات للحصول على فهم كاف لأنظمة العميل التكنولوجية وأثر ذلك على مركزه المالى. كما أنهم لديهم القدرة على تقييم مخاطر المراجعة المرتبطة بإدارة مخاطر الأمن الإلكترونى.

كما يذكر كل من(Bodin et al., 2018; Eaton et al., 2019) أن وجود تقارير توكيد على الافصاح عن إدارة مخاطر الأمن الإلكترونى من قبل مراقبى الحسابات يزيد من ثقة المستثمرين فى الشركات التى تعرضت لتهديدات إلكترونية. كما أن قيام مراقبى الحسابات بمهمة التوكيد على تقارير الإدارة بشأن إدارة مخاطر الأمن الإلكترونى (من وجهة نظر الإدارة) يكون له ما يبرره حيث سيحاول مراقبى الحسابات الحفاظ على سمعتهم وبالتبعية تقليل مخاطر التقاضى وبالتالى سيحمى سمعة الإدارة من خلال بذل العناية المهنية الواجبة، وكذلك للإستفادة من خبراتهم القانونية والفنية فى هذا الشأن، ووجود مايضمن حفاظ مراقبى الحسابات على درجة عالية من الثقة

فى عملية التوكيد من خلال المعايير المهنية، وأخيراً، تحمل مراقبى الحسابات لجزء من مسئوليات الإدارة عند توفير تقرير توكيد معقول.

وبشأن تطور معايير التوكيد على تكنولوجيا المعلومات فقد مرت معايير الرقابة على تكنولوجيا المعلومات بالعديد من المراحل؛ فى السبعينيات من القرن الماضى ركز المراجعون على الأخذ فى الإعتبار أثار معالجة البيانات الإلكترونية على تقييم الرقابة الداخلية للتقارير المالية محل المراجعة. وفى التسعينيات إستخدم المراجعون معيار(SAS 70) للتقرير عن فعالية الرقابة الداخلية على التقرير المالية. وفى بداية القرن الحالى إستخدم المراجعون معايير خدمات الثقة لتقييم الرقابات المرتبطة بالأمن والإتاحة وتكامل العمليات والثقة والنزاهة والسرية والخصوصية، كما تم إصدار معايير(SOC)([8]) لتلبية إحتياجات الإدارة المرتبطة بخدمات التعهيد(OutSourcing). ومنذ عام 2017 بدأ تقديم خدمات التوكيد للأمن الإلكترونى والتقرير عن مدى فعالية الرقابات على برامج إدارة مخاطر الأمن الإلكترونى للشركات. ومن عام 2018 وما بعده تم الإستمرار فى تطوير خدمات التوكيد على إدارة مخاطر الأمن الإلكترونى وتقديم معايير للإدارة لتمكنها من إستمرار العمل مع فهم المخاطر بشكل أفضل(AICPA,2021). ويلخص الجدول التالى تطور معايير الرقابة على تكنولوجيا المعلومات:

([8]) System & Organization Controls

جدول (١)

السنة	رقم المعيار/ الخدمة	إسم المعيار/ الخدمة
١٩٧٤	SAS 3	أثر التشغيل الإلكترونى للبيانات على دراسة وتقييم المراجع للرقابة الداخلية
١٩٨٢	SAS 44	التقرير للأغراض الخاصة على الرقابة المحاسبية الداخلية فى المنظمات الخدمية.
١٩٩٢	SAS 70	المنظمات الخدمية (من أقدم المعايير التى تتعامل مع منظمات تتعامل مع شبكة الإنترنت).
١٩٩٧	Web Trust	مبادئ ومعايير التجارة الإلكترونية والثقة فى الموقع.
١٩٩٩	Sys Trust	مبادئ ومعايير الإعتماد على النظام.
٢٠٠٣	دمج الخدمتين	معايير خدمات الثقة(الأمن، الإتاحة، تكامل العمليات، القابلية للإعتماد) وتكامل خدمتى الثقة فى الموقع والثقة فى النظام.
٢٠١٠	SSAE 16	التقرير عن الرقابات فى المنظمات الخدمية.
٢٠١١	SOC 1,2,3	
	SOC 1	التقرير عن الرقابات فى المنظمات الخدمية الملائمة لإستخدام الوحدات كرقابة داخلية على التقارير المالية.
	SOC 2	التقرير عن الرقابات فى المنظمات الخدمية الملائمة للأمن، والإتاحة، وتكامل العمليات، والثقة، ودليل السرية.
	SOC 3	التقرير عن خدمة الثقة للمنظمات الخدمية.
٢٠١٧	SOC For Cybersecutity	معيار الأمن الإلكترونى والتقرير عن برنامج إدارة مخاطر الأمن الإلكترونى للمنظمة والرقابة عليه.
٢٠١٨		تطوير مستمر فى خدمات الأمن الإلكترونى.

(المصدر: من إعداد الباحث)

كما قام AICPA بتقديم حلول غير ملزمة حول برامج إدارة مخاطر الأمن الإلكترونى، لزيادة درجة الثقة بين إدارة الشركة ومراقب الحسابات والمساهمين والمستثمرين. حيث تم تقديم إطار للتقرير عن إدارة مخاطر الأمن الإلكترونى يتكون من ثلاثة مكونات يمكن للإدارة استخدامه لدعم تقاريرها عن إدارة مخاطر الأمن الإلكترونى وتكون قابلة للتوكيد عليها من قبل مراقبى الحسابات، ومدعوماً بالمعايير ذات الصلة التى يمكن لمراقبى الحسابات إستخدامها للتوكيد على هذه التقارير.

المكون الأول: وصف الإدارة

تم تصميم هذا الوصف لتوفير معلومات حول كيفية إعداد ملف يشتمل على المعلومات الأكثر أهمية، وطرق إدارة مخاطر الأمن الإلكترونى، والسياسات والعمليات الأمنية الرئيسية التى يتم تشغيلها بهدف حماية أصول معلومات الشركة ضد هذه المخاطر، وتوفير فهم للمستخدمين من

خلال توفير الإدارة إفصاحات عن المخاطر التى قد تهدد الشركة، ومدى فاعلية ضوابط الرقابة المدرجة بالبرنامج.

المكون الثانى: مزاعم الادارة

حيث توفر الإدارة تأكيدات(مزاعم) حول الوصف المقدم من حيث توافقه مع المعايير ذات الصلة(معايير الوصف) وما إذا كانت الضوابط داخل البرنامج فعالة لتحقيق الأمن الإلكترونى للشركة.

المكون الثالث: استنتاج مراقب الحسابات المهنى

يتضمن استنتاج مراقب الحسابات وصف وفعالية مزاعم الإدارة حول برنامج إدارة مخاطرالأمن الإلكترونى. (يعرض الملحق رقم (2) نص تقرير توكيد مراقب الحسابات على إدارة مخاطر الأمن الإلكترونى الصادر عن AICPA عام 2017).

ولقد قام AICPA بهذه الخطوة لتوفير ثقة لدى أصحاب المصالح والمستثمرين فى التقارير المعدة حول برامج إدارة مخاطر الأمن الإلكترونى (AICPA, 2018a). فمن غير المرجح قيام المستثمرون بالاستثمار فى شركات تم الإفصاح فيها عن حدوث إختراقات أمنية دون وجود تقرير للتوكيد على هذه الإفصاحات من مراقبى الحسابات(Janvrin& Wang, 2019) .

إلا أن هناك بعض المشاكل التى تواجه مراقبى الحسابات عند القيام بمهمة التوكيد على مزاعم الإدارة بشأن إدارة مخاطر الأمن الإلكترونى ومنها: (Evans et al., 2016; Kahyaoglu & Caliyurt, 2018; Wertheim, 2019)

- عدم توافر خلفية ملائمة فى تكنولوجيا المعلومات.
- عدم توافر توكيد داخلى مستقل من قبل المراجعين الداخليين.
- عدم توافر الوعى بمخاطر الأمن الإلكترونى من قبل الإدارة.
- عدم توافر التأهيل والتدريب اللازمين للمراجعين الداخليين للتعرف على مخاطر الأمن الإلكترونى.
- صعوبة القياس الكمى لجودة الخدمة المقدمة لأنه سلوك بشرى.

- عدم كفاية الموارد والتدريب لدى العاملين بأقسام نظم المعلومات.
- الفهم غير الكافى للمخاطر خاصة فى الشركات متوسطة وصغيرة الحجم.
- عدم توافر هيكل رقابة داخلية فعال.
- عدم وجود خطة للإستجابة للحوادث الأمنية.

كما حدد AICPA خطوات دعم مراقبى الحسابات لبرنامج إدارة مخاطر الأمن الإلكترونى الذى تعدة إدارة الشركة كما يظهر من الجدول التالى:

جدول (٢)

خطوات البرنامج	دور مراقبى الحسابات
١- تحديد أولويات التعرض لمخاطر الأمن الإلكترونى	الإستفادة من خبراتهم فى مجال تكنولوجيا المعلومات ومعرفتهم لأنواع التهديدات الحالية.
٢- تصميم نظام رقابة على الأمن الإلكترونى	المساعدة فى توفير ضوابط رقابية وأفضل ممارسات فى الصناعة ومعايير الرقابة اللازمة.
٣- إختبار الفعالية التشغيلية لضوابط الأمن الإلكترونى	توافر الخبرة المتنوعة لمراقبى الحسابات فى إختبار ضوابط تكنولوجيا المعلومات بالتزامن مع إجراء عمليات المراجعة للبيانات المالية.
٤- إعداد تقرير الإدارة عن إدارة مخاطر الأمن الإلكترونى	المساعدة فى توفير إرشادات إعداد التقرير وفق إرشادات AICPA .
٥- طلب خدمة التوكيد على تقرير الإدارة عن إدارة مخاطر الأمن الإلكترونى	توفير خدمة التوكيد المهنى على تقرير الإدارة عن إدارة مخاطر الأمن الإلكترونى وتقديم تقرير بذلك.

المصدر: (Eaton et al.,2019)

ويخلص الباحث إلى أن خدمة التوكيد المهنى على إدارة مخاطر الأمن الإلكترونى لها أهمية خاصة للشركات، حيث تمكنها من تقييم سياسات إدارة مخاطر الأمن الإلكترونى لديها، ومدى توافقها مع المعايير مما يساعد على اتخاذ نهج استباقى عند تصميم سياساتها بخصوص مواجهة مخاطر الأمن الإلكترونى، وتقييم جودة إدارة هذه المخاطر، وكشف نقاط الضعف الجوهرية فى أنظمة الرقابة الداخلية على أمن المعلومات.

3/7- تحليل العلاقة محل الدراسة واشتقاق فروض البحث:

تتفق الدراسات (عبد الرحيم، O'Reilly, 2009; Levišauskait,2010; Matar, 2020 2012; Zureigat, 2014; Gupta et al.,2018) على أن الهدف من قرار الاستثمار بالأسهم هو تعظيم ربحية المستثمر، وهو من أكثر القرارات أهمية فهو المؤثر على المركز المالى للشركات بصفة عامة إذ يوفر لها أحد أهم مصادر التمويل الذاتى، عن طريق إصدار أسهم أو سندات، وبالتالى فإن الاستثمار فى أسهم يحدد سعر السهم من خلال الشراء والبيع.

ويحتاج المستثمر إلى توكيد مهنى من مراقب الحسابات بشأن مدى مقدرة الإدارة على مواجهة تهديدات الأمن الإلكترونى. ذلك لأن تقرير توكيد مراقب الحسابات هو الأساس الذى يبنى عليه المستثمرون قراراتهم بالإستمرار أو عدمه فى الشركة، وبالتالى فإن وجود تقرير توكيد مهنى على إدارة مخاطر الأمن الإلكترونى بالشركة يزيد من ثقة المستثمرين فى قدرة إدارة الشركة على مواجهة التهديدات الحادثة. ولذلك فإن تقرير التوكيد الذى أصدره AICPA لمراقبى الحسابات يوفر قدراً كبيراً من المعلومات اللازمة التى تساعد المستثمر على إتخاذ قراره بشأن الاستثمار بالأسهم (AICPA,2021).

كما خلصت دراسة(Navarro& Sutton (2021 إلى أن توفير توكيد على تقرير الإدارة بشأن إدارة مخاطر الأمن الإلكترونى يوفر تقييمات أفضل للمستثمرين لمصداقية الإدارة، وبالتالى تقييمات أعلى للأسهم، على عكس الشركات التى لاتوفر مثل هذا التوكيد. كمايختلف رد فعل المستثمرين بإختلاف نوع الصناعة، حيث يتفاعلون مع إنتهاكات معايير الصناعة وتزداد قيمة المصداقية للإدارة مع وجود تقرير توكيد بشأن إدارة مخاطر الأمن الإلكترونى بعد حدوث الإنتهاك.

ولقد إتفقت العديد من الدراسات (Bodin et al., 2018; Eaton et al.,2019; CPA Canada, 2020) على أن حدوث الإختراقات الإلكترونية كان له تأثير جوهرى على مهنة المحاسبة والأثر المالى المرتبط بها على الشركات والمستثمرين، حيث سلطت الضوء على المخاطر الإلكترونية بإعتبارها واحدة من قضايا المخاطر الرئيسية التى يأخذها المستثمرون فى الإعتبار عند إتخاذ قراراتهم الإستثمارية بالأسهم، لذلك تلبى المهنة إحتياجات المستثمرين عن

طريق مجموعة من خدمات التوكيد لتوفير المعلومات اللازمة لهم بشأن أنشطة الأمن الإلكترونى للشركات، من خلال ماوفره مجمع AIPCA من أطر للتقارير سواء للإدارة أو مراقبى الحسابات.

ويتسق ذلك مع ماإنتهت إليه دراسة Gordon et al.,(2015) أن التوكيد على إدارة مخاطر الأمن الإلكترونى يلعب دوراً مهماً فى حماية سمعة الإدارة ومساعدة الشركة على تجنب التداعيات المالية وخطر التقاضى ويزيد ثقة المستثمرين فى التعامل مع الشركة.

ومن ناحية أخرى، وجدت بعض الدراسات (Tan & Yu, 2018; Kamiya et al., 2021) أن هناك عاملين مؤثرين على العلاقة بين وجود توكيد لمراقب الحسابات على إدارة مخاطر الأمن الإلكترونى وقرار الاستثمار بالأسهم، الأول؛ أن تأثير التوكيد على إتخاذ قرار الاستثمار بالأسهم سيختلف مع إختلاف توقع التوكيد، حيث يوجد تأثير إيجابى عند الحصول على توكيد من مراقبى الحسابات بينما يحدث العكس فى حالة عدم وجود توكيد من مراقبى الحسابات. الثانى؛ أن تصورات مصداقية الإدارة تؤثر على قرار الاستثمار بالأسهم، حيث تتأثر مصداقية الإدارة بمصداقية إفصاحاتها المتعلقة بقضايا أمن تكنولوجيا المعلومات، حيث أن الفشل فى الحفاظ على ضوابط الأمن الإلكترونى يشوه صورة الإدارة العليا مما يؤثر على مستقبلهم الوظيفى، وبالتالى وجود توكيد على تقرير الإدارة بشأن إدارة مخاطر الأمن الإلكترونى يعد آلية لحماية سمعة ومصداقية الإدارة، والتى تؤثر بالتبعية على تأثير الإختراق على قرار المستثمرين بالأسهم.

كما توصلت بعض الدراسات (Gordon et al., 2011; Masli et al., 2016; Frank et al., 2019; Navarro& Sutton, 2021) إلى وجود رد فعل سلبى فى السوق تجاه الشركات التى تعرضت لإختراقات أمنية وحوادث أمن إلكترونى بصفة عامة، وأن هذه الحوادث تؤثر على عوائد سوق الأوراق المالية ووجود تحول محتمل فى تقييمات المستثمرين بمرور الوقت، وعلى السمعة التنظيمية للشركة. إلا أن صدور معايير SOC من AICPA للأمن الإلكترونى قد يساعد فى دعم جاذبية الاستثمار بالأسهم ويوفر مزايا أكبر للشركات عن كشف الإختراقات المتوقعة مما يخفف من الأثر السلبى لهذه الإختراقات.

كما أن الشركات التى تفصح عن وجود برامج إدارة مخاطر الأمن الإلكترونى تتلقى تقييمات أفضل لمصداقية الإدارة، وبالتالى تؤثر على أسعار الأسهم إيجاباً مقارنة بتلك الشركات التى ليس لديها هذه البرامج.

وتتفق بعض الدراسات (Khazanchi & Sutton,2001; Cavusoglu et al.,2004; Kamiya et al., 2021; Tosun, 2021) على أن الهجمات الإلكترونية التى لاتنطوى على فقدان المعلومات المالية الشخصية لاتسبب خسارة كبيرة فى ثروة المساهمين مما لايؤثر على أسعار الأسهم، إلا أن الهجمات الإلكترونية الناجحة تؤثر سلباً على أسعار أسهم الشركات فى الصناعة المستهدفة. كما يكون للهجمات الإلكترونية تأثيرين على المدى القصير والطويل الأجل، فعلى المستوى **القصير الأجل** يزيد حجم التداول والسيولة بسبب ضغوط البيع عند الإفصاح عن الهجمات لأول مرة بسبب زيادة إهتمام المستثمرين، حيث وجدت تغيرات سلبية فى أسعار الأسهم فى غضون يومين من تاريخ الإفصاح. وعلى المستوى **طويل الأجل** (خلال 5 سنوات) تمثل صدمات سلبية غير متوقعة لسمعة الشركات، مما يؤدى إلى معدل دوران غير طبيعى للعملاء وفقدان السمعة التجارية، مما يؤثر بدوره على التدفقات النقدية والأرباح.

وتشير العديد من الدراسات (Pflugrath et al.,2011; Asay et al., 2016; Frank et al., 2019; Vekez, 2019) إلى أن شكل إفصاح الإدارة عن إدارة مخاطر الأمن الإلكترونى أيضاً يؤثر على قرار المستثمرين بالاستثمار فى الأسهم، كماً وكيفاً. فمن ناحية الكم؛ فإن المستثمرين يتفاعلون بدرجة أكبر مع كم الإفصاح فى تقرير الإدارة، وتتأثر أحكامهم بدرجة كبيرة كلما كانت مصادر المعلومات خارجية للتحقق من صدق إفصاحات الإدارة، مثل تقارير المحللين ووسائل الإعلام الإخبارية، حيث يقوم المستثمرون بدمج المعلومات الخارجية مع إفصاحات الإدارة عند إصدار أحكام تقييم أداء الشركة. أما من ناحية الكيف؛ فإن ثقة المستثمرين تزداد عندما يتم التوكيد على تقرير الإدارة بشأن إدارة مخاطر الأمن الإلكترونى.

وفى نفس السياق تذكر الدراسات (Gordon et al.,2010; Wang et al., 2013; Ettredge et al., 2018; Haapamäki& Sihvonen.2019) أن هناك تزايداً فى عدد

الشركات التى تقوم بالإفصاح عن إدارة مخاطر الأمن الإلكترونى والتهديدات التى تتعرض لها، مما كان له تأثير قوى سلبى على أسعار الأسهم وقيمة الشركات السوقية، خاصة تلك الشركات التى تنشر تقارير مراقب الحسابات عن تقرير الإدارة عن إدارة مخاطر الأمن الإلكترونى. ولقد ساعدت الإرشادات الصادرة عن مخاطر الأمن الإلكترونى فى توفير تأثير إيجابى على قيمة الشركة وأسعار الأسهم وتقليل حوادث الأمن الإلكترونى.

وتوصلت الدراسات (Spanos & Angelis,2016; Lange & Burger ,2017; Rosati et al.,2017; Bianchi &Tosun, 2019; Tosun, 2021) إلى أن الإفصاح عن إدارة مخاطر الأمن الإلكترونى بدون توكيد من مراقب الحسابات يؤدى إلى العديد من الآثار؛ ففى الأجل القصير، ينخفض سعر السهم ويزيد حجم التداول بالبيع، وفى الأجل الطويل، يوجد أضرار كبيرة لسمعة الشركة وفقدان الميزة التنافسية فى الصناعة، ويظهر الأثر فى الشركات الكبيرة عن الشركات الصغيرة الحجم.

وتوصلت دراسة(2019),.Richardson et al إلى إختلاف تأثير الإفصاح عن مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى على أسعار الأسهم، فإذا كان الإفصاح عن إختراقات لحسابات العملاء سيفقد العملاء الثقة فى الشركة، وتخسر الشركة تعاملاتها معهم، وإذا كان الإفصاح عن إختراق بيانات هامة للشركة أدت لخسائر مالية للمستثمرين سيؤدى إلى فقدان الثقة فى الشركة ويؤثر سلباً على أسعار الأسهم.

ومصرياً، توصلت دراسة الرشيدى، والسيد(2019) إلى أن هناك قصوراً فى الإفصاح عن مخاطر الأمن الإلكترونى، وبرامج إدارة مخاطر الأمن الإلكترونى فى الشركات المصرية العاملة فى مجال تكنولوجيا المعلومات مما يؤثر سلباً على أسعار الأسهم فى البورصة وحجم التداول.

ويخلص الباحث من ذلك إلى وجود تأثير لتوكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية، لذلك يمكن إشتقاق الفرض الأول(**H_1**) على النحو التالى:

H_1: يؤثر توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى إيجاباً ومعنوياً على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية.

وبشأن أثر مستوى التأهيل العلمى للمستثمر على تكوينه المعرفى والذى يمكن أن يساهم فى تحسين جودة قراره، وإدراكه للعلاقة التأثيرية بين توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى وقراره بالاستثمار بالأسهم، فقد وجدت دراسة Wang et al., (2013) أن رد فعل المستثمر تجاه هجمات الأمن الإلكترونى تختلف بإختلاف الصناعة، وإجراءات الشركة، وتأهيل وخبرة المستثمر. وتوصلت دراسة Navarro& Sutton (2021) إلى أن معرفة المستثمرين وتأهيلهم يساعد فى زيادة الطلب على خدمات توكيد مراقب الحسابات على مزاعم الإدارة بشأن إدارة مخاطر الأمن الإلكترونى، على النحو الذى يساعدهم على إتخاذ القرار الرشيد بشأن الاستثمار بالأسهم.

كما إتفقت بعض الدراسات(عبد الرحيم،2020؛ Miazee et al., 2014; Samad, 2017; Gupta et al., 2018)على أن التأهيل العلمى للمستثمر من العوامل الهامة التى تنعكس على عملية إتخاذه للقرار، خاصة التعليم المالى أوالمحاسبى. كما يساعده على فهم المخاطر والفرص الإستثمارية المتاحة وتقييمه للإستثمارات. ويخلص الباحث إلى أن تأهيل المستثمر يؤثر تأثيراً إيجابياً على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية. لذلك يتوقع الباحث أن يختلف التأثير الإيجابى المعنوى لتوكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية بإختلاف مستوى التأهيل العلمى للمستثمر. وبناء على ذلك يمكن إشتقاق الفرض الثانى(**H_2**) على النحو التالى:

H_2: يختلف التأثير الإيجابى المعنوى لتوكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية بإختلاف مستوى التأهيل العلمى للمستثمر.

وبشأن أثر خبرة المستثمر على إدراكه للعلاقة التأثيرية بين توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى وقراره بالاستثمار بالأسهم، فقد وجدت بعض الدراسات(عبد الرحيم، 2020؛ Noghondari & Foong,2013; Casterella et al.,2020) أن مستوى الخبرة لدى المستثمرين يؤثر على هذه العلاقة حيث تؤثر خبرته على حكمه الشخصى، وبناء عليه يتأثر قرار الاستثمار فى الأسهم بمستوى خبرة ومعرفة المستثمر، حيث أن قرارات الأشخاص تختلف تجاه نفس العلاقات بإختلاف خبراتهم الشخصية. كما تختلف قرارتهم بالاستثمار فى أسهم الشركة نفسها من مستثمر لأخر، وبالتالى تختلف قرارتهم بالاستثمار فى الشركة من عدمه بناء على خبراتهم وإدراكهم لأهمية تقرير توكيد مراقب الحسابات على مزاعم الإدارة بشأن إدارة مخاطر الأمن الإلكترونى، مقارنة بشركات أخرى لم تحصل على هذا التوكيد.

ويخلص الباحث مماسبق إلى أن خبرة المستثمر تؤثر تأثيراً إيجابياً على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية. لذلك يتوقع الباحث أن يختلف التأثير الإيجابى المعنوى لتوكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية بإختلاف مستوى خبرة المستثمر. وبناء على ذلك يمكن إشتقاق الفرض الثالث(H_3) على النحو التالى:

> **H_3**: يختلف التأثير الإيجابى المعنوى لتوكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية بإختلاف مستوى خبرة المستثمر.

4/7 – نموذج ومنهجية البحث:

يعرض الباحث فى هذه الجزئية لأهداف الدراسة التجريبية، و مجتمع وعينة الدراسة، وأدوات وإجراءات الدراسة، وتوصيف وقياس متغيرات الدراسة، ونموذج الدراسة، والتصميم التجريبى للدراسة، وأخيراً نتائج اختبار الفروض إحصائياً. وذلك على النحو التالى:

1/4/7- أهداف الدراسة التجريبية:

تهدف الدراسة التجريبية إلى اختبار أثر توكيد مراقب الحسابات على مزاعم الإدارة بشأن إدارة مخاطر الأمن الإلكترونى على قرار الاستثمار بالأسهم. وكذلك اختبار أثر تأهيل وخبرة المستثمرين على العلاقة محل الاختبار، قياساً على (Masli et al., 2016; Frank et al., 2019; Navarro& Sutton, 2021).

2/4/7-مجتمع وعينة الدراسة:

يشتمل مجتمع الدراسة على المستثمرين المؤسسيين والذين يتمثلون فى أمناء الاستثمار فى البنوك التجارية المصرية، وسيتم سحب عينة تحكمية منهم، قياساً على Navarro& Sutton (2021). ويوضح الجدول التالى بيان بالردود على الحالات التجريبية التى تم توزيعها على عينة الدراسة والتى خضعت للتحليل الإحصائى.

جدول (٣): بيان بالردود على الحالات التجريبية

بيان	المستثمرون
عدد الحالات الموزعة	٨٠
عدد الحالات المستلمة	٧٠
نسبة الردود	%٨٧.٥
عدد الحالات السليمة	٦٥
نسبة الردود السليمة	%٩٣

(المصدر: من إعداد الباحث)

3/4/7-أدوات وإجراءات الدراسة:

استخدم الباحث دراسة تجربية (4x2) قياساً على(Navarro& Sutton(2021 لاختبار أثر توكيد مراقب الحسابات على مزاعم الإدارة بشأن إدارة مخاطر الأمن الإلكترونى على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية. وتتضمن الدراسة التجربية قسمين:

القسم الأول: يختص بالتعرف على خصائص المستثمرين المؤسسيين وخاصة مستوى التأهيل العلمى ومستوى الخبرة.

القسم الثانى: الحالة التجربية والتى تنقسم إلى حالتين:

الحالة الأولى: حالة إدارة مخاطر الأمن الإلكترونى بدون توكيد من مراقب الحسابات المستقل.

الحالة الثانية: حالة توقع وجود ارتباط للشركة بخدمة التوكيد من مراقب الحسابات على مزاعم الإدارة بشأن إدارة مخاطر الأمن الإلكترونى.

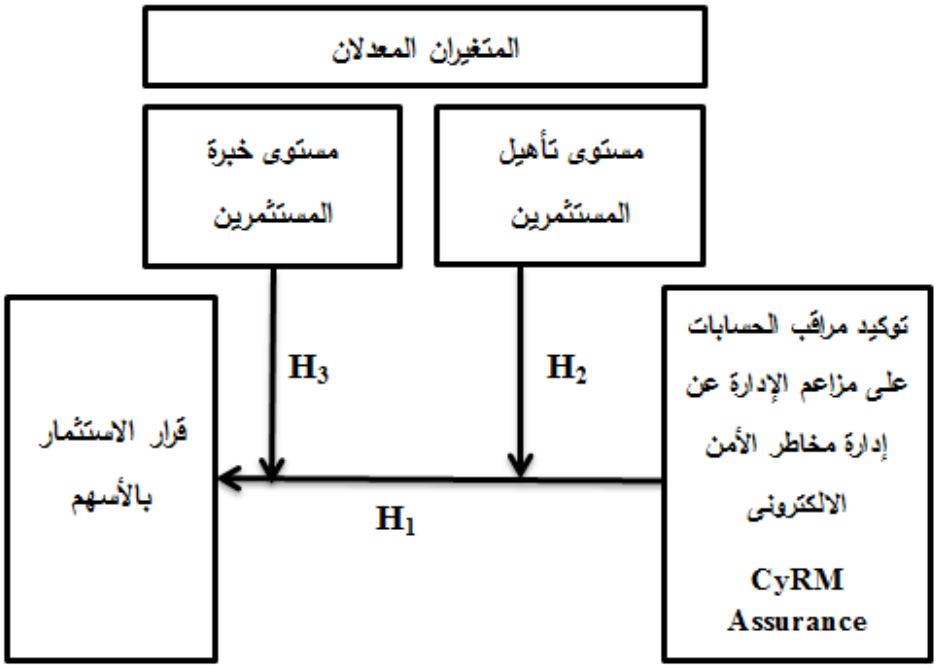
4/4/7- توصيف وقياس متغيرات الدراسة:

يوضح الجدول التالى توصيف وقياس متغيرات الدراسة:

جدول (٤): توصيف وقياس متغيرات الدراسة

نوع المتغير	المتغير والرمز	التعريف وطريقة القياس	التأثير المتوقع
متغير مستقل	**توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى CyRM-Assurance**	متغير وهمى يأخذ القيمة (١) اذا كانت الشركة **مرتبطة بالتوكيد مع مراقب الحسابات** على توكيد إدارة مخاطر الأمن الإلكترونى والقيمة (صفر) بخلاف ذلك، قياسا على: **(Bianchi &Tosun, 2019; Navarro, P. & S. Steve , 2021; Tosun, 2021)**	**إيجابى**
متغير تابع	**قرار الاستثمار بالأسهم Valuation Judgment**	**القيمة المتوقعة** لسعر السهم من جانب أفراد العينة مقاسة بنقاط من (١)إلى (٥) حيث: منخفض جداً =١ مرتفع جدا =٥ قياسا على: **(Richardson et al.,2019; Navarro, P. & S. Steve , 2021)**	
متغير معدل	**مستوى التأهيل العلمى للمستثمر Qualification**	يقاس من خلال مقياس من (١)إلى (٥) حيث: حاصل على دراسات عليا أو شهادات مهنية = ٥ حاصل على مؤهل عادى غير متخصص=١ قياسا على: **(Wang et al., 2013; Miazee et al., 2014; Samad, 2017; Navarro, P. & S. Steve , 2021)**	**إيجابى**
متغير معدل	**مستوى الخبرة للمستثمر Experience**	يقاس من خلال مقياس من (١)إلى (٥) حسب عدد سنوات الخبرة فى إدارة أمناء الاستثمار. قياساً على: **(Noghondari & Foong,2013; Casterella et al.,2020; Navarro, P. & S. Steve , 2021)**	**إيجابى**

5/4/7-نموذج الدراسة: **يظهر نموذج البحث كما يلى:**



(نموذج البحث: من إعداد الباحث)

6/4/7-التصميم التجريبى للدراسة:

لاختبار فروض الدراسة نستخدم التصميم التجريبى(4x2) كما بالجدول التالى:

جدول (٥): التصميم التجريبى(٢×٤)

الخصائص النوعية للمستثمرين / بدائل الافصاح عن التوكيد على مزاعم الإدارة عن إدارة مخاطر الأمن الالكترونى	مستوى تأهيل المستثمر		مستوى خبرة المستثمر	
	مرتفع	منخفض	مرتفع	منخفض
إفصاح عن مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى بدون تقرير توكيد	توقع المستثمر لسعر السهم (المعالجة ١)	توقع المستثمر لسعر السهم (المعالجة ٢)	توقع المستثمر لسعر السهم (المعالجة ٣)	توقع المستثمر لسعر السهم (المعالجة ٤)
إفصاح عن مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى مع وجود تقرير توكيد	توقع المستثمر لسعر السهم (المعالجة ٥)	توقع المستثمر لسعر السهم (المعالجة ٦)	توقع المستثمر لسعر السهم (المعالجة ٧)	توقع المستثمر لسعر السهم (المعالجة ٨)

وبناء على التصميم السابق هناك (8) معالجات تجربية كمايلى:

المعالجة(1): تقدم لعينة المستثمرين المؤسسيين قوائم مالية لشركة تكنولوجيا معلومات مقيدة بالبورصة المصرية تواجه مخاطر أمن الكترونى/ تم الافصاح عن مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى/ دون تقرير توكيد/ مستثمر ذو **مستوى تأهيل مرتفع**/ يطلب منه توقع سعر إقفال السهم بعد عام.

المعالجة(2): تقدم لعينة المستثمرين المؤسسيين قوائم مالية لشركة تكنولوجيا معلومات مقيدة بالبورصة المصرية تواجه مخاطر أمن الكترونى/ تم الافصاح عن مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى/ دون تقرير توكيد/ مستثمر ذو **مستوى تأهيل منخفض**/ يطلب منه توقع سعر إقفال السهم بعد عام.

المعالجة(3): تقدم لعينة المستثمرين المؤسسيين قوائم مالية لشركة تكنولوجيا معلومات مقيدة بالبورصة المصرية تواجه مخاطر أمن الكترونى/ تم الافصاح عن مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى/ دون تقرير توكيد/ مستثمر ذو **مستوى خبرة مرتفع**/ يطلب منه توقع سعر إقفال السهم بعد عام.

المعالجة(4): تقدم لعينة المستثمرين المؤسسيين قوائم مالية لشركة تكنولوجيا معلومات مقيدة بالبورصة المصرية تواجه مخاطر أمن الكترونى/ تم الافصاح عن مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى/ دون تقرير توكيد/ مستثمر ذو **مستوى خبرة منخفض/** يطلب منه توقع سعر إقفال السهم بعد عام.

المعالجة(5): تقدم لعينة المستثمرين المؤسسيين قوائم مالية لشركة تكنولوجيا معلومات مقيدة بالبورصة المصرية تواجه مخاطر أمن الكترونى/ تم الافصاح عن مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى/ مع تقرير توكيد/ مستثمر ذو **مستوى تأهيل مرتفع/** يطلب منه توقع سعر إقفال السهم بعد عام.

المعالجة(6): تقدم لعينة المستثمرين المؤسسيين قوائم مالية لشركة تكنولوجيا معلومات مقيدة بالبورصة المصرية تواجه مخاطر أمن الكترونى/ تم الافصاح عن مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى/مع تقرير توكيد/ مستثمر ذو **مستوى تأهيل منخفض/** يطلب منه توقع سعر إقفال السهم بعد عام.

المعالجة(7): تقدم لعينة المستثمرين المؤسسيين قوائم مالية لشركة تكنولوجيا معلومات مقيدة بالبورصة المصرية تواجه مخاطر أمن الكترونى/ تم الافصاح عن مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى/ مع تقرير توكيد/ مستثمر ذو **مستوى خبرة مرتفع/** يطلب منه توقع سعر إقفال السهم بعد عام.

المعالجة(8): تقدم لعينة المستثمرين المؤسسيين قوائم مالية لشركة تكنولوجيا معلومات مقيدة بالبورصة المصرية تواجه مخاطر أمن الكترونى/ تم الافصاح عن مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى/مع تقرير توكيد/ مستثمر ذو **مستوى خبرة منخفض/** يطلب منه توقع سعر إقفال السهم بعد عام.

ولاختبار فروض البحث تم إجراء المقارنات الأتية:

يتم اختبار الفرض الأول $\mathbf{H_1}$ فى التحليل الأساسى من خلال:

المقارنة الأولى: بين المعالجات {1+2+3+4} والمعالجات {5+6+7+8}.

ثم يتم إجراء تحليل إضافى من خلال إدخال متغيرى تأهيل وخبرة المستثمرين كمتغيرين معدلين Moderating Variables لاختبار أثرهما على العلاقة محل الدراسة من خلال:

المقارنة الثانية: بين المعالجات {1 x 5} والمعالجات {2 x 6}، وذلك لاختبار الفرض $\mathbf{H_2}$.

المقارنة الثالثة: بين المعالجات {3 x 7} والمعالجات {4 x 8}، وذلك لاختبار الفرض $\mathbf{H_3}$.

ثم يتم اختبار الفرض الأول $\mathbf{H_1}$ فى التحليل الإضافى من خلال:

المقارنة الرابعة: بين المعالجات {1 + 3} x {5 + 7} والمعالجات {2 + 4} x {6 + 8}، وذلك لاختبار مدى اختلاف تأثير توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى على قرار الاستثمار فى أسهم الشركات المقيدة بالبورصة المصرية، بإختلاف الأثر المجمع للتأهيل العلمى والخبرة للمستثمرين معاً.

7/4/7- نتائج الدراسة التجريبية:

- **الأساليب الإحصائية المستخدمة:**

استخدم الباحث لتحليل البيانات عدد من الأساليب الإحصائية، كما تم استخدام الإختبارات التى تتفق مع طبيعة البيانات الخاصة بالدراسة التجريبية وفروض البحث، وذلك على النحو التالى:

- **اختبار كرونباغ الفا Cronbach's Alpha:**

استخدم الباحث اختبار معامل كرونباغ الفا وذلك لمعرفة مدى إمكانية الاعتماد على الأسئلة الخاصة بالحالات التجريبية محل الدراسة، وذلك من خلال اختبار مدى ثبات ومصداقية إجابات الأفراد على الأسئلة المقدمة لهم، وتتراوح قيمة معامل كرونباغ الفا بين (صفر ، واحد) حيث إذا كان المعامل يكون مساوياً للواحد الصحيح تكون الإجابات بها ثبات، وإذا كان هذا المعامل يساوى الصفر، فهذا يعنى عدم الثبات فى الإجابات. وتعتبر أصغر قيمة مقبولة لمعامل كرونباغ الفا هى 60%، وأفضل قيمة تتراوح مابين (70% إلى 80%)، والزيادة فى قيمة المعامل تعبر عن الصدق. وإذا كان معامل كرونباغ الفا أقل من 60% يتم استخدام إجراء حذف البند، حيث يتم حذف بعض البنود التى تجعل قيمة معامل كرونباغ ألفا تصل إلى 60% أو أكثر(Bonett & Wright ,2015).

وأظهرت النتائج مصداقية لكل عنصر على حده، وإمكانية الاعتماد على عناصر الأسئلة ككل، حيث أن معامل كرونباغ ألفا أكبر من 60% وكذلك وجد أن هناك مصداقية لأن معامل كرونباغ ألفا لعينة الدراسة 839, وهو أكبر من 60% كما يوضحها الجدول التالى:

جدول(٦) معامل كرونباغ ألفا

Reliability Statistics

Sample		Cronbach's Alpha	Standard Deviation
الحالة الأولي	1Q	0.7485	0.682
	2Q	0.8852	0.060
الحالة الثانية	1Q	0.7629	0.544
	2Q	0.7355	0.786
	3Q	0.7442	0.772
	4Q	0.8835	0.062
Cronbach's Alpha		0.839509	
Std. Cronbachs Alpha		0.453729	

وقدم قام الباحث بإستخدام اختبار كا^2 Chi-square (X^2) للتأكد من مدى معنوية الأسئلة، وأوضحت النتائج أن قيمة P-Value أقل من 5% لمعظم الأسئلة الخاصة بالحالات التجربية مما يعنى **رفض فرض العدم وقبول الفرض البديل** قياساً على (عبدالفتاح،2016).

- **تحديد الإختبارات المناسبة للدراسة:**

تم استخدام اختبار **Kolmogorov-Smirnov** لتحديد مدى استيفاء توزيع البيانات للتوزيع الطبيعى المعتدل، قياساً على(عزام،1990).

ويمكن التعبيرعن فرض العدم والفرض البديل لهذا الاختبار على النحو التالى:

فرض العدم H_0: العينة المسحوبة من مجتمع يتبع التوزيع الطبيعى.

الفرض البديل H_1: العينة المسحوبة من مجتمع لا يتبع التوزيع الطبيعى.

وفيما يلى جدول يوضح نتائج هذا الاختبار:

جدول(٧) نتائج إختبارات توزيع البيانات

Kolmogorov-Smirnov

Sample	Kolmogorov-Smirnov	
	P-Value	Statistic
الحالة الأولي	0.000	0.164
الحالة الثانية	0.000	0.196

ويظهر من الجدول السابق أنه وفقا لاختبار**Kolmogorov-Smirnov** بأن المجتمع الذى سحبت منه عينة الدراسة لايتبع التوزيع الطبيعى المعتدل، وعليه تم رفض فرض العدم وقبول الفرض البديل حيث أن قيمة P-Value أقل من 5% لكل المتغيرات محل الدراسة، وبالتالى سيتم الاعتماد على الإختبارات اللامعلمية لاختبار فروض البحث(عزام،1990).

- **نتائج اختبار فروض البحث فى ظل التحليل الأساسى:**
- **نتيجة اختبار الفرض الأول H_1:**

لاختبار هذا الفرض تم تحويله إلى فرض عدم كالتالى:

فرض العدم H_0 : لايؤثر توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى إيجاباً ومعنوياً على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية.

وتم اختباره بواسطة اختبارWilcoxon Signed Ranks Test على عينتين غير مستقلتين.

فإذا كان وسيط الفروق مساوياً للصفر يدل ذلك على عدم وجود إختلافات معنوية بين إجابات الأسئلة، وبالتالى يتم قبول فرض العدم ورفض الفرض البديل، بينما إذا كان وسيط الفروق غير مساوياً للصفر يدل ذلك على وجود إختلافات معنوية بين إجابات الأسئلة وبالتالى يتم رفض فرض العدم وقبول الفرض البديل، وفيما يلي نتائج اختبار الفرض الأول فى ظل الحالتين التجريبيتين:

جدول(٨) نتيجة إختبار الحالة الأولى

Wilcoxon Signed Ranks Test

Ranks				
		N	Mean Rank	Sum of Ranks
Q1-Q2	Negative Ranks	0[a]	.00	.00
	Positive Ranks	65[b]	33.00	2145.00
	Ties	0[c]		
	Total	65		
a. Q1< Q2				
b. Q1> Q2				
c. Q1= Q2				

Test Statistics[a]	
	Q1-Q2
Z	-7.223[b]
Asymp. Sig. (2-tailed)	.000
a. Wilcoxon Signed Ranks Test	
b. Based on negative ranks.	

(المصدر: إعداد الباحث من نتائج التحليل الإحصائى)

يتضح من الجداول السابقة أن قيمة P-Value (Sig.=0.000) أقل من 5% لذلك **تم رفض فرض العدم وقبول الفرض البديل H_1 فى ظل الحالة الأولى بوجود تأثير لتوكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى إيجاباً ومعنوياً على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية.**

جدول(٩) نتيجة إختبار الحالة الثانية
المقارنة بين إجابات الأسئلة
Wilcoxon Signed Ranks Test

Ranks				
		N	Mean Rank	Sum of Ranks
Q1-Q4	Negative Ranks	0[a]	.00	.00
	Positive Ranks	65[b]	33.00	2145.00
	Ties	0[c]		
	Total	65		
Q2 -Q4	Negative Ranks	0[a]	.00	.00
	Positive Ranks	63[b]	32.00	2016.00
	Ties	2[c]		
	Total	65		
Q3 -Q4	Negative Ranks	0[a]	.00	.00
	Positive Ranks	65[b]	33.00	2145.00
	Ties	0[c]		
	Total	65		
a. Q1< Q4	b. Q1> Q4	c. Q1= Q4		
a. Q2< Q4	b. Q2> Q4	c. Q2= Q4		
a. Q3< Q4	b. Q3> Q4	c. Q3= Q4		

Test Statistics[a]			
	Q1-Q4	Q2 -Q4	Q3 -Q4
Z	-7.144[b]	-7.015[b]	-7.108[b]
Asymp. Sig. (2-tailed)	.000	.000	.000
a. Wilcoxon Signed Ranks Test			
b. Based on negative ranks.			

(المصدر: إعداد الباحث من نتائج التحليل الإحصائى)

يتضح من الجداول السابقة أن قيمة P-Value (Sig.=0.000) أقل من 5% فى جميع المقارنات بين إجابات أسئلة الحالة الثانية، لذلك **تم رفض فرض العدم وقبول الفرض البديل H_1 بوجود تأثير لتوكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى إيجاباً ومعنوياً على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية.**

وتتفق هذه النتائج فى الحالتين مع بعض الدراسات (Bodin et al., 2018; Eaton et al.,2019; CPA Canada, 2020;Navarro& Sutton, 2021) والتى توصلت إلى أن توفير توكيد على تقرير الإدارة بشأن إدارة مخاطر الأمن الإلكترونى يوفر تقييمات أفضل للمستثمرين لمصداقية الإدارة، وبالتالى توقعات أعلى للأسهم. على عكس الشركات التى لاتوفر مثل هذا التوكيد. كما يختلف رد فعل المستثمرين بإختلاف نوع الصناعة، حيث يتفاعلون مع إنتهاكات معايير الصناعة وتزداد قيمة المصداقية للإدارة مع وجود تقرير توكيد بشأن إدارة مخاطر الأمن الإلكترونى بعد حدوث الإنتهاك.

إلا أنها تتناقض مع بعض الدراسات (Gordon et al.,2010; Wang et al., 2013; Ettredge et al., 2018; Haapamäki& Sihvonen.2019) بأن هناك تزايد فى عدد الشركات التى تقوم بالإفصاح عن إدارة مخاطر الأمن الإلكترونى والتهديدات التى تتعرض لها، مما كان له تأثير قوى سلبى على أسعار الأسهم وقيمة الشركات السوقية، خاصة تلك الشركات التى تنشر تقارير مراقب الحسابات عن تقرير الإدارة عن إدارة مخاطر الأمن الإلكترونى.

ويخلص الباحث إلى أن إجابات المستثمرين على أسئلة الحالات التجربية جاءت مؤيدة للفرض الأول، ممايعنى أهمية وجود تقرير توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى إيجاباً ومعنوياً على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية.

- **<u>نتيجة اختبار الفرض الثانى:</u>**

لاختبار هذا الفرض تم تحويله إلى فرض عدم كالتالى:

فرض العدم H_0: لايختلف التأثير الإيجابى المعنوى لتوكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية بإختلاف مستوى التأهيل العلمى للمستثمر.

وتم اختباره بواسطة اختبار Mann-Whitney Test على عينتين مستقلتين.

فإذا كان لايوجد تأثير للتأهيل العلمى للمستثمر على العلاقة محل الدراسة يتم قبول فرض العدم ورفض الفرض البديل، بينما إذا كان يوجد تأثير يتم رفض فرض العدم وقبول الفرض البديل.

وفيما يلى نتائج اختبار الفرض الثانى فى ظل الحالتين التجريبيتين:

جدول(١٠) الحالة الأولى

Mann-Whitney Test				
	التأهيل العلمي للمستثمر	N	Mean Rank	Sum of Ranks
Q1	1	35	33.29	1165.00
	0	30	32.67	980.00
	Total	65		
Q2	1	35	27.64	967.50
	0	30	39.25	1177.50
	Total	65		
a. Grouping Variable: Degree				

Test Statistics[a]		
	Q1	Q2
Mann-Whitney U	515.000	337.500
Wilcoxon W	980.000	967.500
Z	-.162	-3.086
Asymp. Sig. (2-tailed)	.871	.002

يتضح من الجداول السابقة أن قيمة P-Value أكبر من 5% بالنسبة للسؤال الأول Q1 حيث (Sig.=0.871) تعنى عدم وجود تأثير معنوى للتأهيل العلمى للمستثمر على قرار الاستثمار فى الأسهم فى حالة الإفصاح عن إدارة مخاطر الأمن الإلكترونى، وعدم وجود تقرير توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى، بينما كانت P-Value أقل من 5% بالنسبة للسؤال الثانى Q2 حيث (Sig.=0.002) تعنى وجود تأثير معنوى للتأهيل العلمى للمستثمر على توقع سعر السهم وقرار الاستثمار فى الأسهم فى حالة إفصاح الإدارة عن إدارة مخاطر الأمن الإلكترونى وعدم وجود تقرير توكيد مراقب الحسابات لذلك يتم **قبول الفرض البديل قبولاً جزئياً فى ظل الحالة الأولى H_2 بإختلاف التأثير الإيجابى المعنوى لتوكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية بإختلاف مستوى التأهيل العلمى للمستثمر.**

وتتفق هذه النتائج مع الدراسات السابقة (Wang et al., 2013; Miazee et al., 2014; Samad, 2017; Gupta et al., 2018; Navarro& Sutton, 2021) فى وجود تأثير لمستوى التأهيل العلمى للمستثمر على توقعه لسعر السهم، إلا أنها تتناقض معها فى أن مستوى التأهيل العلمى للمستثمر غير مؤثر على وجود تقرير توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى من عدمه.

ويرى الباحث أن هذه النتيجة منطقية لأن التأهيل العلمى قد يؤثر على توقع سعر السهم فى حال عدم وجود تقرير توكيد من مراقب الحسابات، لكنه ليس له علاقة بوجود تقرير توكيد مراقب الحسابات من عدمه.

جدول(١١) الحالة الثانية

Mann-Whitney Test				
	التأهيل العلمي للمستثمر	N	Mean Rank	Sum of Ranks
Q1	1	35	33.36	1167.50
	0	30	32.58	977.50
	Total	65		
Q2	1	35	35.51	1243.00
	0	30	30.07	902.00
	Total	65		
Q3	1	35	35.74	1251.00
	0	30	29.80	894.00
	Total	65		
Q4	1	35	33.57	1175.00
	0	30	32.33	970.00
	Total	65		

Test Statistics[a]				
	Q1	Q2	Q3	Q4
Mann-Whitney U	512.500	437.000	429.000	505.000
Wilcoxon W	977.500	902.000	894.000	970.000
Z	-.262	-1.535	-1.580	-.306
Asymp. Sig. (2-tailed)	.793	.125	.114	.760

يتضح من الجداول السابقة أن قيمة P-Value أكبر من 5% مما يعنى عدم وجود تأثير معنوى للتأهيل العلمى للمستثمر على قرار الاستثمار فى الأسهم فى حالة وجود تقرير توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى، لذلك تم **قبول فرض العدم**

ورفض الفرض البديل فى ظل الحالة الثانية H_2 بإختلاف التأثير الإيجابى المعنوى لتوكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية بإختلاف مستوى التأهيل العلمى للمستثمر.

وتتناقض هذه النتائج مع بعض الدراسات (Wang et al., 2013; Miazee et al., 2014; Samad, 2017; Gupta et al., 2018; Navarro& Sutton, 2021) حيث تبين عدم وجود تأثير لتوكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية بإختلاف مستوى التأهيل العلمى للمستثمر.

ويرى الباحث أنها نتيجة منطقية أيضاً، حيث وجود تقرير توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى فى حد ذاته يوفر الثقة للمستثمر ويجعله معتمداً عليه فى توقع سعر السهم دون الحاجة للتأهيل العلمى له.

- **<u>نتيجة اختبار الفرض الثالث:</u>**

لاختبار هذا الفرض تم تحويله إلى فرض عدم كالتالى:

فرض العدم H_0: لايختلف التأثير الإيجابى المعنوى لتوكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية بإختلاف مستوى خبرة المستثمر.

وتم اختباره بواسطة اختبار Mann-Whitney Test على عينتين مستقلتين.

فإذا كان لايوجد تأثير لخبرة المستثمر على العلاقة محل الدراسة يتم قبول فرض العدم ورفض الفرض البديل، بينما إذا كان يوجد تأثير يتم رفض فرض العدم وقبول الفرض البديل.

وفيما يلى نتائج اختبار الفرض الثالث فى ظل الحالتين التجريبيتين:

جدول(١٢) الحالة الأولى

Mann-Whitney Test				
	خبرة المستثمر	N	Mean Rank	Sum of Ranks
Q1	1	32	35.72	1143.00
	0	33	30.36	1002.00
	Total	65		
Q2	1	32	26.05	833.50
	0	33	39.74	1311.50
	Total	65		

Test Statistics[a]		
	Q1	Q2
Mann-Whitney U	441.000	305.500
Wilcoxon W	1002.000	833.500
Z	-1.406	-3.652
Asymp. Sig. (2-tailed)	.160	.000

يتضح من الجداول السابقة أن قيمة P-Value أكبر من 5% بالنسبة للسؤال الأول Q1 حيث (Sig.=0.160) تعنى عدم وجود تأثير معنوى لخبرة المستثمر على قرار الاستثمار فى الأسهم فى حالة الإفصاح عن إدارة مخاطر الأمن الإلكترونى وعدم وجود تقرير توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى، بينما كانت P-Value أقل من 5% بالنسبة للسؤال الثانى Q2حيث (Sig. =0.000) تعنى وجود تأثير معنوى لخبرة المستثمر على توقع سعر السهم وقرار الاستثمار فى الأسهم فى حالة إفصاح الإدارة عن إدارة مخاطر الأمن الالكترونى وعدم وجود تقرير توكيد مراقب الحسابات. لذلك يتم **قبول الفرض البديل قبولاً جزئياً فى ظل الحالة الأولى H_3 بإختلاف التأثير الإيجابى المعنوى لتوكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية بإختلاف مستوى خبرة المستثمر.**

وتتفق هذه النتائج مع الدراسات السابقة (Noghondari & Foong,2013; Casterella et al.,2020) فى وجود تأثير لمستوى الخبرة للمستثمر على توقعه لسعر السهم، إلا أنها تتناقض معها فى أن مستوى الخبرة للمستثمر غير مؤثر على وجود تقرير توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى من عدمه.

ويرى الباحث أن هذه النتيجة منطقية لأن مستوى الخبرة للمستثمر قد يؤثر على توقع سعر السهم فى حال عدم وجود تقرير توكيد من مراقب الحسابات، لكنه ليس له علاقة بوجود تقرير توكيد مراقب الحسابات من عدمه.

جدول(١٣) الحالة الثانية

Mann-Whitney Test				
	خبرة المستثمر	N	Mean Rank	Sum of Ranks
Q1	1	32	35.14	1124.50
	0	33	30.92	1020.50
	Total	65		
Q2	1	32	38.11	1219.50
	0	33	28.05	925.50
	Total	65		
Q3	1	32	38.23	1223.50
	0	33	27.92	921.50
	Total	65		
Q4	1	32	32.27	1032.50
	0	33	33.71	1112.50
	Total	65		

Test Statistics[a]				
	Q1	Q2	Q3	Q4
Mann-Whitney U	459.500	364.500	360.500	504.500
Wilcoxon W	1020.500	925.500	921.500	1032.500
Z	-1.433	-2.844	-2.749	-.358
Asymp. Sig. (2-tailed)	.152	.004	.006	.720

يتضح من الجداول السابقة أن قيمة P-Value أكبر من 5% بالنسبة للسؤال الأول والرابع Q1 و Q4 حيث (Sig.=0.152, 0.720) تعنى عدم وجود تأثير معنوى لخبرة المستثمر على سعر السهم، وتوقع سعر السهم فى حالة وجود تقرير توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى، بينما كانت P-Value أقل من 5% بالنسبة للسؤال الثانى والثالث Q2، Q3 حيث (Sig.=0.004, 0.006) تعنى وجود تأثير معنوى لخبرة المستثمر على قرار الاستثمار فى الأسهم، وأولوية الاستثمار فى أسهم الشركة بالنسبة للمنافسين، فى حالة إفصاح الإدارة عن إدارة مخاطر الأمن الإلكترونى ووجود تقرير توكيد مراقب الحسابات، لذلك يتم **قبول الفرض البديل قبولاً جزئياً فى ظل الحالة الثانية H_3 بإختلاف التأثير الإيجابى المعنوى لتوكيد**

مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية بإختلاف مستوى خبرة المستثمر.

وتتفق هذه النتائج مع الدراسات السابقة (Noghondari & Foong,2013; Casterella et al.,2020) فى وجود تأثير لمستوى الخبرة للمستثمر عند إتخاذ القرار بالاستثمار فى أسهم الشركة، وعلى تحديد أولوية الاستثمار فى أسهم الشركة مقارنة بالشركات المنافسة فى حالة وجود تقرير مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى.

إلا أنها تتناقض معها فى أن مستوى الخبرة للمستثمر غير مؤثر على تحديد سعر السهم للشركة، وعلى توقع المستثمر لسعر السهم، فى حالة وجود تقرير مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى.

ويرى الباحث أن هذه النتيجة منطقية لأنه فى حالة وجود تقرير مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى، فإن المستثمر لايستخدم خبرته فى تحديد سعر السهم أو توقعه وإنما يعتمد على تقرير مراقب الحسابات فى هذه الحالة.

- **نتائج اختبار التحليلات الأخرى للفرض الأول:**

تهتم التحليلات الأخرى بإعادة اختبار الفرض الرئيسى فى التحليل الأساسى من خلال إضافة متغير جديد كمتغير معدل أو رقابى، وذلك لاختبار قوة نتائج التحليل الأساسى ومدى كفاية وملاءمة افتراضات بناء نموذجه، وتوفير مزيداً من الوضوح للعلاقة الرئيسية (زكى،2018).

ولذلك سيعتمد الباحث من خلال تحليل الدراسات السابقة (Wang et al., 2013; Miazee et al., 2014; Samad, 2017; Gupta et al., 2018; Casterella et al., 2020; Navarro& Sutton, 2021) على اختبار تأثير مستوى التأهيل والخبرة للمستثمر معاً كمتغير معدل للعلاقة الرئيسية، حيث يختبر تأثير توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى كمتغير مستقل على قرار المستثمرين فى مصر للإستثمار فى الأسهم كمتغير تابع فى ظل إختلاف مستوى التأهيل والخبرة للمستثمر معاً كمتغير معدل، وذلك بإجراء اختبار Mann-Whitney Test على عينتين مستقلتين، ولاختباره إحصائياً تم إعادة صياغته كفرض عدم كما يلى:

فرض العدم H_0: لايختلف التأثير الإيجابى المعنوى لتوكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية بإختلاف مستوى التأهيل والخبرة للمستثمر معاً.

فإذا كان لايوجد تأثير مشترك للتأهيل العلمى وخبرة المستثمر معاً على العلاقة محل الدراسة يتم قبول فرض العدم ورفض الفرض البديل، بينما إذا كان يوجد تأثير مشترك يتم رفض فرض العدم وقبول الفرض البديل. وفيما يلى نتائج اختبار الفرض فى ظل الحالتين التجريبيتين:

جدول(١٤) الحالة الأولى

Mann-Whitney Test				
	خبرة وتأهيل معا	N	Mean Rank	Sum of Ranks
Q1	١	32	35.72	1143.00
	٠	33	30.36	1002.00
	Total	65		
Q2	١	32	26.05	833.50
	٠	33	39.74	1311.50
	Total	65		

Test Statistics[a]		
	Q1	Q2
Mann-Whitney U	441.000	305.500
Wilcoxon W	1002.000	833.500
Z	-1.406	-3.652
Asymp. Sig. (2-tailed)	.160	.000

يتضح من الجداول السابقة أن قيمة P-Value أكبر من 5% بالنسبة للسؤال الأول Q1 حيث (Sig.=0.160) تعنى عدم وجود تأثير معنوى مشترك للتأهيل العلمى وخبرة المستثمر معاً على قرار الاستثمار فى الأسهم فى حالة الإفصاح عن إدارة مخاطر الأمن الإلكترونى، وعدم وجود تقرير توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى، بينما كانت P-Value أقل من 5% بالنسبة للسؤال الثانى Q2حيث (Sig. =0.000) تعنى وجود تأثير معنوى مشترك للتأهيل العلمى وخبرة المستثمر معاً على توقع سعر السهم وقرار الاستثمار فى الأسهم فى حالة إفصاح الإدارة عن إدارة مخاطر الأمن الإلكترونى وعدم وجود تقرير توكيد مراقب

الحسابات. لذلك يتم **قبول الفرض البديل قبولاً جزئياً فى ظل الحالة الأولى H_1 بإختلاف التأثير الإيجابى المعنوى لتوكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية بإختلاف مستوى التأهيل والخبرة للمستثمر معاً.**

وتتفق هذه النتائج مع بعض الدراسات السابقة (Wang et al., 2013; Miazee et al., 2014; Samad, 2017; Gupta et al., 2018; Casterella et al., 2020; Navarro& Sutton, 2021) فى وجود تأثير مشترك لمستوى التأهيل والخبرة للمستثمر عند توقع سعر السهم، إلا أنها تتناقض معها فى أن مستوى التأهيل والخبرة للمستثمر معاً غير مؤثر على وجود تقرير توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى من عدمه.

ويرى الباحث أن هذه النتيجة منطقية لأن مستوى التأهيل والخبرة للمستثمرمعاً قد يؤثر على توقع سعر السهم فى حال عدم وجود تقرير توكيد من مراقب الحسابات، لكنه ليس له علاقة بوجود تقرير توكيد مراقب الحسابات من عدمه.

جدول(١٥) الحالة الثانية

Mann-Whitney Test				
	خبرة وتأهيل معا	N	Mean Rank	Sum of Ranks
Q1	1	32	35.14	1124.50
	0	33	30.92	1020.50
	Total	65		
Q2	1	32	38.11	1219.50
	0	33	28.05	925.50
	Total	65		
Q3	1	32	38.23	1223.50
	0	33	27.92	921.50
	Total	65		
Q4	1	32	32.27	1032.50
	0	33	33.71	1112.50
	Total	65		

Test Statistics[a]				
	Q1	Q2	Q3	Q4
Mann-Whitney U	459.500	364.500	360.500	504.500
Wilcoxon W	1020.500	925.500	921.500	1032.500
Z	-1.433	-2.844	-2.749	-.358
Asymp. Sig. (2-tailed)	.152	.004	.006	.720

يتضح من الجداول السابقة أن قيمة P-Value أكبر من 5% بالنسبة للسؤال الأول والرابع Q1 و Q4 حيث (Sig.=0.152, 0.720) تعنى عدم وجود تأثير معنوى مشترك للتأهيل العلمى وخبرة المستثمر معاً على سعر السهم وعلى توقع سعر السهم فى حالة وجود تقرير توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى، بينما كانت P-Value أقل من 5% بالنسبة للسؤال الثانى والثالث Q2, Q3 ، حيث (Sig.=0.004, 0.006) تعنى وجود تأثير معنوى مشترك للتأهيل العلمى وخبرة المستثمر معاً على قرار الاستثمار فى الأسهم، وأولوية الاستثمار فى أسهم الشركة بالنسبة للمنافسين، فى حالة إفصاح الإدارة عن إدارة مخاطر الأمن الإلكترونى ووجود تقرير توكيد مراقب الحسابات، لذلك يتم **قبول الفرض البديل قبولاً جزئياً فى ظل الحالة الثانية H_1 بإختلاف التأثير الإيجابى المعنوى لتوكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية بإختلاف مستوى التأهيل والخبرة للمستثمر معاً.**

وتتفق هذه النتائج مع الدراسات السابقة (Wang et al., 2013; Miazee et al., 2014; Samad, 2017; Gupta et al., 2018; Casterella et al., 2020; Navarro& Sutton, 2021) فى وجود تأثير مشترك لمستوى التأهيل والخبرة للمستثمر معاً عند إتخاذ القرار بالاستثمار فى أسهم الشركة، وعلى تحديد أولوية الاستثمار فى أسهم الشركة مقارنة بالشركات المنافسة فى حالة وجود تقرير مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى.

إلا أنها تتناقض معها فى أن مستوى التأهيل والخبرة للمستثمر معاً غير مؤثر على تحديد سعر السهم للشركة، وعلى توقع المستثمر لسعر السهم، فى حالة وجود تقرير مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى.

ويرى الباحث أن هذه النتيجة منطقية لأنه فى حالة وجود تقرير مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى، فإن المستثمر لايستخدم تأهيله أو خبرته فى تحديد سعر السهم أو توقعه وإنما يعتمد على تقرير مراقب الحسابات فى هذه الحالة. كما أن أهمية التأهيل والخبرة للمستثمر فى مصر تقل حيث يتجه كثير من المستثمرين لشركات الوساطة والسمسرة للقيام بإتخاذ قرار الاستثمار بدلاً منهم.

جدول(١٦) ملخص نتائج إختبار فروض الدراسة

الفرض	فروض البحث فى ظل التحليل الأساسى	نتائج الحالة الأولى	نتائج الحالة الثانية
H_1	يؤثر توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى إيجاباً ومعنوياً على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية.	تم قبوله	تم قبوله
H_2	يختلف التأثير الإيجابى المعنوى لتوكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية بإختلاف مستوى التأهيل العلمى للمستثمر.	تم قبوله جزئياً	تم رفض الفرض
H_3	يختلف التأثير الإيجابى المعنوى لتوكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية بإختلاف مستوى خبرة المستثمر.	تم قبوله جزئياً	تم قبوله جزئياً
الفرض	فرض البحث فى ظل التحليل الإضافى	نتائج الحالة الأولى	نتائج الحالة الثانية
H_1	يختلف التأثير الإيجابى المعنوى لتوكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية بإختلاف مستوى التأهيل والخبرة للمستثمر معاً.	تم قبوله جزئياً	تم قبوله جزئياً

5/7- النتائج والتوصيات ومجالات البحث المقترحة

استهدف البحث دراسة واختبار العلاقة بين توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى وقرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية. وكذلك اختبار أثر تأهيل وخبرة المستثمرين على العلاقة محل الاختبار، ولقد اعتمد الباحث على إجراء دراسة تجريبية، على عينة من 65 من المستثمرين المؤسسيين والذين يتمثلون فى أمناء الاستثمار فى البنوك التجارية المصرية.

وأجابت الدراسة فى شقها التجريبى على **السؤال الأول** والخاص بماهو شكل وإتجاه العلاقة بين توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى وقرار الاستثمار بالأسهم؟، حيث تم قبول الفرض الرئيسى H_1 .

وركز **السؤال الثانى** والخاص بهل تختلف هذه العلاقة بإختلاف مستوى التأهيل والخبرة للمستثمر؟، حيث تم قبول الفرض H_2 قبولاً جزئياً حيث أن التأهيل العلمى قد يؤثر على توقع سعر السهم فى حال عدم وجود تقرير توكيد من مراقب الحسابات، لكنه ليس له علاقة بوجود تقرير توكيد مراقب الحسابات من عدمه. كما أن وجود تقرير توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى فى حد ذاته يوفر الثقة للمستثمر ويجعله معتمداً عليه فى توقع سعر السهم دون الحاجة للتأهيل العلمى له.

كما تم قبول الفرض H_3 قبولاً جزئياً حيث أن مستوى الخبرة للمستثمر قد يؤثر على توقع سعر السهم فى حال عدم وجود تقرير توكيد من مراقب الحسابات، لكنه ليس له علاقة بوجود تقرير توكيد مراقب الحسابات من عدمه. كما أن وجود تقرير مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى، يجعل المستثمر لايستخدم خبرته فى تحدد سعر السهم أو توقعه وإنما يعتمد على تقرير مراقب الحسابات فى هذه الحالة.

وأكدت التحليلات الأخرى نتائج التحليل الأساسى بشأن أثر إختلاف مستوى التأهيل والخبرة معاً للمستثمر على هذه العلاقة، حيث تم القبول الجزئى للفرض، حيث تبين أن مستوى التأهيل والخبرة للمستثمرمعاً قد يؤثر على توقع سعر السهم فى حال عدم وجود تقرير توكيد من مراقب الحسابات، لكنه ليس له علاقة بوجود تقرير توكيد مراقب الحسابات من عدمه. كما أن وجود تقرير مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى، يجعل المستثمر لايستخدم تأهيله أو خبرته فى تحديد سعر السهم أو توقعه وإنما يعتمد على تقرير مراقب الحسابات فى هذه الحالة.

وفى ضوء أهداف البحث وحدوده ومشكلته وما إنتهى إليه من نتائج، يوصى الباحث بمايلى:

- إصدار دليل إسترشادى للأمن الإلكترونى يحدد الضوابط المتعلقة بالأمن الإلكترونى التى تساعد على تحسين إدارة والإفصاح عن إدارة مخاطر الأمن الإلكترونى فى الشركات.
- إصدار قانون ملزم للشركات المقيدة بالبورصة للإفصاح عن مخاطر الأمن الإلكترونى وبرامج إدارة مخاطر الأمن الإلكترونى.
- توفير التأهيل والتدريب اللازمين للمراجعين الداخليين للتعرف على مخاطر الأمن الإلكترونى.

- توفير الخلفية الملائمة فى تكنولوجيا المعلومات فى الشركات، خاصة للعاملين بإدارة تكنولوجيا المعلومات وإدارة المراجعة الداخلية وإدارة المخاطر.
- توفير الوعى بمخاطر الأمن الإلكترونى من قبل الإدارة فى الشركات، مع توفير تأمين خاص على تعاملاتها الإلكترونية ضد مخاطر الأمن الإلكترونى.
- توفير التأهيل والتدريب اللازمين لمكاتب المراجعة لتوفير خدمات التوكيد على الإفصاح عن إدارة مخاطر الأمن الإلكترونى.
- تحديث معيار التأكد المصرى رقم 3000 ليواكب تعديلات نظيره الدولى ISA 3000.

وفى ضوء ماسبق يقترح الباحث المجالات البحثية التالية مستقبلاً:

- أثر توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى على قرار منح الإئتمان – دراسة تجربية.
- أثر الافصاح عن توكيد المراجع الداخلى على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى على قرار الاستثمار بالأسهم – دراسة تجربية.
- أثر الإفصاح عن إدارة مخاطر الأمن الإلكترونى فى التقارير المالية على أسعار الأسهم وأحجام التداول فى البورصة– دراسة تطبيقية.
- دور إدارة المراجعة الداخلية التوكيدى والاستشارى فى إدارة مخاطر الأمن الإلكترونى فى التقارير المالية– دراسة تجربية.
- أثر الافصاح عن مخاطر الأمن الإلكترونى على تقرير المراجع الخارجى وأتعاب عملية المراجعة– دراسة تطبيقية.
- أثر إدماج مخاطر الأمن الإلكترونى فى نموذج خطر المراجعة على تخطيط واجراءات المراجعة الخارجية – دراسة تجربية.

مراجع البحث

أولاً: المراجع العربية

- الاستراتيجية الوطنية للأمن السيبرانى.2017. ***المجلس الأعلى للأمن السيبرانى***، رئاسة مجلس الوزراء– جمهورية مصر العربية.
- الرشيدى، طارق عبدالعظيم، ودالیا عادل عباس السيد.2019. أثر الإفصاح عن مخاطر الأمن السيبرانى فى التقارير المالية على أسعار الأسهم وأحجام التداول– دراسة مقارنة فى قطاع تكنولوجيا المعلومات. ***مجلة المحاسبة والمراجعة، كلية التجارة– جامعة دمياط***، العدد الثانى:439–487.
- السمحان، منى عبدالله.2020. متطلبات تحقيق الأمن السيبرانى لأنظمة المعلومات الإدارية بجامعة الملك سعود. ***مجلة كلية التربية، جامعة المنصورة***، العدد111، يوليو:1– 28.
- الموسوعة السياسية، متاحة على الموقع:

https:political-encyclopedia.org

- الهيئة الوطنية للأمن السيبرانى، السعودية. 2017.
- داود، حسن طاهر.2000. جرائم نظم المعلومات. ***مجلة الأمن والحياة، جامعة نايف العربية للعلوم الأمنية***: 171–200.
- دستور جمهورية مصر العربية.2014.
- زكى، نهى محمد. 2018. ***أثر جودة المراجعة الخارجية على الحد من السلوك الانتهازى للإدارة ومنع الغش بالقوائم المالية: دراسة تطبيقة على الشركات المقيدة بالبورصة المصرية***، رسالة دكتوراه غير منشورة، كلية التجارة، جامعة الاسكندرية.
- عبدالرحيم، رضا محمود.2020.أثر التعديلات فى شكل ومحتوى تقرير مراقب الحسابات وفقا لمعيار المراجعة الدولي رقم 570 المعدل لسنة 2015 بشأن الإستمرارية على قرارى الاستثمار ومنح الإئتمان: دراسة تجربية، ***مجلة الاسكندرية للبحوث المحاسبية***، قسم المحاسبة والمراجعة، العدد الثانى، مايو – المجلد الرابع:1–94.

- عبدالفتاح،إسراء مصطفى.2016. ***أثر المعاملات مع الأطراف ذوى العلاقة على تخطيط إجراءات المراجعة وتقرير مراقب الحسابات***، رسالة ماجستير غير منشورة، كلية التجارة – جامعة الاسكندرية.
- عزام،عبدالمرضى حامد.1990. ***الإحصاء فى الإدارة***، لنكولن تشاو- ترجمة عبدالمرضى حامد عزام، دار المريخ، الرياض، السعودية.
- قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018.
- قرار رئيس الوزراء رقم 2259 لسنة 2014.
- قرار رئيس الوزراء رقم 1630 لسنة 2016.
- قرار رئيس الوزراء رقم 994 لسنة 2017.
- قرار رئيس الوزراء رقم 276 لسنة 2020.
- ماجد، أنور.2016. الأمن السيبرانى والقمة الخليجية الأمريكية. ***مجلة الأمن والحياة، جامعة نايف العربية للعلوم الأمنية***:18– 38.
- موسى، سعاد زغلول عبده. 2018. ***أثر توكيد المراجع الخارجى على تقارير الأعمال المتكاملة على قرارى الاستثمار ومنح الائتمان، دراسة تجريبية.*** رسالة دكتوراه غير منشورة، كلية التجارة – جامعة الاسكندرية.

ثانياً: المراجع الأجنبية

- AICPA.2017. Description Criteria for Management's Description of the Entity's Cybersecurity Risk Management Program. ***https://www.aicpa.org***
- AICPA. 2018a.Cybersecurity risk management reporting fact sheet. ***https://www.aicpa.org***
- AICPA.2018b.SOC for cybersecurity: a backgrounder. ***https://www.aicpa.org***
- AICPA.2021. SOC for Cybersecurity: Information for Organizations. ***https://www.aicpa.org***
- AICPA.2021. SOC for Cybersecurity: Information for CPAs. ***https://www.aicpa.org***
- AICPA.2021. SOC for Cybersecurity: Helping you build trust and transparency, ***https://www.aicpa.org***
- Agrafiotis, I., J.R. Nurse, M. Goldsmith, S.Creese, and D.Upton. 2018. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate, ***Journal of Cybersecurity***, Vol. 4, No. 1: 1-15.
- Aldorisio, J. 2020.Best Practices for Cybersecurity Auditing -a Step-by-Step Checklist, ***https://securityscorecard.com/***
- Amir, E., S.Levi, and T.Livne. 2018. Do firms underreport information on cyber-attacks? Evidence from capital markets. ***Rev. Account. Stud.***: 1–30.
- Amoroso, E.2007.***Cyber Security***. Kindle Edition.
- Asay, H., W. Elliott, and K. Rennekamp.2016. Disclosure Readability and the Sensitivity of Investors' Valuation Judgments to Outside Information, ***http://dx.doi.org/10.2139/ssrn.2497697***
- Bahmanziari, T., M. Odomb, and J. Ugrin.2009. An experimental evaluation of the effects of internal and external e-Assurance on initial trust formation in B2C e-commerce, ***International Journal of Accounting Information Systems***, 10: 152–170.
- Bianchi, D., and O.Tosun.2019. Cyber attacks and stock market activity. ***WBS Finance Group Research Paper*** ,No. 251, ***http:// dx.doi. org/ 10.2139/ssrn.3190454***

- Biener, C., M. Eling, and H.Wirfs. 2015. Insurability of cyber risk: an empirical analysis. Geneva Pap, ***Risk Insurance-Issues Pract***. 40 (1): 131–158.
- Bodin, L., L.A. Gordon, M.P. Loeb and A. Wang. 2018. Cybersecurity insurance and risk-sharing. ***Journal of Accounting and Public Policy***, 37(6): 527–544.
- Bonett, D., and T.Wright.2015. Cronbach's Alpha Reliability: Interval Estimation, Hypothesis Testing, and Sample Size Planning. ***Journal of Organizational Behavior***, 36 (1): 3-15.
- Casterella, R., R.Desir, M.Stallings, and J.Wainberg.2020. Information Transfer of Bankruptcy Announcements: Examining the Impact of Auditor Opinions, ***Accounting Horizons***, 34(1): 45-66.
- Cavusoglu, H., B. Mishra, and S. Raghunatha.2004. The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. ***International Journal of Electronic Commerce***, fall, Vol. 9, No. 1: 69-104.
- CESG .2012.Assurance of ICT systems and services. Good Practice Guide, No. 30, CESG Information Assurance Portal, ***available at: www.ncsc.gov.uk/content/files/guidance.***
- CPA Canada. 2020. When the world is evolving faster by the second, how can your cybersecurity keep up? Cybersecurity disclosure report, ***Available at https://assets.ey.com/content/dam/ey-sites/ey-com/en_ ca/ topics/cybersecurity/articles/how-tsx-top-60-are-approaching-cybersecurity-related-disclosures-/ey-cpa-cybersecurity-report.pdf.***
- Curtis, S., J.Carre, and D. Jones.2018.Consumer security behaviors and trust following a data breach, ***Managerial Auditing Journal***, Vol. 33, No. 4: 425-435.
- Demetz, L., and D.Bachlechner. 2013. To invest or not to invest? Assessing the economic viability of a policy and security configuration management tool. ***The Economics of Information Security and Privacy***, Springer: 25–47.

- Eaton, T., J. Grenier, and D. Layman.2019. Accounting and Cybersecurity Risk Management. ***American Accounting Association***, Vol. 13, No. 2: C1–C9.
- Ettredge, M.L., F.Guo, and Y. Li.2018.Trade secrets and cyber security breaches. ***Journal of Accounting and Public Policy***, Vol. 37, No. 6: 564-585.
- Evans, M., L. Maglaras, Y. He and H. Janicke. 2016. Human behaviour as an aspect of cybersecurity assurance. SECURITY AND COMMUNICATION NETWORKS. ***Security Comm. Networks***, 9:4667–4679.
- Frank, M. L., J. H. Grenier, and J.S. Pyzoha. 2019. How disclosing a prior cyberattack influences the efficacy of cybersecurity risk management reporting and independent assurance. ***Journal of Information Systems***, 33(3): 183–200.
- Frank M., H. Grenier, and S. Pyzoha.2021. Board liability for cyberattacks: The effects of a prior attack and implementing the AICPA's cybersecurity framework. ***J. Account. Public Policy***: 1-16.
- Gal-Or, E., and A.Ghose. 2005. The economic incentives for sharing security information incentives for sharing security information. ***Inf. Syst. Res***, 16 (2): 186–208.
- Ghosh, S., and X. Li. 2013. A real options model for generalized meta-staged projects – ***valuing the migration to SOA. Inform. Syst. Res***, 24 (4):1011–1027.
- Goldstein, P. 2021. What Is a Cyber security Audit and Why Is It Important ? Cyber security audits help ensure agencies comply with IT security regulations and requirements. ***https://fedtechmagazine.com/***
- Gordon, A., M. Loeb, W. Lucyshyn, and T. Sohail. 2006. The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. ***Journal of Accounting and Public Policy***, 25: 503–530.
- Gordon, A. and P. Loeb. 2006. ***Managing Cybersecurity Resources: A Cost–Benefit Analysis***, McGraw Hill, New York, NY, ISBN 0-07-145285-0.

- Gordon, L. A., M.P. Loeb, and L. Zhou. 2011. The impact of information security breaches: Has there been a downward shift in costs?. ***Journal of Computer Security***, 19(1): 33–56.
- Gordon, L.A., M. Loeb, W. Lucyshyn, and L. Zhou. 2015. The impact of information sharing on cybersecurity underinvestment: a real options perspective. ***Journal of Accounting and Public Policy***, 34(5):509–519.
- Gordon, L.A., M.Loeb, and T.Sohail.2010.Market value of voluntary disclosures concerning information security. ***MIS Quarterly***, Vol. 34, No. 3: 567-594.
- Gupta, G., J. Mahaud, and B. Debata. 2018. Impact of CEO's characteristics on investment decisions of Indian listed firms: does crisis make any difference, ***available at https:// doi.org/ 10.1080/ 23322039.***
- Haapamäki, E. and J. Sihvonen.2019. Cybersecurity in accounting research. ***Managerial Auditing Journal***, Vol. 34, No. 7: 808-834.
- Hancock, M. 2017.UK cyber security research report. Department for Digital, Culture, Media & Sport, ***available at: www.gov.uk/ government/publications/cyber-security-breaches-survey***
- Illiashenko, O., V. Kharchenko, and A. Kor .2018. GAP-Analysis of Assurance Case-Based Cybersecurity Assessment: Technique and Case study. ***Advanced Information Systems***, Vol. 2, No. 1:64-68.
- Janvrin, D. and T. Wang. 2019. Implications of Cybersecurity on Accounting Information. ***Journal of Information Systems***, American Accounting Association, Vol. 33, No. 3, fall: A1–A2.
- Jeong, C., S. Lee, and J. Lim. 2018. Information security breaches and IT security investments: Impacts on competitors***. Information & Management, https: //doi.org/ 10.1016/j.im.2018.11.003.***
- Kahyaoglu S. and K. Caliyurt.2018. Cyber security assurance process from the internal audit perspective. ***Managerial Auditing Journal***, Vol. 33, No. 4: 360-376.
- Kamiya, S., J.K. Kang, J. Kim, A. Milidonis, and R.M. Stulz. 2021. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. ***Journal of Financial Economics,*** 139: 719–749.

- Kelton, A. and R. Pennington.2019. Do voluntary disclosures mitigate the cybersecurity breach contagion effect?. ***Forthcoming, Journal of Information Systems, https:// www. researchgate. net/ publication/***
- Khazanchi, D.and S. Sutton.2001. Assurance Services for Business-to-Business Electronic Commerce: A Framework and Implications. ***Journal of the Association for Information Systems***, Faculty Publications. 3***. https://digitalcommons.unomaha.edu/isqafacpub/3***
- Kissel, R. 2013.Explore terms: a glossary of common cybersecurity terminology, National Initiative for Cybersecurity Careers and Studies, ***available at: https://niccs.us-cert.gov/glossary.***
- Lange, R., and EW.Burger .2017. Long-term market implications of data breaches. ***Journal of Information Privacy and Security***: 211-220.
- Lawrence A., P. Gordon, L. Loeb, and L. Zhou.2015. The impact of information sharing on cybersecurity underinvestment: A real options perspective. ***J. Account. Public Policy***, 34: 509–519.
- Lawrence D., G.Lawrence, M. Loebb, and A. Wangc. 2018. Cybersecurity insurance and risk-sharing***. Journal of Accounting and Public Policy***, 37: 527–544.
- Levišauskait, K.2010.Investment Analysis and Portfolio Management. Leonardo da Vinci programme project. ***Education and Culture DG, Vytautas Magnus University Kaunas, Lithuania, Bulgaria.***
- Masli, V.J, M.W. Watson, and R.W. Zmud. 2016. Senior executives' IT management responsibilities: serious IT-related deficiencies and CEO/CFO turnover. ***MIS Quarterly***, 40(3): 687–708.
- Matar, S. 2012. The impact of legal responsibility of external auditors on auditing quality and investment level. ***Unpublished PHD dissertation, Brunel University London.***
- Miazee, M., A. Shareef, and M. Hasan. 2014. Fundamentals knowledge of investor and its influence on investment in capital market- A study from Dhaka stock exchange. ***Research Journal of Finance and Accounting***, 5 (24): 192-204.
- National Institute of Standards and Technology (NIST) .2013a. Glossary of key information security terms, National Institute of

Standards and Technology Interagency or Internal Report, NISTIR 7298, Revision 2, ***available at: http://csrc.nist.gov/publications.***

- Navarro, P. and S. Sutton. 2021. Investors' Judgment and Decisions after a Cyber security Breach: Understanding the Value Relevance of Cyber security Risk Management Assurance, (February, 1):1-52. ***Available at http://dx.doi.org/10.2139/ssrn.3817763***
- No and Vasarhelyi. 2017. Cybersecurity and Continuous Assurance. ***Journal of Emerging Technologies in Accounting***, Vol. 14, No. 1:1-12.
- Noghondari, T., and S. Foong.2013. Antecedents and consequences of audit expectation gap: Evidence from the banking sector in Malaysia. ***Managerial Auditing Journal***, 28 (5): 384-406.
- O'Reilly, D.M. 2009. Do investors perceive the going-concern opinion as useful for pricing stocks? ***Managerial Auditing Journal***, 25(1): 4-16.
- Pflugrath, G., P. Roebuck ,R. Simnett.2011. Impact of Assurance and Assurer's Professional Affiliation on Financial Analysts' Assessment of Credibility of Corporate Social Responsibility Information, ***Auditing: A Journal of Practice & Theory***, 30 (3): 239–254. https: //doi.org/ 10.2308/ajpt-10047.
- Richardson, V., M. Watson, and R.Smith .2019. Much Ado about Nothing: The (Lack of) Economic Impact of Data Privacy Breaches. ***Journal of Information Systems***, Vol. 33, No. 3: 227-265.
- Rosati, P.2019. Audit Firm Assessments of Cyber-Security Risk: Evidence from Audit Fees and SEC Comment Letters. ***The International Journal of Accounting***, Vol. 54, No. 3:1-56.
- Rosati, P., M.Cummins, P.Deeney, F.Gogolin, L.Werff, and T.Lynn.2017.The effect of data breach announcements beyond the stock price: Empirical evidence on market activity. ***International Review of Financial Analysis***, V.49:146-154.
- Samad, A. 2017.Relationship and Impact of Risk Aversion & Financial Knowledge on Individual Investment's Decision, ***available at https://www.linkedin.com.***

- Santhosh, T. and K.Thiyagu. 2021. Cognizing Scams and Frauds in Cyber Space and its Preventive Measures. ***Academia Letters, Article 1170,https://doi.org/10.20935/AL1170***.
- Securities and Exchange Commission (SEC). 2018. Commission Statement and Guidance on Public Company Cybersecurity Disclosures Release Nos. 33-10459; 34-82746. ***Available at: https:// www. sec. gov/ rules/interp/ 2018/33-10459.pdf.***
- Spanos, G., and L. Angelis. 2016. The impact of information security events to the stock market***: A systematic literature review, Computers & Security***, Vol.58:216–229.
- Tan, H. T., and Y. Yu. 2018. Management's Responsibility Acceptance, Locus of Breach, and Investors' Reactions to Internal Control Reports. ***The Accounting Review***, 93 (6): 331–355.
- Tosun, O. K.2021. Cyber-attacks and stock market activity. ***International Review of Financial Analysis*** ,76 :1-15.
- Vekez, N. 2019. Three Studies on Cybersecurity Disclosure and Assurance, ***A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy***. University of Central Florida.
- Wang, Y., K.Kannan, and J.Ulmer.2013.The association between the disclosure and the realization of information security risk factors. ***Information Systems Research***, Vol. 24, No. 2: 201-218.
- Wertheim, S.2019. Auditing for Cybersecurity Risk. ***https://www.cpajournal.com/***
- Zureigat, Q. M .2014. Factors Associated with Audit Reports in Saudi Arabia. ***Global Journal of Management and Business Research***, 14 (5):67-74.

ملحق رقم (1)

معايير الأمن الإلكترونى

أولاً: معايير الوصف

المجموعة	المعيار
1- طبيعة الأعمال والعمليات	م1: مراعاة طبيعة أعمال المنظمة وعملياتها بما فى ذلك المنتجات أو الخدمات الرئيسية والأسواق الرئيسية وطرق التسويق بها.
2- طبيعة المعلومات فى بيئة الخطر	م2: مرعاة طبيعة المعلومات الأساسية التى تم إنشائها أو جمعها أو إرسالها أو إستخدامها أو تخزينها بواسطة الأفراد.
3- أهداف برنامج إدارة مخاطر الأمن الإلكترونى	م3: مراعاة أهداف البرنامج المتعلقة بالإتاحة والسرية وسلامة البيانات والمعالجة. م4: إنشاء أهداف للأمن الإلكترونى والحفاظ عليها والموافقة عليها لدعم تحقيق أهداف المنظمة.
4- العوامل المؤثرة على إدارة مخاطر الأمن الإلكترونى	م5: تشمل هذه العوامل: (1) خصائص التقنيات وأنواع الإتصال وقنوات الإتصال المستخدمة من قبل المنظمة، (2)الخصائص التنظيمية،(3) خصائص البيئة التكنولوجية والتغيرات التنظيمية والتغييرات الأخرى خلال فترة التقرير. م6: فى حالة حدوث إختراقات يجب:(1)تحديده خلال ال 12 شهر التى سبقت هذه الفترة التى حددت فيها الإدارة الوصف،(2) تحديد قيمة الإنخفاض الحادث فى المنظمة ومدى تحقيق أهداف الأمن الإلكترونى مع الإفصاح عمايلى: (أ) طبيعة الإختراق، (ب) توقيت الإختراق، (ج) تأثير هذا الإختراق وكيفية التخلص منه.
5- هيكل حوكمة إدارة	م7: ترسيخ قيم النزاهة والأخلاق والحفاظ عليها ونقلها إلى العاملين ببرنامج إدارة مخاطر الأمن الإلكترونى.

مخاطر الأمن الإلكترونى	م8: إشراف مجلس الإدارة على برنامج إدارة مخاطر الأمن الإلكترونى للمنظمة. م9: إنشاء خطوط للمساءلة والتقرير فى مجال الأمن الإلكترونى. م10: تطوير مهارات الأفراد القائمين على مسئوليات الأمن الإلكترونى.
6- تقييم مخاطر الأمن الإلكترونى	م11: (1) تحديد مخاطر الأمن الإلكترونى والبيئة والتغيرات التكنولوجية والتنظيمية والتغييرات الأخرى التى يكون لها تأثير جوهرى على مخاطر الأمن الإلكترونى للمنظمة. (2) تقييم المخاطر ذات الصلة بتحقيق المنظمة لأهداف الأمن الإلكترونى. م12: تحديد وتقييم وإدارة المخاطر المرتبطة بالموردين وشركاء العمل.
7- إتصالات الأمن الإلكترونى وجودة معلومات الأمن الإلكترونى	م13: وجود إتصال داخلى بمعلومات الأمن الإلكترونى الضرورية لدعم أداء برنامج إدارة مخاطر الأمن الإلكترونى للمنظمة بما فى ذلك:(1) أهداف ومسئوليات الأمن الإلكترونى(2) خطوات الإتصال المحددة للإختراقات الأمنية التى يتم مراقبتها والتحقيق فيها وتحديد أنها إختراقات أمنية تتطلب الإستجابة أو العلاج أو كليهما. م14: التواصل مع الأطراف الخارجية فيما يتعلق بالأمور التى تؤثر على أداء برنامج إدارة مخاطر الأمن الإلكترونى للمنظمة.
8- مراقبة برنامج إدارة مخاطر الأمن الإلكترونى	م15: إجراء تقييمات مستمرة ودورية للفعالية التشغيلية لأنشطة الرقابة الرئيسية والمكونات الأخرى للرقابة الداخلية المتعلقة بالأمن الإلكترونى. م16: تقييم التهديدات الأمنية المحددة والإفصاح عنها فى الوقت الملائم وكذلك نقاط الضعف فى الرقابة على الأطراف المسئولة عند إتخاذ الإجراءات التصحيحية بما فى ذلك الإدارة ومجلس الإدارة.
9- مراقبة الأمن الإلكترونى	م17: تطوير الإستجابة للمخاطر المتوقعة بما فى ذلك التصميم وتنفيذ عمليات المراقبة. م18: تحديد ملخص للبنية التحتية لتكنولوجيا المعلومات فى المنظمة وخصائص شبكة المعلومات. م19: تحديد السياسات والعمليات الأمنية الرئيسية التى تم تنفيذها وتشغيلها

	للتعامل مع مخاطر الأمن الإلكترونى للمنظمة، ويتضمن ذلك: (أ) منع الإختراقات الأمنية المقصودة وغير المقصودة. (ب) الإفصاح عن الإختراقات الأمنية وتحديدها وتطوير وسائل التعامل معها وعلاجها. (ج) إدارة القدرة على توفير عمليات مستمرة خلال حدوث أحداث أمنية أو تشغيلية أو بيئية.(د) الإفصاح عن الأحداث البيئية والتخفيف من حدتها وعلاجها وإستخدام النسخة الإحتياطية وإجراءات دعم النظام.(هـ) تحديد المعلومات السرية عند إستلامها أو إنشائها وتحديد فترة الإحتفاظ بها وكيفية التخلص منها بعد فترة الإحتفاظ.

ثانياً: معايير الرقابة (خدمات الثقة)

(الثقة، والاتاحة، ونزاهة المعالجة، والسرية، والخصوصية)

وضعت اللجنة التنفيذية لخدمات الضمان فى 2017 (ASEC) التابعة ل AICPA معايير الرقابة لإستخدامها فى عمليات التصديق أو الإستشارات لتقييم والإبلاغ عن الضوابط على أمن المعلومات والأنظمة أو توفرها أو تكاملها أو سريتها أو خصوصيتها .

تم تعديل هذا الإصدار من معايير خدمات الثقة من قبل AICPA ليشمل المطابقة والتغييرات اللازمة بسبب إصدار (**SOC**)([9]) جديد فى مارس 2020 لمعالجة مخاطر الأمن الإلكترونى .

ويقوم المراجع بفحص وتقرير فعالية الضوابط (المناسبة من التصميم وفعالية التشغيل) ذات الصلة بالثقة أو الاتاحة أو نزاهة معالجة النظام أو السرية أو الخصوصية للمعلومات التي تتم معالجتها بواسطة نظام ينتج ، أو توزيع المنتجات.

خلفية:

وضعت اللجنة التنفيذية لخدمات التوكيد (ASEC) مجموعة من المعايير (معايير خدمات الثقة) لاستخدامها عند تقييم ملاءمة التصميم والفعالية التشغيلية للضوابط ذات الصلة بأمن المعلومات والأنظمة أو توافرها أوتكاملها أومعالجتها، أوخصوصية المعلومات التي تتم معالجتها بواسطة الأنظمة في كيان أو قسم أو وحدة تشغيل كيان. بالإضافة إلى ذلك ، يمكن استخدام معايير خدمات الثقة عند تقييم التصميم والتشغيل لفعالية الضوابط ذات الصلة للثقة، والاتاحة، ونزاهة المعالجة، والسرية، والخصوصية.

([9]) System and Organization Controls

أولاً: معايير الثقة

تحتفظ المنشأة وتراقب وتقيم قدرة المعالجة الحالية واستخدام نظام العناصر الأساسية (البنية التحتية والبيانات والبرمجيات) لإدارة الطلب على وتمكين توجيه القدرة الإضافية للمساعدة في تحقيق أهدافها.

الخصائص المهمة المتعلقة بهذا المعيار:

A1.1: يصرح الكيان أو يصمم أو يطور أو يكتسب أو ينفذ أو يشغل أو يوافق أو يحافظ على ويراقب حماية البيئة، والبرامج ، وعمليات النسخ الاحتياطي للبيانات ، والبنية التحتية للاسترداد لتحقيق أهدافها.

A1.2: تختبر الجهة إجراءات خطة الاسترداد التي تدعم استرداد النظام لتحقيق أهدافها.

ثانياً: معايير الإتاحة

تعنى الاتاحة أن المعلومات والأنظمة متاحة للتشغيل والاستخدام لتلبية أهداف الكيان– وإمكانية الوصول إلى المعلومات التي تستخدمها أنظمة الكيان وكذلك المنتجات أو الخدمات المقدمة لعملائها. هدف الإتاحة في حد ذاته لا يحدد الحد الأدنى من مستوى الأداء المقبول ؛ ولايعالج وظائف النظام (الوظائف التي يؤديها النظام) أو قابلية الاستخدام (قدرة المستخدمين على تطبيق وظائف النظام على أداء مهام أو مشاكل محددة). ومع ذلك ، فإنه يتناول ما إذا كانت الأنظمة تشمل أم لا ضوابط لدعم إمكانية الوصول للتشغيل والمراقبة والصيانة.

ثالثاً: معايير السرية

1– يحدد الكيان المعلومات السرية ويحافظ عليها لتلبية أهداف الكيان ذات الصلة إلى السرية.

2– يتصرف الكيان في المعلومات السرية لتحقيق أهداف الكيان المتعلقة بالثقة.

رابعاً: معايير نزاهة المعالجات

يحصل الكيان على أو ينشئ ويستخدم ويبلغ المعلومات ذات الصلة والجودة فيما يتعلق بالأهداف المتعلقة بالمعالجة، بما في ذلك تعريفات بيانات المعالجة والمنتج والخدمة والمواصفات، لدعم استخدام المنتجات والخدمات.

PI1.1: يحدد المعلومات اللازمة لدعم استخدام سلعة أو منتج – من المعلومات التي يقدمها الكيان مطلوبة لاستخدام السلعة أو المنتج وفقًا لما يلي:

1– المعلومات المطلوبة متوفرة لمستخدم السلعة أو المنتج.

2- المعلومات المطلوبة قابلة للتحديد بوضوح.

3- التحقق من صحة المعلومات المطلوبة للتأكد من اكتمالها ودقتها.

PI1.2: ينفذ الكيان السياسات والإجراءات على مدخلات النظام، بما في ذلك الضوابط على الوفرة والدقة ، لينتج عنهما المنتجات والخدمات والتقارير لتلبية أهداف الكيان.

PI1.3: يقوم الكيان بتنفيذ السياسات والإجراءات على معالجة النظام للحصول على المنتجات وإعداد التقارير لتلبية أهداف الكيان.

PI1.4: ينفذ الكيان السياسات والإجراءات لإتاحة أو تسليم المخرجات بالكامل ، بشكل منظم ، وفي الوقت المناسب وفقًا للمواصفات لتلبية أهداف الجهة.

PI1.5: يقوم الكيان بتنفيذ السياسات والإجراءات لتخزين المدخلات والعناصر قيد المعالجة والمخرجات بشكل كامل ودقيق وفي الوقت المناسب وفقًا لمواصفات النظام لتلبية متطلبات الكيان.

خامساً: معايير الخصوصية:

P1.0: معايير الخصوصية المتعلقة بإشعار وتواصل الأهداف المتعلقة بالخصوصية.

P1.1: يقدم الكيان إشعارًا لموضوعات البيانات حول ممارسات الخصوصية الخاصة به لتلبية أهداف الكيان المتعلقة بالخصوصية .يتم تحديث الإشعار وإبلاغه لأصحاب البيانات في الوقت المناسب والتغييرات التي تطرأ على ممارسات خصوصية الكيان ، بما في ذلك التغييرات في استخدام المعلومات الشخصية ، إلى تلبية أهداف الكيان المتعلقة بالخصوصية.

P2.0: **معايير الخصوصية المتعلقة بالاختيار والموافقة**

P2.1: يقوم الكيان بإبلاغ الخيارات المتاحة فيما يتعلق بالتجميع والاستخدام والاحتفاظ والإفصاح والتخلص من المعلومات الشخصية لأصحاب البيانات، إن وجدت ، لكل اختيار .والموافقة الصريحة على جمع المعلومات الشخصية واستخدامها والاحتفاظ بها والكشف عنها والتخلص منها، ويتم الحصول عليها من أصحاب البيانات أو غيرهم من الأشخاص المصرح لهم ، إذا لزم الأمر. يتم الحصول على هذه الموافقة فقط للغرض المقصود من المعلومات لتلبية أهداف الكيان المتعلقة بالخصوصية. لتحديد الموافقة الضمنية على الجمع والاستخدام والاحتفاظ والإفصاح وتم توثيق التخلص من المعلومات الشخصية.

P3.0: **معايير الخصوصية المتعلقة بالمجموعة**

P3.1: *يتم جمع المعلومات الشخصية بما يتفق مع أهداف الكيان المتعلقة بالخصوصية.*

P3.2: للحصول على معلومات تتطلب موافقة صريحة ، يقوم الكيان بالإبلاغ عن الحاجة إلى مثل هذه الموافقة، بالإضافة إلى عواقب عدم تقديم الموافقة على طلب المعلومات الشخصية، ويحصل على الموافقة قبل جمع المعلومات لتحقيق أهداف الكيان فيما يتعلق بالخصوصية.

P4.0: **معايير الخصوصية المتعلقة بالإستخدام والإحتفاظ والتخلص.**

P4.1: يحدد الكيان استخدام المعلومات الشخصية للأغراض المحددة في أهداف الكيان المتعلقة بالخصوصية.

P4.2: يحتفظ الكيان بالمعلومات الشخصية المتوافقة مع أهداف الكيان المتعلقة بالخصوصية.

P4.3: يتصرف الكيان بشكل آمن في المعلومات الشخصية لتحقيق أهداف الكيان المتعلقة بالخصوصية.

P5.0: **معايير الخصوصية المتعلقة بالوصول.**

P5.1: يمنح الكيان البيانات المحددة والمصادق عليها القدرة على الوصول إلى البيانات المخزنة لكل منهم. والمعلومات الصوتية للمراجعة ، وعند الطلب ، وتوفر نسخًا مادية أو إلكترونية من ذلك في تشكيل موضوعات البيانات لتحقيق أهداف الكيان المتعلقة بالخصوصية .وإذا تم رفض الوصول، البيانات يتم إبلاغ الأشخاص بالرفض وسبب هذا الرفض، على النحو المطلوب، لتلبية متطلبات الكيان النصوص المتعلقة بالخصوصية.

P5.2: يقوم الكيان بتصحيح المعلومات الشخصية أو تعديلها أو إلحاقها بناءً على المعلومات المقدمة من موضوعات البيانات وتنقل هذه المعلومات إلى أطراف ثالثة، حسب الالتزام أو المطلوب، إلى تلبية أهداف الكيان المتعلقة بالخصوصية .إذا تم رفض طلب التصحيح ، يتم رفض موضوعات البيانات إبلاغه بالرفض وسببه لتحقيق أهداف الجهة المتعلقة بالخصوصية.

P6.0: **معايير الخصوصية المتعلقة بالإفشاء والإخطار.**

P6.1: يكشف الكيان عن المعلومات الشخصية لأطراف ثالثة بموافقة صريحة من أصحاب البيانات، ويتم الحصول على هذه الموافقة قبل الإفصاح لتلبية أهداف الكيان المتعلقة بالخصوصية.

P6.2: ينشئ الكيان ويحتفظ بسجل كامل ودقيق وفي الوقت المناسب لعمليات الإفصاح المصرح بها عن المعلومات الشخصية لتلبية أهداف الجهة المتعلقة بالخصوصية.

P6.3: يُنشئ الكيان ويحتفظ بسجل كامل ودقيق وفي الوقت المناسب للاكتشافات أو الإبلاغ عنها والإفصاحات الخاضعة للرقابة (بما في ذلك الخروقات) للمعلومات الشخصية لتحقيق أهداف الكيان المتعلقة بالخصوصية.

P6.4: يحصل الكيان على التزامات الخصوصية من البائعين والأطراف الثالثة الأخرى الذين لديهم حق الوصول إلى المعلومات الشخصية لتلبية أهداف الجهة المتعلقة بالخصوصية. يقوم الكيان بتقييم هؤلاء الأشخاص على أساس دوري وحسب الحاجة واتخاذ الإجراءات التصحيحية ، إذا لزم الأمر.

P6.5: يحصل الكيان على التزامات من البائعين والأطراف الثالثة الأخرى التى لها حق الوصول إلى المعلومات الشخصية وتشكيل لإخطار الكيان فى حالة الإفصاح الفعلى أوالمشتبه به غير المصرح به لكل المعلومات الصوتية. ويتم الإبلاغ عن هذه الإخطارات إلى الموظفين المناسبين ويتم التصرف بناءً عليها فى التوافق مع إجراءات الاستجابة للحوادث المعمول بها لتلبية أهداف الكيان المتعلقة.

P6.6: يقدم الكيان إخطاراً بالانتهاكات والحوادث لموضوعات البيانات والهيئات التنظيمية المتأثرة والآخرين لتحقيق أهداف الكيان المتعلقة بالخصوصية.

P6.7: يزود الكيان موضوعات البيانات بمحاسبة عن المعلومات الشخصية التي يحتفظ بها ويفصح عنها، والتأكد من المعلومات الشخصية لأصحاب البيانات، بناءً على طلب أصحاب البيانات، لتلبية إحتياجات الكيان الأهداف المتعلقة بالخصوصية.

P7.0: **معايير الخصوصية المتعلقة بالجودة**

P7.1: يجمع الكيان معلومات شخصية دقيقة وحديثة وكاملة وذات الصلة ويحافظ عليها لتحقيق أهداف الجهة المتعلقة بالخصوصية.

P8.0: **معايير الخصوصية المتعلقة بالمراقبة والإنفاذ.**

P8.1: ينفذ الكيان عملية لتلقي القرار ومعالجته وحلّه وإبلاغه–الرد على الاستفسارات والشكاوى والنزاعات من أصحاب البيانات وغيرهم ومراقبة بشكل دورى لتلبية أهداف الكيان المتعلقة بالخصوصية. والتصحيحات وغيرها ضرورية اتخاذ الإجراءات المتعلقة بأوجه القصور المحددة أو إتخاذها فى الوقت المناسب.

ملحق رقم (2)
الحالة التجريبية الأولى

الأستاذ الفاضل /.....

تحية طيبة وبعد..... ،،،

يقوم الباحث بإعداد بحث فى مجال أثر توكيد مراقب الحسابات على مزاعم الإدارة عن إدارة مخاطر الأمن الإلكترونى على قرار الاستثمار بالأسهم – دراسة تجريبية.

وتمثل الحالات المرفقة أهم أدوات البحث لإجراء الدراسة التجريبية.

ويقدر الباحث مسبقاً لكم حسن تعاونكم الفعال فى إثراء المعرفة المحاسبية، لذلك يأمل الباحث فى تعاونكم المثمر من خلال إبداء رأيكم على الاسئلة التى تتضمنها الحالات المرفقة، مع التأكيد، على أن إجاباتكم على هذه الأسئلة، سوف تحظى بالسرية الكاملة ولأغراض البحث العلمى فقط.

وتفضلوا بقبول فائق الإحترام،،،،

الباحث/

د/ هانى خليل فرج

أستاذ المحاسبة المساعد

كلية التجارة – جامعة الاسكندرية

البيانات الشخصية:

❖ **الوصف الوظيفى:**

.....

❖ **المؤهل:**

- **بكالوريوس**
- **ماجستير**
- **دكتوراه**
- **أخرى** .....

❖ **التخصص:**

- **محاسبة**
- **إدارة اعمال**
- **أخرى** .....

❖ **الشهادة المتخصصة فى المحاسبة:**

- **CMA**
- **CPA**
- **CFA**
- **لا يوجد**
- **اخرى** .....

❖ **عدد سنوات الخبرة:**

- **أقل من خمس سنوات**
- **من خمس إلى عشر سنوات**
- **أكثر من عشر سنوات**

مصطلحات فنية:

- **مخاطر الأمن الإلكترونى:** هى القدرة على تدمير أو تعطيل أو التهديد بتقديم الخدمات الأساسية أو استغلال الثغرات للسطو على المعلومات والأموال والتى تسبب خسائر مالية أو فقدان الشركة لسمعتها عند تعطل أحد أنظمة المعلومات بها.
- **جهود المنظمات الدولية لمواجهة مخاطر الأمن الإلكترونى:**

1- **مجمع المحاسبين القانونيين الأمريكىAICPA:** وضع عام 2017 إقتراح للتقرير عن إدارة مخاطر الأمن الإلكترونى وكيفية إفصاح الشركات عنها.

2- **لجنة البورصة الأمريكية SEC** : أصدرت عام 2018 دليلاً استرشادياً عن متطلبات الإفصاح عن إدارة مخاطر الأمن الإلكترونى.

- **الجهود المصرية لمواجهة مخاطر الأمن الإلكترونى:**

نص الدستور المصرى 2014 – مادة (31) على أن: أمن الفضاء المعلوماتى جزء أساسى من منظومة الإقتصاد والأمن القومى، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه على النحو الذى ينظمه القانون.

الحالة التجريبية:

بإفتراض أن إحدى شركات تكنولوجيا المعلومات ش. م. م. خاضعه لقانون 159 لسنه 1981 ومقيدة بالبورصة المصرية تواجه مخاطر أمن الكترونى، وتم الإفصاح عن إدارة مخاطر الأمن الإلكترونى ضمن الايضاحات المتممة للقوائم المالية مع تقرير مراقب الحسابات عن القوائم المالية السنوية الكاملة فقط. على النحو التالى:

القوائم المالية للشركة:

١ـ قائمة المركز المالى فى ٣١/ ١٢/ ٢٠٢٠ : القيمة بالالف جنيه

بيان	٢٠٢٠	٢٠١٩
الأصول:		
إجمالى الأصول غير المتداولة	٦٦٧٣٣٧٩١	٥٧٨٤٧٥٩١
إجمالى الأصول المتداولة	١٧٧٠٩٢٧٩	١٥٤٠٣٩٠٤
إجمالى الأصول	٨٤٤٤٣٠٧٠	٧٣٢٥١٤٩٥
الإلتزامات:		
إجمالى الإلتزامات غير المتداولة	١١٠٠٩٤٠٥	١١٥١٤٣٨٩
إجمالى الإلتزامات المتداولة	٣٤٦٩٩٩٨٥	٢٦٥١٥٩٦٩
إجمالى الإلتزامات	٤٥٧٠٩٣٩٠	٣٨٠٣٠٣٥٨
حقوق الملكية:		
رأس المال	١٧٠٧٠٧١٦	١٧٠٧٠٧١٦
إحتياطيات	٥٠٢٩٣١٧	٤٧٦٢٦٢٥
أرباح مرحلة	١٦٦١٧٦١٩	١٣٣٧١٩٩٣
صافى ربح العام	١٦٠٢٨	١٥٨٠٣
إجمالى حقوق الملكية	٣٨٧٣٣٦٨٠	٣٥٢٢١١٣٧
إجمالى الإلتزامات وحقوق الملكية	٨٤٤٤٣٠٧٠	٧٣٢٥١٤٩٥

٢ـ قائمة الدخل عن الفترة المنتهية فى ٣١/ ١٢/ ٢٠٢٠ : القيمة بالألف جنيه

بيان	٢٠٢٠	٢٠١٩
ايرادات النشاط	٣١٩١٢٣٦٦	٢٥٨٠٥٠٩٠
يخصم: تكاليف النشاط	٩٦٦٣٣٣٥	١٦٣٦١٨٣١
مجمل ربح النشاط	١٢٢٤٩٠٣١	٩٤٤٣٢٥٩
يضاف: ايرادات اخرى	٤٦٢١٠٣	٤٧٠٩٣٦
يخصم: مصروفات اخرى	٦٠٨٦٣٢٠	٤٤١٧٥٧٥
صافى الربح قبل الضريبة	٦٦٢٤٨١٤	٥٤٩٦٦٢٠
يخصم: الضريبة	١٧٦٧٢٨٢	١٠٩٠٧٣٠
صافى الربح بعد الضريبة	٤٨٥٧٥٣٢	٤٤٠٥٨٩٠
نصيب السهم من صافى الربح	٢.٣٥	٢.١٠
سعر السهم	١٢.٢٥	١١.٦٥

٣ـ قائمة التدفقات النقدية فى ٣١/ ١٢/ ٢٠٢٠ : القيمة بالالف جنيه

بيان	٢٠٢٠	٢٠١٩
صافى تدفقات نقدية من انشطة التشغيل	٨٢٩٧٣٢٠	٢٩٩١٣٧٢
صافى تدفقات نقدية من انشطة الاستثمار	(١١٠٩١٩٣٥)	(٥٢٦١٤٢٤)
صافى تدفقات نقدية من انشطة التمويل	٣٤١٨٩٧٣	٢٧٢٩٢٧١
صافى التغير فى النقدية	٦٢٤٣٥٨	٤٥٩٢١٩
رصيد نقدية اول الفترة	١٣١٢٥٨٥	٨٥٢١٧٢
رصيد نقدية اخر الفترة	١٩٣٦٩٤٣	١٣١١٣٩١

الإيضاحات المتممة:

- تم إعداد القوائم المالية المجمعة فى 31 ديسمبر 2020 طبقا لمعايير المحاسبة المصرية وفى ضوء القوانين واللوائح المصرية ذات العلاقة.
- أعدت القوائم المالية على أساس التكلفة التاريخية باستثناء بعض أنواع الإستثمارات المالية والتى يتم تقييمها بالقيمة العادلة وفقا لمعايير المحاسبة المصرية.
- تم عرض القوائم المالية بالجنيه المصرى والذى يمثل عملة التعامل للشركة.
- تتطلب إعداد القوائم المالية وفقا لمعايير المحاسبة المصرية قيام الإدارة بعمل تقديرات وإفتراضات والتى تؤثر على تطبيق السياسات المحاسبية وعلى قيم الأصول والإلتزامات والايرادات والمصروفات. ويتم مراجعة التقديرات والإفتراضات بشكل دورى مستمر.
- تدار أنشطة التشغيل الخاصة بالشركة عن طريق قطاعات تشغيلية على مستوى أنشطة الشركة ككل كأنشطة متكاملة وذلك على اساس طبيعة الخدمة المقدمة.

ويتم اعداد التقارير القطاعية وفق ثلاث قطاعات:

الأول: قطاع الاتصالات والكوابل البحرية والبنيه التحتية.

الثانى: قطاع خدمات الانترنت الثابت.

الثالث: قطاع خدمات التعهيد.

- **رأس مال الشركة:** راس المال المصدر والمدفوع بالكامل 17070716 الف جنيه مصرى مقسم لأسهم قيمة السهم الإسمية 10 جنيه مصرى.
- المخاطر التى تواجهها الشركة:
- **خطر الائتمان:** يتمثل فى خطر عدم وفاء أحد أطراف الأدوات المالية لالتزاماته، ويعرض الطرف الاخر لخسائر مالية، وينشأ هذا الخطر بصفة رئيسية من عملاء الشركه والمدينين الاخرين.
- **خطر السيولة:** يتمثل فى خطر عدم وفاء الشركة إلتزاماتها فى تاريخ استحقاقها.
- **خطر السوق:** يتمثل فى خطر التغيرات فى أسعار السوق مثل أسعار صرف العملات الأجنبية وسعر الفائدة وأسعار أدوات حقوق الملكية.
- **مخاطر الأمن الإلكترونى** : تتمثل فى أن الهجمات الالكترونية يمكن أن تؤدى الى تخفيض الايرادات أو زيادة المصروفات أو إلحاق الضرر بسمعة الشركة، ويوجد تطور للتهديدات الالكترونية بإستمرار وليس لدى الشركه حاليا القدرة على كشف بعض الثغرات الأمنية مما قد يؤدى إلى تعطيل أمان النظم مما قد يضعف قدرة الشركة على تقديم خدماتها للعملاء وحماية الخصوصية لديهم.

تقرير مراقب الحسابات عن القوائم المالية للشركة فى 2020/12/31

إلى السادة /مساهمى شركة (س)" شركة مساهمة مصرية"

راجعنا القوائم المالية للشركة (س) فى 2020/12/31 والمتمثلة فى ميزانية الشركة وكذا قائمة الدخل، وكذا قائمة التدفقات النقدية عن السنة المالية المنتهية فى ذلك التاريخ، وملخص للسياسات المحاسبية الهامة وغيرها من الإيضاحات المتممة للقوائم المالية.

مسئولية الإدارة عن القوائم المالية:

هذه القوائم المالية مسئولية إدارة الشركة، فالإدارة مسئولة عن إعداد وعرض القوائم المالية عرضاً عادلاً وواضحاً وفقا لمعايير المحاسبة المصرية وفى ضوء القوانين المصرية السارية. وتتضمن مسئولية الإدارة تصميم وتنفيذ والحفاظ على إجراءات رقابة داخلية ذات صلة بإعداد وعرض القوائم المالية عرضا عادلاً وواضحاً خالياً من أى تحريفات هامة ومؤثرة سواء ناتجة عن الغش أو الخطأ،

كما تتضمن هذه المسئولية اختيار السياسات المحاسبية الملائمة وتطبيقها وعمل التقديرات المحاسبية الملائمة للظروف.

مسئولية مراقب الحسابات :

تنحصر مسئوليتنا فى إبداء الرأى على هذه القوائم المالية بناءاً على مراجعتنا لها. وقد تمت مراجعتنا وفقا لمعايير المراجعة المصرية وفى ضوء القوانين المصرية السارية. وتتطلب هذه المعايير تخطيط وأداء المراجعة للحصول على تأكيد مناسب بأن القوائم المالية خالية من أية أخطاء هامة ومؤثرة.

وتتضمن أعمال المراجعة أداء إجراءات للحصول على أدلة مراجعة بشأن القيم والافصاحات فى القوائم المالية، وتعتمد الإجراءات التى تم اختيارها على الحكم الشخصى للمراقب ويشمل ذلك تقييم مخاطر التحريف الهام والمؤثر فى القوائم المالية سواء الناتج عن الغش أو الخطأ. وعند تقييم هذه المخاطر يضع المراقب فى إعتباره إجراءات الرقابة الداخلية ذات الصلة بقيام الوحدة بإعداد القوائم المالية والعرض العادل والواضح لها. وذلك لتصميم إجراءات مراجعة مناسبة للظروف ولكن ليس بغرض إبداء رأى على كفاءة الرقابة الداخلية فى الوحدة، وتشمل عملية المراجعة أيضا تقييم مدى ملاءمة السياسات المحاسبية والتقديرات المحاسبية الهامة التى أعدت بمعرفة الإدارة، وكذا سلامة العرض الذى قدمت به القوائم المالية. ونرى أن أدلة المراجعة التى قمنا بالحصول عليها كافية ومناسبة وتعد أساساً مناسباً لإبداء رأينا على القوائم المالية.

الرأى:

من رأينا أن القوائم المالية المشار إليها أعلاه تعبر بعدالة ووضوح ، فى جميع جوانبها الهامة، عن المركز المالى للشركة (س) فى 2020/12/31 وعن أدائها المالى عن السنة المالية المنتهية فى ذلك التاريخ، وذلك طبقا لمعايير المحاسبة المصرية وفى ضوء القوانين واللوائح المصرية ذات الصلة.

المتطلبات القانونية والتنظيمية الأخرى:

تمسك الشركة حسابات مالية منتظمة كل ما نص القانون ونظام الشركة على وجوب اثباته فيها وقد وجدت القوائم المالية متفقة مع ما هو وارد بتلك الحسابات. كما تطبق الشركة نظام تكاليف يفى بالغرض منه وقد تم جرد المخزون بمعرفة ادارة الشركة طبقاً للأصول المرعية.

البيانات الواردة بتقرير مجلس الادارة المعد وفقاً لمتطلبات رقم 159 لسنة 1981 ولائحته التنفيذية

متفقة ماهو وارد بدفاتر الشركة،وذلك فى الحدود التى تثبت بها مثل تلك البيانات بالدفاتر.

تاريخ التقرير: 2021/3/25 مراقب الحسابات: عبد الوهاب نصر – KPMG

❖ **<u>الأسئلة المطروحة على عينة المستثمرين:</u>**

Q1: هل توافق على أنك بحاجة لتقرير توكيد مراقب الحسابات عن توكيدات الإدارة على إدارة مخاطر الأمن الإلكترونى عند اتخاذك لقرار الاستثمار؟

أوافق تماما	أوافق بدرجة كبيرة	أوافق	لا أوافق إلى حد ما	لا أوافق تماما

Q2: إذا كان سعر الإقفال الفعلى لسهم الشركة فى يوم العمل التالى لتاريخ تقرير مراقب الحسابات هو:

26 مارس 2021 كان 12,25 جنيه.

فإن سعر الإقفال المتوقع لسهم الشركة بعد تقرير مراقب الحسابات فى 2022 فى ضوء المعلومات السابقة من وجهة نظركم سيكون: ..... جنيه.

الحالة التجريبية الثانية

إفترض فى الحالة السابقة مايلى:

1- أن إدارة الشركة أفصحت عن وجود نظام لإدارة مخاطر الأمن الإلكترونى .

2- الشركة كلفت مراقب حساباتها بإعداد تقرير عن التوكيد على إفصاح الإدارة عن إدارة مخاطر الأمن الإلكترونى .

3- أن تقرير التوكيد هذا كان كالتالى:

تقرير مراقب الحسابات عن إدارة مخاطر الأمن الإلكترونى لشركة (س) فى 2020/12/31 إلى السادة /مساهمى شركة (س) شركة مساهمة مصرية

<u>النطاق:</u>

لقد قمنا بفحص تأكيدات إدارة الشركة (س) الخاصة بإدارة مخاطر الأمن الإلكترونى، وبرنامج الإدارة خلال الفترة من 1 يناير 2020 ، إلى 31 ديسمبر 2020 ، وبناءً على المعايير المذكورة

أدناه. لقد قمنا أيضًا بفحص فعالية إجراءات الرقابة الداخلية ضمن هذا البرنامج لتحقيق أهداف الأمن الالكترونى للشركة بناءً على المعايير المذكورة أدناه.

المعايير المستخدمة لإعداد تأكيدات إدارة الشركة:

هى المعايير المستخدمة لتقييم ما إذا كانت إجراءات الرقابة الداخلية داخل برنامج إدارة مخاطر الأمن الإلكترونى للشركة فعالة لتحقيق أهداف الأمن الالكترونى للشركة وهي معايير الثقة والاتاحة والسرية ونزاهة المعالجة، والخصوصية .

ويمثل برنامج إدارة مخاطر الأمن الإلكترونى للشركة مجموعة السياسات والعمليات وإجراءات الرقابة المصممة لحماية المعلومات والأنظمة من الأحداث الأمنية التي قد تعرض تحقيق أهداف الأمن الالكترونى للشركة للخطر واكتشافها والتعامل معها والتخفيف من اثارها وعلاجها في الوقت المناسب ، ومحاولة منعها.

مسئوليات الإدارة:

إدارة الشركة (س) مسئولة عما يلى:

- تحديد أهداف الأمن الالكترونى للشركة.
- تصميم وتنفيذ وتشغيل برنامج إدارة مخاطر الأمن الإلكترونى للشركة ، بما في ذلك إجراءات الرقابة داخل هذا البرنامج ، لتحقيق أهداف الأمن الالكترونى للشركة.
- إعداد الوصف المصاحب لبرنامج إدارة مخاطر الأمن الإلكترونى للشركة.
- تقديم تأكيدات حول ما إذا كان وصف إدارة مخاطر الأمن الإلكترونى للشركة يتم وفقًا للمعايير المستخدمة لإعداد تأكيدات إدارة الشركة، وما إذا كان كانت إجراءات الرقابة داخل برنامج إدارة مخاطر الأمن الإلكترونى للشركة فعالة لتحقيق أهداف برنامج الأمن الالكترونى للشركة.

كما أنها تكون مسئولة عن:

(أ) اختيار وتحديد المعايير المستخدمة لإعداد تأكيدات إدارة الشركة ، ومعايير الرقابة على تأكيداتها.

و(ب) أن يكون لديها أساس معقول لتأكيداتها حول ما إذا كانت إجراءات الرقابة داخل الشركة وبرنامج إدارة مخاطر الأمن الإلكترونى فعالاً لتحقيق أهداف الأمن الالكترونى للشركة من خلال إجراء تقييم لفعالية تلك الإجراءات بناءً على معايير الرقابة المستخدمة. ووصف برنامج إدارة مخاطر الأمن الإلكترونى للشركة وتأكيدات الإدارة.

مسئوليات مراقب الحسابات:

وتنحصر مسئوليتنا فى إبداء الرأى ، بناءً على فحصنا ، حول ما إذا كان برنامج إدارة مخاطر الأمن الإلكترونى للشركة يقدم وفقًا للمعايير المستخدمة لإعداد تأكيدات إدارة الشركة، وما إذا كانت إجراءات الرقابة داخل هذا البرنامج فعالة لتحقيق أهداف الأمن الالكترونى للشركة على أساس معايير الرقابة.

ولقد تم إجراء فحصنا وفقًا لمعايير التوكيد الأمريكية. وتتطلب هذه المعايير أن نقوم بتخطيط وتنفيذ الفحص للحصول على توكيد معقول حول ما إذا كان برنامج إدارة مخاطر الأمن الإلكترونى للشركة ، فى جميع جوانبه الهامة، يتوافق مع المعايير المستخدمة لإعداد تأكيدات إدارة الشركة، وما إذا كانت إجراءات الرقابة داخل البرنامج فعالة لتحقيق أهداف الأمن الالكترونى للشركة بناءً على معايير الرقابة. ولقد شمل فحصنا:

- الحصول على فهم لأهداف الأمن الالكترونى للشركة، وبرنامج إدارة مخاطر الأمن الإلكترونى الخاصة بها.
- تقييم مخاطر ما إذا كان برنامج إدارة مخاطر الأمن الإلكترونى للشركة غير متوافق مع المعايير المستخدمة لإعداد تأكيدات إدارة الشركة ، وما إذا كانت إجراءات الرقابة داخل ذلك البرنامج لم تكن فعالة .
- القيام بإجراءات للحصول على أدلة حول ما إذا كان برنامج إدارة مخاطر الأمن الإلكترونى للشركة متوافق مع المعايير المستخدمة لإعداد تأكيدات إدارة الشركة ، وما إذا كانت إجراءات الرقابة داخل ذلك البرنامج فعالة .

ولقد تضمن فحصنا أيضًا بعض الإجراءات الأخرى التى رأيناها ضرورية في مثل هذه الظروف.

ونرى أن أدلة المراجعة التى قمنا بالحصول عليها كافية ومناسبة وتعد أساساً مناسباً لإبداء رأينا.

الحدود الملازمة:

هناك قيود ملازمة لفعالية أى هيكل للرقابة الداخلية، بما في ذلك احتمال حدوث خطأ بشري وتجاوز إجراءات الرقابة من جانب الإدارة. بسبب القيود المتأصلة فى برنامج إدارة مخاطر الأمن الإلكترونى ، وقد تحقق الشركة توكيداً معقولًا، وليس مطلقًا، أنه يتم منع جميع الأحداث الأمنية، وبالنسبة لأولئك الذين لم يتم منعهم ، يتم اكتشافهم فى الوقت المناسب.

وتتضمن أمثلة القيود الملازمة فى برنامج إدارة مخاطر الأمن الإلكترونى ما يلى:

- نقاط الضعف فى مكونات تكنولوجيا المعلومات نتيجة التصميم من قبل الشركة المصنعة لها أو المطورة لها.
- إجراءات الرقابة غير الفعالة لدى البائع أو الشريك التجارى.
- المهاجمون المستمرون مع الموارد لاستخدام الوسائل التقنية المتقدمة والاجتماعية المتطورة والتقنيات الهندسية التى تستهدف الشركة على وجه التحديد.

علاوة على ذلك، فإن توقعات أي تقييم للفعالية للفترات المستقبلية تخضع لمخاطر أنه قد تصبح إجراءات الرقابة غير كافية بسبب التغيرات في الظروف أو أن درجة الامتثال لها قد تتدهور فى السياسات أو الإجراءات.

الاستنتاج:

ومن رأينا أن برنامج إدارة مخاطر الأمن الإلكترونى للشركة (س) المشار إليه أعلاه متوافق ، فى جميع جوانبه الهامة، عن السنة المالية المنتهية فى 31 ديسمبر 2020، مع المعايير المستخدمة لإعداد تأكيدات إدارة الشركة. وأن إجراءات الرقابة داخل ذلك البرنامج فعالة لتحقيق أهداف الأمن الالكترونى للشركة بناءً على معايير الرقابة.

تاريخ التقرير: 2021/3/25 مراقب الحسابات: عبد الوهاب نصر – KPMG

❖ **الأسئلة المطروحة على عينة المستثمرين:**

Q1: هل توافق على أن تقرير توكيد مراقب الحسابات عن توكيدات الإدارة على إدارة مخاطر

الأمن الإلكترونى يؤثر على توقع سعر السهم؟

أوافق تماما	أوافق بدرجة كبيرة	أوافق	لا أوافق إلى حد ما	لا أوافق تماما

Q2: هل توافق على أن تقرير توكيد مراقب الحسابات عن توكيدات الإدارة على إدارة مخاطر الأمن الإلكترونى ذو أهمية لك عند اتخاذ قرار الاستثمار؟

أوافق تماما	أوافق بدرجة كبيرة	أوافق	لا أوافق إلى حد ما	لا أوافق تماما

Q3: هل توافق على أن الشركة التى توفر تقرير توكيد مراقب الحسابات سيكون لها الأولوية للاستثمار فى أسهمها مقارنة بالشركات المنافسة التى لاتوفر تقرير توكيد عن إدارة مخاطر الأمن الإلكترونى ؟

أوافق تماما	أوافق بدرجة كبيرة	أوافق	لا أوافق إلى حد ما	لا أوافق تماما

Q4: إذا كان سعر الإقفال الفعلى لسهم الشركة (س) فى يوم العمل التالى لتاريخ تقرير مراقب الحسابات هو:

26 مارس 2021 كان 12,25 جنيه.

فإن سعر الإقفال المتوقع لسهم الشركة بعد تقرير مراقب الحسابات فى 2022 فى ضوء المعلومات السابقة من وجهة نظركم سيكون: ..... جنيه.