AL KUT JOURNAL OF ECONOMIC AND ADMINISTRATIVE SCIENCES
Publisher: College of Economics and Management - Wasit University

تأثير مخاطر الأمن السيبراني في التقارير المالية وانعكاسها على مسؤولية مراقب الحسابات

محمد خزعل خشان عبدالله الزاملي [1] mabdullah@uowasit.edu.iq

أ.د. ستار جابر خلاوي الحجامي[2] Salradi@uowasit.edu.iq

جامعة واسط/ كلية الإدارة والاقتصاد

المستخلص

في ظل التطورات التكنولوجية المتسارعة، أصبحت مخاطر الأمن السيبراني من أكثر التحديات الرئيسة التي تواجه الوحدات الاقتصادية، حيث أخذت الهجمات الإلكترونية تهدد سلامة أنظمتها المحاسبية والمالية، وتعرض مواردها وبنيتها التحتية لمخاطر جسيمة، وتؤدي هذه التهديدات إلى تراجع ثقة مستخدمي التقارير المالية، نتيجة القلق المتزايد من فقدان الأصول المالية والبيانات الحساسة، في ظل التوسع المستمر في استخدام الأنظمة الذكية والأجهزة الإلكترونية، وما يرافقه من تصاعد في الجرائم السيبرانية، لذا يهدف هذا البحث إلى تحليل تأثير مخاطر الأمن السيبراني على جودة التقارير المالية، مع تسليط الضوء على العلاقة بين هذه المخاطر ومسؤولية مراقب الحسابات، ودوره في اكتشافها والحد منها، من خلال تطبيق إجراءات رقابية وتقنية متطورة تعزز أمن المعلومات المحاسبية وتضمن موثوقية التقارير المالية، ولتحقيق أهداف البحث تم استعمال منهجين المنهج الاستقرائي، في استعراض الجانب النظري للبحث عن طريق استقراء المصادر والأدبيات المتعلقة بموضوع البحث بغية التوصل إلى استنتاجات نظرية تدعم أراء الباحث، والمنهج الوصفي (التحليلي)، لدراسة وتحليل البيانات الاحصائية باستعمال برنامج الحزم الإحصائية للعلوم الاجتماعية (SPSS) التي تم الحصول عليها من خلال توظيف الاستبانة للحصول على أراء مراقبي الحسابات فيما يتعلق بالجانب العملي ليجري بعدها جمع أراء المجيبين وتحليلها للوصول الى نتائج التي ثبتت ان للأمن السيبراني دور فاعل في حماية بيانات الوحدة الاقتصادية من المخاطر السيبرانية، ويحسن من جودة التقارير المالية عبر ما يحققه من اظهار المعلومات بمصداقية وشفافية وبما يلائم احتياجات المستخدمين لغرض اتخاذهم القرارات المناسبة.

Abstract

In light of rapid technological developments, cyber security risks have become one of the most significant challenges facing economic entities, Cyber-attacks threaten the integrity of their accounting and financial systems, exposing their resources and infrastructure to serious risks, These threats lead to a decline in the confidence of financial report users, due to the

growing concern over the loss of financial assets and sensitive data, This is in light of the continued expansion in the use of smart systems and electronic devices, and the accompanying rise in cybercrimes. Therefore, this research aims to analyze the impact of cyber security risks on the quality of financial reports, highlighting the relationship between these risks and the auditor's responsibility, and their role in detecting and mitigating them through the implementation of advanced control and technical procedures that enhance the security of accounting information and ensure the reliability of financial reports, To achieve the research objectives, two approaches were used: the inductive approach, which reviewed the theoretical aspect of the research by extrapolating sources and literature related to the research topic with the aim of arriving at theoretical conclusions that support the researcher's views, and the descriptive (analytical) approach, which studied and analyzed the statistical data using the Statistical Package for the Social Sciences (SPSS) program, which was obtained through The questionnaire was used to obtain auditors' opinions on practical aspects, The respondents' opinions were then collected and analyzed to arrive at conclusions that demonstrated that cyber security plays an effective role in protecting economic unit data from cyber risks. It also improves the quality of financial reports by presenting information with credibility and transparency, in a manner that meets users' needs for appropriate decision-making.

المقدمة

شهدت السنوات الأخيرة تطورًا كبيراً في التكنولوجيا والاعتماد المتزايد على الأنظمة الرقمية في مختلف القطاعات، لذا يعدُّ الأمن السيبراني الوسيلة المثلى لحماية الأنظمة والشبكات والبرمجيات من الهجمات الإلكترونية، تلجأ الدول والمؤسسات والوحدات الاقتصادية والأفراد إلى هذه الإجراءات لحماية المعلومات الحساسة ومراكز البيانات والأنظمة الرقمية الأخرى من المخترقين الذين يسعون لتغييرها أو حذفها أو تدميرها أو ابتزاز أصحابها، مما جعل الأمن السيبراني قضية محورية تؤثر على المؤسسات والشركات والوحدات الاقتصادية، مع تزايد الهجمات الإلكترونية والاختراقات الأمنية، أصبح من الضروري دراسة تأثير مخاطر الأمن السيبراني على التقارير المالية، حيث يمكن أن تؤدي هذه المخاطر إلى خسائر مالية كبيرة، والتلاعب في البيانات المالية، وفقدان ثقة المستثمرين وأصحاب المصالح، إذ تلعب التقارير المالية دورًا أساسيًا في تقديم صورة شفافة عن الأداء المالي للمؤسسات، وتعتمد على دقة البيانات وسلامتها، ومع ذلك فإن التعرض للتهديدات السيبرانية قد يؤدي إلى تحريف المعلومات المالية، مما ينعكس على جودة التقارير المالية ومدى موثوقيتها ودقتها، وهنا تبرز مسؤولية مراقب الحسابات، الذي يُعد مسؤولًا عن ضمان نزاهة البيانات المالية والكشف عن أي مخاطر قد تؤثر على عدالة التقارير المالية، يسعى هذا البحث إلى دراسة تأثير مخاطر الأمن السيبراني على التقارير المالية، وتحليل انعكاساتها على مسؤولية مراقب الحسابات، وذلك من خلال استعراض التحديات التي تواجه مراقبي الحسابات في ظل التطور التكنولوجي، ودورهم في تقييم المخاطر السيبرانية واتخاذ الإجراءات المناسبة للحد منها، كما يهدف البحث إلى تقديم توصيات لتعزيز دور مراقبي الحسابات في مواجهة هذه المخاطر، وتحقيق مستوى أعلى من الشفافية والمصداقية في التقارير المالية. ولتحقيق اهداف البحث قد قسم هذا البحث على اربعة

محاور، تضمن **المحور الاول**: منهجية البحث، وتناول **المحور الثاني:** الاطار النظري للبحث، في حين تناول **المحور الثالث**: الجانب التطبيقي للبحث، أما **المحور الرابع**: يمثل أهم ما توصل إلية البحث من استنتاجات وتوصيات.

المحور الاول: منهجية البحث:-

1- مشكلة البحث:-

بعد أن شهد العالم انفتاحًا في وسائل الاتصال الرقمي بين الوحدات الاقتصادية، أصبحت المعلومات متاحة على شبكات الإنترنت ويمكن الوصول إليها من أي جهة تحاول الدخول إلى قاعدة بيانات الوحدة الاقتصادية، لذا من الطبيعي أن تواجه الوحدة الاقتصادية بين الحين والآخر بعض الهجمات الإلكترونية التي تعرضها ومواردها للمخاطر، مما يؤدي إلى انخفاض حجم الثقة لدى المستخدمين نتيجة فقدان أموالهم، ومن هنا تتبلور مشكلة البحث في التساؤل الآتي: **كيف تؤثر مخاطر الامن السيبراني في التقارير المالية وهل تنعكس على مسؤولية مراقب الحسابات ؟** من خلال السؤال الرئيسي يمكن صياغة عدة أسئلة فرعية:-

1. هل تؤثر مخاطر الأمن السيبراني على التقارير المالية من حيث الإدارة والمسؤوليات وانعكاس ذلك على مسؤولية مراقب الحسابات؟
2. هل تؤثر مخاطر الأمن السيبراني على التقارير المالية من حيث الحماية وحفظ البيانات المالية وانعكاس ذلك على مسؤولية مراقب الحسابات ؟
3. هل تؤثر مخاطر الأمن السيبراني على التقارير المالية من حيث مراقبة الأنظمة والشبكات وانعكاس ذلك على مسؤولية مراقب الحسابات ؟
4. هل تؤثر مخاطر الأمن السيبراني على التقارير المالية من حيث القوانين والتشريعات وانعكاس ذلك على مسؤولية مراقب الحسابات ؟
5. هل تؤثر مخاطر الأمن السيبراني على التقارير المالية من حيث البعد الاقتصادي والاجتماعي والسياسي وانعكاس ذلك على مسؤولية مراقب الحسابات ؟

2- أهمية البحث :-

تتلخص أهمية البحث بالآتي:-

أن أهمية البحث ناتجة من أهمية مخاطر الأمن السيبراني والمعلومات الرقمية التي تولد نوع من عدم التأكد بالنسبة لمراقب الحسابات وهو غير متخصص بهكذا مواضيع قد تؤثر على البيانات المالية وبالنتيجة تؤثر على التقرير الذي يقوم بأعداده ، ويعد الأمن السيبراني ذو أهمية للأنظمة المرتبطة في الشبكات وتكنولوجيا المعلومات فالالتزام بتطبيق الأمن السيبراني يضمن الحماية على المعلومات من أي خطر أو تهديد قد تواجه نتيجة وجود خطر على الأنظمة وشبكات تكنولوجيا المعلومات ان وجود معلومات محمية بعيدة عن الغش والاحتيال والتلاعب هو هدف كل وحدة اقتصادية.

3- أهداف البحث:-

وفقا لمشكلة البحث والتساؤلات المطروحة فأن البحث يهدف الى تحقيق عدة أهداف التي يمكن بيانها بحسب الآتي:-

1. بيان تأثير مخاطر الأمن السيبراني في التقارير المالية وانعكاسها على مسؤولية مراقب الحسابات.
2. توضيح مفهوم ومخاطر الأمن السيبراني في حماية المعلومات والبيانات المالية .
3. مدى فاعلية تأثير الأمن السيبراني في خلق جدار صد فعال للمحافظة علي التقارير المالية للحد من منع حالات الاختراقات والمخاطر الالكترونية عبر شبكة الانترنيت .
4. التوصل الى تحديد مسؤولية مراقب من مخاطر الأمن السيبراني في ظل عدم التأكد.

4- فرضيات البحث:-

بناءاً على مشكلة البحث يمكن صياغة الفرضية الرئيسة الآتية:-

أولاً: عدم وجود تأثير ذات دلالة معنوية عند مستوى معنويه (0.05) لمخاطر الامن السيبراني على التقارير المالية.

ثانياً: عدم وجود تأثير ذات دلالة معنوية عند مستوى معنويه (0.05) لمخاطر الامن السيبراني على مسؤولية مراقب الحسابات.

من خلال الفرضيتين الرئيستين يمكن صياغة الفرضيات الفرعية الآتية:-

1. عدم وجود تأثير ذات دلالة معنوية عند مستوى معنويه (0.05) لمخاطر الامن السيبراني من حيث الادوار والمسؤوليات على التقارير المالية وانعكاسها على مسؤولية مراقب الحسابات.
2. عدم وجود تأثير ذات دلالة معنوية عند مستوى معنويه (0.05) لمخاطر الامن السيبراني من حيث الحماية وحفظ البيانات المالية على التقارير المالية وانعكاسها على مسؤولية مراقب الحسابات.
3. عدم وجود تأثير ذات دلالة معنوية عند مستوى معنويه (0.05) لمخاطر الامن السيبراني من حيث مراقبة الانظمة والشبكات وتطويرها على التقارير المالية وانعكاسها على مسؤولية مراقب الحسابات.
4. عدم وجود تأثير ذات دلالة معنوية عند مستوى معنويه(0.05) لإدارة الوحدة الاقتصادية للمخاطر السيبرانية من حيث القوانين والتشريعات على التقارير المالية وانعكاسها على مسؤولية مراقب الحسابات.
5. عدم وجود تأثير ذات دلالة معنوية عند مستوى معنويه (0.05) لمخاطر الامن السيبرانية من ناحية البعد الاقتصادي والاجتماعي والسياسي على التقارير المالية وانعكاسها على مسؤولية مراقب الحسابات.

المحور الثاني: الأطار النظري للبحث

1- نبذه تأريخيه عن نشأة الامن السيبراني :-

نشأ الامن السيبراني في اواخر فترة السبعينات من القرن الماضي كاستجابة للتحديات المتعلقة بالآمن المعلوماتي وحماية البيانات، إذ شهد هذا المجال نمواً كبيراً خلال هذه الفترة بسبب التطورات التكنولوجية المتسارعة والاعتماد المتزايد على التقنيات الرقمية في جميع مناحي الحياة، و كانت بداياته الأولى عند استخدام أجهزة الكمبيوتر واتصالها بالإنترنت إذ ظهرت تهديدات ومحاولات للوصول إلى الملفات والوثائق المهمة التي كان من الضروري أن يكون لدى

الوحدة الاقتصادية خطة دفاع قوية لمنع الوصول والاختراق والبحث والتوسع التدريجي في السبعينيات بدأت التكنولوجيا تتحدث عن ظهور أمن الشبكات، كان بوب توماس هو أول من درس أمن الشبكات (Kamiya et al, 2018: 22)، إذ يمكن القول إن مخاطر الأمن السيبراني ظهرت منذ بداية عصر الإنترنت والحوسبة الرقمية وتطورت بشكل متسارع مع تطور هذه التقنيات وانتشارها على نطاق واسع نتيجة التطور السريع للتكنولوجيا، الاعتماد المتزايد عليها، ظهور تهديدات معقدة، والنقص في الوعي والمهارات الأمنية اللازمة، هذه العوامل سهلت الوصول إلى البيانات والأنظمة الحساسة وزادت من احتمالية حدوث هجمات سيبرانية ناجحة وبسبب دخول خدمة استخدام الانترنت في كثير من المجالات وازدياد المستخدمين للعديد من المواقع الالكترونية (الشورة، 2020: 22).

2- مفهوم الأمن السيبرانى:-

يشير مفهوم الأمن السيبراني إلى الإجراءات والموارد المستعملة لضمان سلامة البرامج والأنظمة المتصلة بالأمن السيبراني من الأحداث غير القانونية (Al shamsi, 2019: 9)، ويرتبط ارتباطاً وثيقاً بأمن المعلومات، إذ أنَّ الوصول إلى أمن المعلومات أو بثها أو حتى مجرد الاطلاع عليها هو ما يسبب في غالب الاحيان عمليات الاختراق للشبكات، وان الحديث عن الأمن السيبراني يستدعى تعريف الخطر وهو التهديدات التي يتعرض له النظام بالإضافة إلى نقاط الضعف أو الثغراتالتي تعتريه، ثم اتخاذ الإجراءات الأمنية المفروض اتخاذها لدفع الخطر(المري، 2020: 964)،

إذ يعد مفهوم الامن السيبراني من المفاهيم التي لاقت اهتماماً كبيراً في الآونة الأخيرة نظراً لظهور تقنيات تكنولوجية جديدة، واستخدامها بشكل واقع في كافة المنشآت، وقد عرف بأنه عبارة عن مجموع من الإجراءات التقنية والإدارية تشمل العمليات والآليات التي يتم اتخاذها لمنع أي تدخل غير مقصود أو غير مصرح به بالتجسس أو الاختراق لاستخدام أو سوء الاستغلال للمعلومات والبيانات الإلكترونية الموجودة على نظم الاتصالات والمعلومات، كما يتضمن تأمين وحماية كاملة لسرية وخصوصية البيانات الشخصية للمواطنين، كما يشمل ضمان حماية واستمرارية عمل معدات الحاسب الآلي ونظم المعلومات والاتصالات والخدمات من أي تغيير أو تلف (Raigen, 2014: 15)، ويعد الوسيلة المثلى لحماية الأنظمة والشبكات والبرمجيات من الهجمات الإلكترونية، تلجأ الدول والمؤسسات والوحدات الاقتصادية والأفراد إلى الأمن السيبراني لحماية المعلومات الحساسة ومراكز البيانات والأنظمة الرقمية الأخرى من المخترقين الذين يسعون لتغييرها أو حذفها أو تدميرها أو ابتزاز أصحابها (Eaton, 2019: 4)، وقد عرف الأمن السيبراني بأنه " مجموعة من السياسات والعمليات والإجراءات الرقابية المصممة لحماية المعلومات والأنظمة الإلكترونية من الحوادث الأمنية التي تهدد أمن الوحدة الاقتصادية السيبراني وتعرضها لمخاطر عدم تحقيق أهدافها، تساعد هذه الإجراءات في اكتشاف الهجمات الأمنية والاستجابة لها وتخفيف آثارها، وتساعد أيضًا في التخلص بسرعة من الآثار السلبية التي تنتج عن الهجمات التي لا يمكن منعها (Jayakumar, 2020: 17)، وعرف أيضاً هو " عملية حماية المعلومات من خلال معالجة التهديدات التي تتعرض لهذه المعلومات التي يتم معالجتها وتخزينها ونقلها عبر أنظمة المعلومات المتداخلة بين الشبكات، ويشمل جميع المجالات الاقتصادية والاجتماعية والسياسية والقانونية في جميع المجتمعات المعاصرة" (اميرهم، 2022: 337).

3- أهداف الأمن السيبراني:-

يمكـن تحديد أهـم أهداف الأمـن السيبراني على الــنحو الآتي: (Haapamak & Sihvoneni, 2019:809) :-

أ. ضمان السرية حيث يتم التأكد من أن الأفراد الذين لديهم الصلاحية فقط يمكنهم الوصول إلى المعلومات وتغييرها أو إدارتها.

ب. ضمان النزاهة حيث يتم التأكد من أن الأشخاص أو العمليات المصرح لهم فقط هم الذين يمكنهم إجراء أي تغييرات في النظام.

ت. توفير نظام ومعلومات يتم إدارتها بواسطة النظام ومشغليه، مما يضمن أن الكيانات المرخص لها فقط يمكنها الوصول إلى المعلومات أو الموارد المخزنة أو المستعملة في البنية التحتية للمؤسسات.

4- المفاهيم المرتبطة بالأمن السيبراني:-

هناك العديد من المفاهيم والمصطلحات الأخرى المرتبطة بالأمن السيبراني، التي من أهمها:-

أ- أمن المعلومات: يعرف أمن المعلومات بأنه نظام حماية المعلومات الرقمية ويمكن من خلاله تشفير البيانات، وتوفير الشبكات والبنية التحتية التي تحتوي على معلومات شخصية، ومعلومات مالية، وبيانات خاصة بالوحدات الاقتصادية، وتكون كلها محمية بشكل مكثف ضد أي اختراقات (عبد الجواد، 2020: 388)

ب- الفضاء السيبراني: عرفته الوكالة الفرنسية لأمن أنظمة الإعلام "(ANSSSI)" وهي وكالة حكومية مكلفة بالدفاع السيبراني الفرنسي - بأنه: فضاء التواصل المشكل من خلال ربط البنى العالمية لمعدات المعالجة الآلية للمعطيات الرقمية، فهو بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية، مكوّن من مجموعة من الأجهزة الرقمية وأنظمة الشبكات والبرمجيات و المستخدمين سواء مشغلين أم مستعملين، كما أن هناك من عرف الفضاء السيبراني بوصفه الذراع الرابعة للجيوش الحديثة (السيد, 2024: 526)، وبذلك فالفضاء السيبراني هو فضاء افتراضي يضم العديد من المجتمعات الموزعة على نحو غير متساو باستعمال بيئة تقنية الإنترنت في المقام الأول، حيث يستفيد المواطنون والمؤسسات من تكنولوجيا المعلومات والاتصالات في تفاعلاتهم من الشبكة المترابطة من البنى التحتية لتكنولوجيا المعلومات، التي تشمل الإنترنت وشبكات الاتصالات السلكية واللاسلكية والنظم الحاسوبية والمعالجات المدمجة وأجهزة التحكم (Bicak et al., 2015: 56).

ت- الجريمة السيبرانية: مجموعة الأفعال والأعمال غير القانونية التي تتم عبر معدات أو أجهزة إلكترونية أو شبكة الإنترنت، وهي ذلك النوع من الجرائم التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها، فهي الجريمة المتصلة باستعمال الكمبيوتر، أي تصرف غير قانوني، يرتكب باستعمال تقنيات المعلومات والاتصالات، بقصد السيطرة على نظام الوحدة الاقتصادية الإلكتروني (Catota et al., 2019: 18).

ث- الهجمات السيبرانية: يمكن تعريفها بأنها فعلا يقوض من قدرات ووظائف شبكة الكمبيوتر لغرض قومي أو سياسي من خلال استغلال نقطة ضعف معينة تمكن المهاجم من التلاعب بالنظام (Waxman, 2011: 423).

ج- الردع السيبراني: يعرف بأنه يشير إلى منع الأعمال الضارة التي تستهدف الأصول الوطنية في المجال الفضائي والأصول التي تدعم العمليات الفضائية (بوغراره، 2018: 107).

5- ابعاد الامن السيبراني:-

يتعلق الأمن السيبراني بمجالات سياسية وعسكرية واقتصادية وقانونية واجتماعية مختلفة؛ بهدف تحقيق نظام أمن متكامل يحمي الأمن القومي للدولة ويحافظ على حقوق وحريات المواطنين الشخصية من أي هجمات أو تهديدات سيبرانية محتملة، يمكن توضيح ذلك عن طريق (المرداس، 2023: 11):

أ. البعد العسكري: يكمن أهمية الأمن السيبراني في هذا البعد في تقليل خطورة الهجمات السيبرانية والاختراقات التي تؤدي إلى نشوب الحروب والصراعات المسلحة، كما يساعد في تبادل المعلومات الهامة بين المؤسسات العسكرية بشكل إلكتروني.

ب. البعد الاقتصادي: أصبحت الإنترنت أساسًا للتجارة والمال والاقتصاد، وتستعمل الحواسيب في إدارة وتطوير الصناعات وتنشيط الاقتصاد، وأصبح الجميع متصلًا عبر شبكات الكمبيوتر، مما يستدعي الحديث عن أهمية تحقيق الأمن السيبراني في المجال الاقتصادي.

ت. البعد السياسي: تعتمد الجوانب السياسية للأمن السيبراني على حماية نظام الدولة السياسي وهويتها، حيث يمكن استخدام التكنولوجيا في نشر معلومات وبيانات قد تؤدي إلى تعكير استقرار الدول والحكومات، حيث يصل بسرعة هائلة إلى أكبر عدد من المواطنين بغض النظر عن صحة البيانات والمعلومات المنشورة.

ث. البعد الاجتماعي: يعدُّ الإنترنت مكانًا مفتوحًا للجميع، حيث يمكن لجميع المستخدمين الاستفادة من البنية التحتية والخدمات المتاحة لهم دون تحمل المخاطر الأمنية، وهنا يجب التأكيد على أهمية التوعية بأخلاقيات الأمن السيبراني.

ج. البعد القانوني: الثورة في مجال المعلومات والاتصالات والتكنولوجيا أدت بشكل عام إلى ظهور أنماط جديدة من السلوك الذي يعدُّ مخالفًا ويترتب عليه المسؤولية الجنائية والمدنية، ونتيجة لذلك تم تطبيق إطار تشريعي حديث لمكافحة جرائم الفضاء السيبراني لمواكبة هذا التطور السريع في التكنولوجيا وتعزيز التعاون الدولي في مكافحة الجريمة السيبرانية، ومن أهم الممارسات القانونية في مجال الأمن السيبراني هو ضمان بعض الحقوق في هذا المجال، مثل حق الوصول إلى الشبكة المعلوماتية وحق إنشاء المدونات الإلكترونية وحق ملكية البرامج الثقافية.

5- انواع المخاطر السيبرانية

ومن ابرز انواع الهجمات السيبرانية ما يأتي (Shahimi & Mahzan, 2018: 1257):-

أ- مخاطر سيبرانية تتعلق بالحفاظ على السرية: تحدث عندما يتم الكشف عن المعلومات السرية داخل المؤسسة لجهة ثالثة، مثل حدوث اختراق للبيانات.

ب- مخاطر سيبرانية تتعلق بالنزاهة: تتعلق بسوء استخدام الأنظمة، مثل الاحتيال.

ت- مخاطر سيبرانية تتعلق بالاستمرارية: تتمثل في تعطل أو توقف العمليات التجارية.

ومن بين أهم المخاطر التي تشكل خطرًا على الأمن السيبراني هي اختراق الأنظمة والوصول إلى البيانات والمعلومات دون إذن والتجسس على الاتصالات والتلاعب بها وتعديلها وتدميرها، ويعدُّ ذلك انتهاكًا للحريات الشخصية والحقوق، بالإضافة إلى الجرائم العادية التي يتم تنفيذها عبر الإنترنت مثل السرقة والغش والترويج لأنشطة غير قانونية، وبالآتي فإن المخاطر التي يمكن أن تواجهها الشبكة العنكبوتية تهدف إلى تدمير الأهداف السياسية والعسكرية والاقتصادية وغيرها (الشورة، 2020: 15).

6- مفهوم الإطار المفاهيمي للتقارير المالية:-

تعد التقارير المالية وسيلة فعالة للتواصل ونقل المعلومات المتعلقة بأنشطة الوحدة الاقتصادية بشكل دوري إلى المستويات الإدارية المختلفة، وتمكنها من اتخاذ القرارات المناسبة وفرض الرقابة على العمليات والموجودات، إذ تلعب دورًا حيويًا في تصحيح الأخطاء في الوقت المناسب، وتمكن الإدارة من متابعة العمليات وتقييم كفاءتها وتحسينها ومعالجة نقاط الضعف من خلال تحليل التقارير المالية (احمد، 2019: 172)، وتؤدي التقارير المالية دورًا هامًا في المجال المحاسبي إذ تُعنى بتوفير بيانات ومعلومات عالية الجودة تتميز بالدقة والوضوح والشفافية، تساهم في تقليل عدم التماثل في المعلومات بين الإدارة وصانعي القرارات من المستثمرين وتمكن للوحدة الاقتصادية من الوصول إلى جميع المعلومات اللازمة لاتخاذ القرارات(عبادي، 2023: 37)، إذ انها تقدم نتائج نظم المعلومات المحاسبية للمستخدمين المختلفين داخل الوحدة الاقتصادية وخارجها، وتعمل كحلقة وصل بينهم وبين نظام المعلومات المحاسبية ، وأن الوظيفة الأساس لنظام المعلومات المحاسبية هي توفير المعلومات اللازمة لمستخدميها عند اتخاذ قراراتهم أو إصدار أحكامهم، وهذا يفرض على النظام مسؤولية تقديم المعلومات المناسبة لمختلف متخذي القرارات بشكل كافٍ من حيث الملاءمة والموضوعية (عبدالله واخرون، 2017: 56)، ويمكن القول إن التقارير المالية هي مستندات تعرض جميع الأنشطة المالية وغير المالية التي تقوم بها الوحدة الاقتصادية خلال فترة زمنية محددة على أن تكون هذه الأنشطة قد أُعدت وفقًا لمبادئ المحاسبة المعترف بها والمقبولة عمومًا وأن يتم اعتمادها من قبل مراقب حسابات خارجي مستقل، بغرض توفير معلومات موثوقة تساعد المستخدمين الداخليين والخارجيين على فهم نتائج أعمال الوحدة الاقتصادية ومواردها والتزاماتها وقدرتها على تحقيق الأرباح خلال فترة زمنية معينة، فضلاً عن دعم الإدارة في تحقيق أهدافها ووضع الخطط المستقبلية وتقييم مستوى الأداء في الوحدة الاقتصادية، وتحتوي التقارير المالية على معلومات تتعلق بالأنشطة المالية والاجتماعية والبيئية التي تقوم بها الوحدة الاقتصادية بشرط أن تكون هذه المعلومات قد أُعدت وفقًا لمبادئ المحاسبة المقبولة قبولا عاما (وفقان، 2021: 36)، إذ ان التقارير المالية هي " المخرجات النهائية لنظم المحاسبة، حيث تُعرض بالأرقام والكلمات لنتائج الأنشطة الاقتصادية في نهاية الفترة المالية، وتعتبر الوسيلة الأساسية لنقل المعلومات الناتجة عن معالجة بيانات أنشطة الوحدة الاقتصادية إلى الأطراف المعنية، كما يمكن أن تتضمن التقارير معلومات مالية وغير مالية (ابو العلا، 2018: 273)، إذ تُعرّف التقارير المالية على أنها المخرجات الناتجة عن العمليات المحاسبية في أي كيان اقتصادي، حيث تُعد حصيلة لمعالجات محاسبية تُجرى على البيانات المرتبطة بالأحداث والأنشطة التي تقوم بها الوحدة الاقتصادية، بهدف عرضها بطريقة شاملة وموجزة لأصحاب المصلحة، بما يمكّنهم من استخدامها في دعم قراراتهم المختلفة (عبد الوهاب والصيرفي، 2020: 7)، أن التقارير المالية تلعب دورًا حيويًا في الجانب المحاسبي وإدارة الأعمال لاتخاذ القرارات الاستراتيجية؛ إذ تساعد التقارير المالية في تقييم أداء الوحدة الاقتصادية وقياس كفاءة أعمالها المالية، تتيح للمديرين فهم أداء الوحدة الاقتصادية في عدة مجالات مثل المبيعات والأرباح والتكاليف والديون، تمكن التقارير المالية من تحليل الاتجاهات والتطورات المالية في مجال الأعمال، وايضاً يمكن للوحة الاقتصادية تحليل بياناتها المالية لفهم توجهات السوق والمخاطر المحتملة وفرص النمو، تعتبر هذه المعلومات قيمة حيث تساعد على اتخاذ قرارات استراتيجية مستنيرة، توفر التقارير المالية معلومات للمساهمين الرئيسيين مثل المستثمرين والبنوك والمؤسسات المالية، تعتبر هذه المعلومات مهمة جدًا لاتخاذ قرارات الاستثمار وتقييم المخاطر المالية وغير المالية (192-191 .(Mohammad et al, 2013:

7- العلاقة بين التقارير المالية ومخاطرالأمن السيبراني:-

إذ تسعى معظم الوحدات الاقتصادية إلى فهم طبيعة الجريمة السيبرانية، التي تمثل تهديدًا رئيسيًا يجب مكافحته، واستنادًا إلى مبدأ "لا جريمة ولا عقاب دون نص" قامت العديد من الدول بوضع نصوص قانونية تحدد حجم هذه الجرائم، تشمل هذه الجرائم مجموعة واسعة من الأنشطة غير المشروعة التي تستعمل أجهزة الكمبيوتر والشبكات كوسيلة لتنفيذ الجريمة أو كهدف لها، بدءًا من اختراق الأنظمة المعلوماتية وأنظمة الاتصالات وصـولًا إلى الهجمات التي تـؤدي إلـى تعطيل النظـام المحاسبي (ساسوي، 2020: 23)، إذ قامت الاتفاقية الأوروبية لمكافحة الجريمة السيبرانية بتقسيم الجرائم السيبرانية إلى مجموعتين (Eling & Wirfs, 2016: 25):-

المجموعة الأولى تصنف الجريمة السيبرانية على أنها أي تصرف غير قانوني موجه بواسطة الوسائل الإلكترونية نحو أمن أنظمة المعلومات والبيانات التي تحتويها، بينما المجموعة الثانية تعرف الجريمة السيبرانية على أنها أي تصرف غير قانوني يتم باستعمال الأنظمة المعلوماتية أو بطريقة مرتبطة بها، وتشمل جرائم مثل الحيازة غير القانونية أو عرض المعلومات عبر الشبكات او الأنظمة المعلوماتية.

لذا فإن تأثير مخاطر الأمن السيبراني على دقة وموثوقية التقارير المالية يشمل العديد من الأضرار، مثل التلاعب في البيانات المالية الذي يؤدي إلى تقارير غير دقيقة، وفقدان بيانات مالية هامة تؤثر على إعداد التقارير المالية، كما قد ينجم عن هذه المخاطر انخفاض الثقة لدى المستثمرين والمساهمين، مما يضر بسمعة الوحدة الاقتصادية ويؤثر على التقارير المالية والمعلومات المحاسبية، وفي حال تعرضت الوحدة الاقتصادية لمخاطر سيبرانية، قد تتكبد تكاليف باهظة لاستعادة البيانات المالية وإصلاح الأضرار، مما يؤثر سلبًا على ربحيتها ويضعف من قدرتها على المنافسة مع الوحدات الاقتصادية الاخرى ، لذا تحتاج الوحدات الاقتصادية الى وضع اجراءات وسياسات تنظيمية تهدف الى تقليل المخاطر السيبرانية وضمان استمرارية التنافس (Ghelani ,2022: 16)، وإن المعلومـات المحـاسبية تحتـاج إلـى حمـايـة قـويـة مـن مخـاطـر الأمـن السيبراني، ويـتـطلـب ذلـك اتخـاذ الإجـراءات الآتيـة (Barry, 2022: 12):

1. تتطلب التقارير المالية إجراءات أمنية قوية وشاملة، و إشراك خبراء المحاسبة في المناقشات حول الأمن السيبراني للأعمال .
2. أهمية حماية البيانات المالية واستخدام الإجراءات المحاسبية لمنع الخسائر المالية والتنظيمية والتكنولوجية والعلاقات العامة والاستثمارية كجزء من استراتيجيات الأمن السيبراني.
3. التركيز على المفاهيم العامة للحماية من تهديدات الأمن السيبراني، مثل ثغرات الاختراق، بغض النظر عن نوع الهجوم السيبراني .
4. التنبؤ بالحجم المحتمل لحوادث الأمن السيبراني والاحتمالات المرتبطة بها.
5. ضمان كفاية التدابير الوقائية للحد من مخاطر الجرائم الإلكترونية والتعامل مع العواقب المرتبطة بها.

أن من أهم الارشادات التي اصدرتها هيئـة الأوراق الماليـة والبورصـات الأمريكيـة (SEC) بشـأن مخـاطر الأمـن السيبراني وكالاتي (الرشيدي ، 2019: 20):-

1- طبيعة مخاطر الأمن السيبراني على المستثمرين و التقارير المالية والوحدات الاقتصادية ، وطرق وأهداف الحوادث السيبرانية، والآثار السلبية لوقوعها، وأهمية الإفصاح للمستفيدين، والتأثير على الوحدة الاقتصادية وعملياتها ومركزها المالي.

2- الإفصاح عن مخاطر الأمن السيبراني، و التركيز على حقيقة أنه على الرغم من عدم ذكر متطلبات الإفصاح عن مخاطر وحوادث الأمن السيبراني التي تتعرض لها الوحدة الاقتصادية في مجال عملها، إلا أنه قد تكون الوحدات الاقتصادية ملزمة بالإفصاح عن هذه المخاطر والحوادث والمتمثلة بالاتي:

أ. أهمية سياسات وإجراءات الرقابة المؤسسية المتعلقة بحوادث ومخاطر الأمن السيبراني.

ب. منع المعاملات الداخلية من قبل الأطراف ذات الصلة في حال وقوع حوادث ومخاطر تتعلق بالأمن السيبراني.

3- مراجعة لقواعد الإفصاح عن مشاكل مخاطر الأمن السيبراني المتمثلة بالاتي (Ealon et al , 2019: 3):-

أ. الأهمية النسبية يجب على الوحدات الاقتصادية مراعاة أهمية مخاطر وحوادث الأمن السيب راني عند إعداد التقارير السنوية والإفصاح عن المعلومات المتعلقة بمخاطر وتهديدات الأمن السيبراني في التقارير الدورية بشكل مناسب ومستمر.

ب. قد تكون هناك معلومات جوهرية تتعلق بالأمن السيبراني منها الحوادث السابقة للأمن السيبراني ومدى حدتها وتكرارها.

4. خصائص عمليات الوحدة الاقتصادية التي قد تزيد من حدوث المخاطر السيبرانية الأساسية، والمتمثلة بالاتي (Hilary et al.,2016: 11) :

أ- قد يتعرض النظام المالي للوحدة لاختراقات تؤدي إلى تسريب معلومات حساسة تتعلق بالميزانية، والإيرادات، والمصروفات، والتوقعات المستقبلية، هذا التسريب لا يؤثر فقط على سمعة الوحدة الاقتصادية، بل قد يؤدي أيضاً إلى تلاعب في التقارير المالية، فعلى سبيل المثال قد يتلاعب المخترقون في القوائم المالية من خلال تعديل الأرقام أو تزييف المعاملات المالية لتغطية الأنشطة غير القانونية.

ب- قد تؤدي إلى تعطيل الأنظمة المالية، مما يعيق قدرة الوحدات الاقتصادية على إعداد تقارير مالية دقيقة في الوقت المحدد، ويمكن ان تؤدي هذه الهجمات إلى فقدان البيانات المالية المهمة، مما يضر بصحة القرارات المالية التي تعتمد عليها الإدارات العليا في اتخاذ القرارات.

ت- عندما تتعرض أنظمة الوحدة الاقتصادية لتهديدات سيبرانية، فإن ذلك يمكن أن يخلق بيئة من الشكوك بشأن مصداقية البيانات المالية المقدمة لان المصداقية والشفافية من المبادئ الأساسية في إعداد التقارير المالية ، على سبيل المثال في حالة حدوث هجوم سيبراني ناجح على قسم المالي للوحدة الاقتصادية، قد يصعب على الأطراف المعنية مثل المستثمرين والمراجعين الماليين أن يثقوا في التقارير المالية للوحدة.

8- نشأة مهنة مراقب الحسابات:-

تُعد مهنة مراقبة الحسابات مهنة قديمة نشأت مع سعي الإنسان لتلبية احتياجاته من خلال التفاعل مع الطبيعة، ومع ذلك لم تتطور المحاسبة بشكل منظم إلا بعد اختراع الأرقام واستعمال النقود كوحدة قياس لقيم السلع والخدمات المتبادلة، وقد ظهرت مهنة مراقبة الحسابات لاحقًا مع تطور النظام المحاسبي، حيث أصبحت تستند الى مجموعة من المبادئ والقواعد التي تهدف إلى فحص الحسابات والتأكد من مدى صحتها والتزامها بالإجراءات المحاسبية المعتمدة عند تسجيل

المعاملات المالية، (Basu,2016: 6)، فإذا نظرنا إلى تأثير مهنة مراقب الحسابات عبر التاريخ، نجد أنها نشأت نتيجة الحاجة الملحة لها من قبل رؤساء القبائل أو الجماعات أو أصحاب الأموال والحكومات لمراقبة أولئك الذين يقومون بعمليات التحصيل والدفع والاحتفاظ بالمواد في المخازن نيابة عنهم، تعود جذور المراقبة إلى حكومات المصريين القدماء واليونانيين الذين استعملوا المراقبين للتحقق من صحة الحسابات العامة، حيث كان مراقب الحسابات في ذلك الوقت يراجع الحسابات شفهياً او المدونة بوسائل بدائية، بهدف التأكد من خلوها من أي تلاعبات أو أخطاء مما يضمن دقة المعلومات المالية وصحتها (قرفي، 2020: 3-4).

كما توضح المادة (7) من نظام ممارسة مهنة مراقبة وتدقيق الحسابات رقم (3) لعام 1999، أن مفهوم مراقب الحسابات هو شخص مؤهل يُمنح ترخيصًا لممارسة المهنة بعد أن يقوم بأعمال التدقيق ويخضع لتدريب لمدة سنتين في ديوان الرقابة المالية الاتحادي أو مكتب مراقبة الحسابات، أي أن مراقب الحسابات "هو شخص خبير متخصص في المحاسبة والتدقيق، مؤهل قانونياً، يتم التعاقد معه من قبل جهة مختصة قانونياً للقيام بأعمال التدقيق و المراقبة الخارجية وغيرها من المهام المنصوص عليها في القانون لفترة زمنية محددة، بهدف الوصول إلى رأي فني محايد حول مدى دقة القوائم المالية وصدق تمثيلها للمركز المالي الحقيقي للوحدة الاقتصادية".

9- المسؤولية المهنية لمراقب الحسابات

أولاً- يتمثل القسم الأول من مسؤوليات مراقب الحسابات بالمسؤولية القانونية، وتتكون من ثلاثة أنواع وهي كالآتي:

1. مسؤولية المدقق تجاه الزبون:-

تُعرف هذه المسؤولية بالمسؤولية التعاقدية نظرًا للعلاقة التعاقدية بين المدقق والزبون، حيث تحدد هذه العلاقة واجبات وحقوق المدقق كما هو موضح في نص العقد المبرم بين الطرفين، تنشأ مسؤولية المدقق تجاه زبونه بسبب عدم تنفيذه للعقد الموقع وعدم الالتزام بجميع بنوده بشكل كامل، إذ يعدُّ العقد المبرم بين المدقق والزبون أساسًا لأي مسؤولية تجاهه ، يتحمل المدقق دائمًا المسؤولية أمام زبونه عن الأضرار الناتجة عن إهماله إذا لم يلتزم بمعيار العناية المهنية أثناء عملية التدقيق أوالخدمات ذات الصلة (القاضي واخرون، 2017: 137-138)، وتنقسم دعاوى الإهمال إلى فئتين (ديري، 2010: 88):

أ- حالات يتحمل فيها الزبون خسائر نتيجة اعتماده على الكشوفات المالية المدققة من قبل المدقق.

ب- حالات يفشل فيها المدقق في تقديم خدماته بعناية واجبة، حيث رفعت الدعوى عليه لخرقه عقد الاتفاق مع الزبون.

2. مسؤولية المدقق تجاه الطرف الثالث:-

يشير الطرف الثالث هنا إلى جميع الجهات التي تعتمد على القوائم المالية المدققة وما تحتويه من معلومات محاسبية لاتخاذ قرارات اقتصادية مختلفة، باستثناء الزبون الذي وقع العقد مع المدقق، ومن بين هذه الأطراف، يوجد المساهمون الحاليون والمحتملون، والبائعون، والمصارف، والدائنون المختلفون (سواد، 2009: 140-141)، إذ تنشأ هذه المسؤولية نتيجة عدم الوفاء بالتزامات ناتجة عن سياسات اجتماعية، وقد عدل مفهوم الطرف الثالث لاحقًا ليشمل أولئك الذين يمكن للمدقق توقع استعمالهم للقوائم المالية التي قام بتدقيقها بشكل معقول، وبالآتي يكون المدقق مسؤولًا عن إهماله العادي تجاه طرف ثالث معروف له، أو تجاه طرف آخر كان ينبغي على المدقق توقع احتمال استخدامه للقوائم المالية (Basu, 2016: 253).

3. المسؤولية الجنائية:-

تتحقق هذه المسؤولية عندما يقوم المدقق بعمل يعدُّ موجهًا ضد المجتمع، ويحدث ذلك في حالة وقوع ضرر يؤثر على المجتمع بشكل عام (دحدوح والقاضي،2012: 19-20)، ومن بين الأضرارالمتعلقة بالمجتمع، ما يلي (الحسيني،2011: 14):

أ- تسجيل بيانات كاذبة في أي تقرير أو حسابات أو وثيقة أعدها أثناء أداء عمله.

ب- إعداد تقرير يتعارض مع الحقيقة أو التصديق على وقائع غير صحيحة في أي وثيقة تتعلق بممارسة المهنة.

ت- جريمة التستر على حقائق معينة.

كما تنص المادة (218) من قانون الشركات العراقي رقم (21) لسنة 1997 المعدل على معاقبة أي موظف في شركة يقدم، وهو على علم، بيانات أو معلومات غير صحيحة إلى جهة رسمية بشأن نشاط الشركة أو حصص أعضائها أو كيفية توزيع الأرباح، بالحبس لمدة لا تزيد عن سنة، وبغرامة لا تتجاوز اثني عشر مليون دينار، أو بالعقوبتين معاً.

ثانيا- القسم الثاني من مسؤوليات مراقب الحسابات فتمثَّل بالمسؤولية المهنية (الأخلاقية):-

تشير المسؤولية المهنية إلى المجال القانوني الذي يتضمن واجبات المدققين في التصرف بطريقة مهنية أثناء أداء مهامهم، والامتثال للقوانين واللوائح التي تنظم المهنة، وتجنب تضارب المصالح، ووضع مصالح الزبائن فوق مصالحهم الشخصية، إذ إن مفهوم العناية المهنية يتطلب مستوى عالٍ من الأداء يجب تحقيقه حيث يدخل هذا المستوى ضمن ما يعرف بالمسؤولية المهنية أو الأخلاقية، و يتجلى هذا النوع من المسؤولية في المبادئ الأخلاقية التي يجب أن يتحلى بها المدقق، مما يسهم في تعزيز الثقة بشكل عام فيما يقوم به من أعمال، وما يقدمه من آراء، وما يعده من تقارير، لأنه يتوقف تقييم الجهات التي تستعمل التقارير المنشورة لمراقب الحسابات على مدى قدرته على تحمل المسؤولية، وذلك كلما زادت كفاءة المراقب في تحمل مسؤوليته، زاد احترام هذه الجهات له (الحسيني، 2011: 16)، إذ يقوم مراقب الحسابات بتقديم خبرته وخدماته للشركات والوحدات الاقتصادية وكذلك للأطراف الثالثة التي تستعمل القوائم المالية وكل من له علاقة بها ، بالإضافة إلى حياده واستقلاله في أداء مهنته، من العناصر الأساسية لمراقب الحسابات، حيث أن أداءه لمهامه يسهم في خدمة العديد من الجهات التي تعتمد على نتائج أعماله (Johnstone, 2013: 18 -16).

10- <u>أهمية معايير التدقيق وعلاقتها بمسؤولية مراقب الحسابات:-</u>

تطورت مهنة مراقب الحسابات بشكل عام وظهرت العديد من الهيئات والمنظمات تهتم بهذه المهنة، ومن بين الأمور التي ركزت عليها هذه المنظمات هو إصدار معايير للأداء المهني في شكل نشرات، التي تعتبر بمثابة إطار شامل للممارسة المهنية الجيدة، كما تستعمل هذه المعايير كأداة لتحديد المسؤولية وتنظيم العلاقة بين أعضاء المهنة أنفسهم، وعلاقتهم بزبائنهم وجميع أفراد المجتمع الذين يستفيدون من خدماتهم، لذا أخذت تتجلى أهمية معايير المراقبة في أنها تحدد مسؤولية مراقب الحسابات نتيجة قيامه بعملية المراقبة أو الفحص واصبح من الضروري أن يتم الفحص وفقًا لتلك المعايير حتى لا يتحمل مراقب الحسابات أي مسؤولية في حال ظهور غش أو تلاعب لاحقًا، كما تُعتبر معايير التدقيق ذات أهمية كبيرة بالنسبة للأطراف التي تستعمل التقارير والمعلومات المحاسبية مثل البنوك والموردين والجهات الضريبية والحكومة وغيرها، لأنها توضح لهم كيفية إجراء الفحص الذي قام به مراقب الحسابات، والمسؤولية التي يتحملها، مما يحدد درجة الاعتماد على القوائم المالية، (حكيمة ، 2009: 24- 25)، إذ تعد معايير التدقيق مجموعة من القواعد والإرشادات تساعد مراقب الحسابات على أداء عمل مهني منظم ومتسق عالمياً، وضعت من قبل

الجهات المنظمة للمهنة وهي تمثل مستويات للأداء المهني و تهدف إلى ضمان تقديم تقارير مالية ومهنية عالية الجودة، تتسم بالشفافية، والدقة، والكفاءة، وتحدد نوعاً من الإطار الذي يعمل مراقب الحسابات ضمنه (Arens, 2013: 85-90) ، وتحقيقا لذلك فقد حدد المعهد الامريكي للمحاسبين القانونيين، اربعة معايير تعتبر كإرشادات عامة لأعداد التقرير، على النحو الآتي (حكيمة مناعي، 2009: 69):

1. أشار المعيار (ISA700) الى صدق وعدالة عرض القوائم المالية: يتطلب هذا المعيار من مراقب الحسابات أن يوضح في تقريره ما إذا كانت القوائم المالية قد تم إعدادها وعرضها وفقًا للمبادئ المحاسبية المقبولة عمومًا، من الناحية المهنية يعدُّ مراقب الحسابات أن المبادئ المحاسبية المقبولة عمومًا هي المعيار الذي يقيس صدق وعدالة عرض القوائم المالية، مما يعني أن التزام الإدارة بهذه المبادئ أثناء إعداد وعرض القوائم المالية يضمن دقتها، أي أنها ستكون خالية من التحريفات الجوهرية، سواء كانت تلك التحريفات متعمدة او غير متعمدة.

2. أشار المعيار (ISA710) الى ظروف عدم الثبات في تطبيق مقياس صدق القوائم المالية: يتطلب هذا المعيار من مراقب الحسابات الإشارة في تقريره إلى الحالات التي لم تلتزم فيها الإدارة بالثبات في تطبيق المبادئ المحاسبية في الفترة المحاسبية الحالية مقارنة بالفترة السابقة، ويهدف معيار الثبات إلى تحقيق هدفين رئيسيين هما:

أ. ضمان قابلية المقارنة: التأكد من أن قابلية القوائم المالية للمقارنة بين الفترات المختلفة لم تتأثر تأثيراً جوهريا.

ب. ضمان الإفصاح عند التغيير: في حال وجود تأثير جوهري على قابلية المقارنة بسبب تغيير في المبادئ

المحاسبية، يتعين على مراقب الحسابات الإشارة إلى ذلك بشكل مناسب في تقريره.

3. أشار المعيار (ISA706) الى مدى كفاية الإفصاح في القوائم المالية: ينص المعيار الثالث من معايير التقرير على ضرورة أن تكون المعلومات المقدمة في القوائم المالية كافية بشكل معقول، وإذا توصل المراقب إلى أن الإفصاح الوارد في القوائم المالية غير كافٍ أو غير متوافق مع المبادئ المحاسبية المتعارف عليها، فإنه لا يملك سلطة إجبار الإدارة على تعديل القوائم، ومع ذلك يحق لمراقب الحسابات التحكم في محتوى تقريره من خلال تضمينه الإفصاح الضروري في حال تجاهل القوائم المالية للوحدة الاقتصادية هذا الإفصاح أو إذا تضمنت معلومات غير دقيقة.

4. أشار المعيار (ISA705) الى وحدة الرأي: يشترط هذا المعيار أن يتضمن تقرير مراقب الحسابات رأياً فنياً محايداً وشاملاً حول القوائم المالية ككل، التي تشمل قائمة المركز المالي، قائمة الدخل، وقائمة التدفقات النقدية، ولا يحق له إبداء الرأي حول بعض القوائم فقط دون الأخرى، وفي حال تعذر إبداء الرأي، يجب عليه توضيح الأسباب بوضوح في تقريره.

12- العلاقة بين مسؤولية مراقب الحسابات ومخاطر الامن السيبراني:-

هناك علاقة وثيقة بين مخاطر الأمن السيبراني ومسؤولية مراقب الحسابات، حيث تطورت هذه المسؤولية بشكل كبير مع التقدم التكنولوجي السريع وزيادة الهجمات السيبرانية التي تؤثر بشكل مباشر على العمليات المحاسبية والمالية، أصبح من الضروري أن يقوم مراقب الحسابات بإجراء تقييم شامل لضمان أن الوحدة الاقتصادية تمتلك نظام حماية فعالًا وشاملًا، والتأكد من كفاية الإجراءات والسياسات المتبعة لإدارة مخاطر الأمن السيبراني، بهدف حماية التقارير المالية من التهديدات الرقمية التي تمثل خطرًا مباشرًا على صحة ودقة البيانات المحاسبية، هذه التهديدات قد تؤدي إلى تعطل الأنظمة المالية، مما ينعكس سلبًا على دقة وموثوقية التقارير المالية (Cheong et al, 2021: 79).

إذ تمثل العلاقة بين مخاطر الأمن السيبراني والتقارير المالية للوحدات الاقتصادية علاقة معقدة ومتعددة الأبعاد، وتزداد أهميتها مع تزايد الاعتماد على التقنيات الرقمية في العمليات المالية، نظرًا لأن التقارير المالية تعتمد على البيانات

المعلوماتية، فإن أي تهديدات أو مخاطر تتعلق بالأمن السيبراني قد تؤثر سلباً على دقة وموثوقية التقارير المالية (Ghelani, 2022: 25)، تنشأ مخاطر الأمن السيبراني من مصادر متعددة، مثل الهجمات الإلكترونية، وانتهاكات البيانات، والبرامج الضارة، والتهديدات الداخلية، وضعف تدابير الأمن السيب راني، هذه المخاطر قد تؤثر بشكل كبير على المركز المالي للوحدة الاقتصادية من خلال التسبب في خسائر مالية لها، لذلك يتعين على مراقب الحسابات التعاون مع خبراء الأمن السيبراني لتحديد وتحليل المخاطر المحتملة، خاصة أن هذه المواضيع تتجاوز نطاق خبرته ، لكونها أصبحت تشكل تأثيرًا كبيرًا على البيانات المالية للوحدة الاقتصادية التي يقوم بتدقيقها، هذا التعاون يمكن أن يساهم في تعزيز قدرة مراقب الحسابات على تقديم تقارير دقيقة وموثوقة تعكس الوضع المالي الحقيقي للوحدة الاقتصادية، إذ يعد مراقب الحسابات العنصر الاساسي في الحفاظ على نزاهة وشفافية العمليات المالية المحاسبية، ويمكن ان يتم الاعتماد عليه كوظيفة استشارية تعمل على تحسين إدارة المخاطر، وفي عصرنا هذا وبعد حدوث الهجمات السيبرانية التي أخذت تشكل تهديدا متزايداً لحياة وامن الانسان والتحول الكبير إلى الاعتماد على العمل عبر الإنترنت وعقد الاجتماعات وتبادل المعلومات والملفات عن بعد (Eling, 2016: 36).

المحور الثالث: أختبار الفرضيات وتحليل النتائج:-

تم وضع استمارة الاستبيان واستعمال مقياس ليكارت الخماسي لمعرفة مدى تأثير مخاطر الامن السيبراني في التقارير المالية وانعكاسها على مسؤولية مرقب الحسابات، لذا تم وضع الفروض اللازمة للدراسة .

الفرضيتان الرئيسيتان:-

أولاً: عدم وجود تأثير ذات دلالة معنوية عند مستوى معنويه (0.05) لمخاطر الامن السيبراني على التقارير المالية.

ثانياً : عدم وجود تأثير ذات دلالة معنوية عند مستوى معنويه (0.05) لمخاطر الامن السيبراني على مسؤولية مراقب الحسابات.

فرضية العدم الاولى : عدم وجود تأثير ذات دلالة معنوية عند مستوى معنويه (0.05) لمخاطر الامن السيبراني من حيث الادوار والمسؤوليات على التقارير المالية وانعكاسها على مسؤولية مراقب الحسابات.

فرضية العدم الثانية : عدم وجود تأثير ذات دلالة معنوية عند مستوى معنويه (0.05) لمخاطر الامن السيبراني من حيث الحماية وحفظ البيانات المالية على التقارير المالية وانعكاسها على مسؤولية مراقب الحسابات.

فرضية العدم الثالثة : عدم وجود تأثير ذات دلالة معنوية عند مستوى معنويه (0.05) لمخاطر الامن السيبراني من حيث مراقبة الانظمة والشبكات وتطويرها على التقارير المالية وانعكاسها على مسؤولية مراقب الحسابات.

فرضية العدم الرابعة :عدم وجود تأثير ذات دلالة معنوية عند مستوى معنويه (0.05) لإدارة الوحدة الاقتصادية للمخاطر السيبرانية من حيث القوانين والتشريعات على التقارير المالية وانعكاسها على مسؤولية مراقب الحسابات.

فرضية العدم الخامسة : عدم وجود تأثير ذات دلالة معنوية عند مستوى معنويه (0.05) لمخاطر الامن السيبرانية من ناحية البعد الاقتصادي والاجتماعي والسياسي على التقارير المالية وانعكاسها على مسؤولية مراقب الحسابات.

ولتحديد اجابات أفراد عينة الدراسة تجاه الفقرات الرئيسة التي ضمنتها أداة الدراسة تم استخدام الوسط الحسابي والانحراف المعياي والنسبة المئوية واتجاه العينة للفقرات على الشكل الآتي:

- ❖ المتوسط الحسابي: (Mean)، وذلك لمعرفة مدى ارتفاع أو انخفاض اجابات أفراد الدراسة عن كل فقرة من فقرات الدراسة .
- ❖ الانحراف المعياري: (Standard Deviation)، للتعرف على مدى انحراف اجابات أفراد الدراسة لكل فقرة من فقرات الدراسة عن متوسطها الحسابي، ويلاحظ أن الانحراف المعياري يوضح التشتت في اجابات أفراد الدراسة للفقرات إلى جانب المحاور الرئيسية، فكلما اقتربت قيمته من الصفر كلما تركزت الاجابات وانخفض تشتتها بين المقياس .
- ❖ حساب المدى، وهو في هذه الحالة عبارة عن (أكبر قيمة- أصغر قيمة)، في مقياس ليكارت الخماسي أي (5-1=4).
- ❖ ثم يتم تحديد طول الخلية عن طريق (قسمة المدى على عدد حقول مقياس ليكارت)، أي (5/4=0.80).
- ❖ بعد ذلك يتم إضافة طول الخلية إلى أصغر قيمة في المقياس وهي(1) للحصول على الحد الأعلى للخلية (لا اتفق بشدة) وهكذا حتى نصل إلى الحدود الدنيا والعليا لكل خلية وستكون كالآتي:

- أي وسط تقع قيمته بين (1 - 1,79)، يصنف في الخلية (لا اتفق بشدة). وهو ما يشكل نسبة أقل من (20%).
- أي وسط حسابي قيمته أكبر من (1.80 وحتى 2.59) يصنف في الخلية (لا اتفق). وهو ما يشكل نسبة ما بين (21%) إلى (40%).
- أي وسط قيمته أكبر من (2.60 وحتى 3.39) يصنف في خلية (محايد). وهو ما يشكل نسبة ما بين (41%) الى (60%).
- أي وسط حسابي قيمته أكبر من (3.40 وحتى 4.19) يصنف في الخلية (اتفق). وهو ما يشكل نسبة ما بين (61%) إلى (80%).
- أي وسط حسابي قيمته أكبر من (4.20 وحتى 5) يصنف في الخلية (اتفق بشدة). وهو ما يشكل نسبة أكثر من (81%). كما موضح في الجدول (1).

الجدول رقم (1) بيان مقياس الاجابات.

الدرجة	1	2	3	4	5
التصنيف	لا اتفق بشدة	لا اتفق	محايد	اتفق	اتفق بشدة
المدى	1_1.79	1.80_2.59	2.60_3.39	3.40_4.19	4.20_5
النسبة	20%	40%	60%	80%	80_100%

المصدر: من اعداد الباحث بالاعتماد على برنامج (SPSS V 21).

دراسة تأثير مخاطر الامن السيبراني على التقارير المالية:

الفرضية الرئيسة : عدم وجود تأثير ذات دلالة معنوية عند مستوى معنويه (0.05) لمخاطر الامن السيبراني على التقارير المالية

لدراسة اثر ابعاد مخاطر الامن السيبراني على التقارير المالية لابد من وضع الفرض الملائم لها اذ تحتوي على خمسة متغيرات والمتمثلة بـ (x_1، x_2، x_3، x_4، x_5) وهي متغيرات مستقلة اما بالنسبة للمتغير التابع والمتمثل (التقارير المالية) ولدراسة الفرضية لابد من وضع الانموذج الملائم للبيانات والذي يمثل مشكلة الدراسة تمثيلا دقيقا ، فمن خلال

الجدول رقم (2) وبعد قياس التأثير واختيار الانموذج الافضل للبيانات تبين ان قيمة (0.891= R^2) والذي يعني (معامل تحديد افضل نموذج) اي ان المتغيرات المستقلة تفسر (89%) تؤثر في المتغير التابع (y) اي ان ما تبقى يعدُّ من الاخطاء العشوائية في اختيار الاجابة المحددة او يعزى الى اخطاء غير معروفة اذ بلغت قيمتها (11%) اما بالنسبة لقياس دور العلاقة بين المتغيرات فقد بلغت قيمة (R=0.943) وهذا يدل على ان العلاقة قوية ،اما بالنسبة لقيمة اختبار (F=21.450) التي تدرس مدى ملائمة خط انحدار البيانات وفرضيته العدم الخاصة بأنموذج الانحدار اذ بلغ مستوى المعنوية (0.000) وهو اقل من (0.05) مما يدل عدم وجود فروق معنوية وان النموذج يمثل الظاهرة المدروسة ثميلا دقيقا وان خط الانحدار يلائم البيانات المعطاة اي رفض فرضية العدم وقبول الفرضية البديلة اي بمعنى وجود تأثير لأبعاد مخاطر الامن السيبراني على التقارير المالية ، اما بالنسبة لمعامل (β) والذي يمثل تأثير كل متغير من المتغيرات المستقلة على المتغير التابع بمستوى معنوية اقل من (0.05) بعد اجتيازه اختبار (t)، اي بمعنى ان العلاقة طردية وذات تأثير معنوي، وكما موضح بالجدول (2):-

جدول (2)

معامل تحديد افضل انموذج ومقدار التأثير للمتغيرات المستقلة للفرضية الرئيسية

Model Summary						
Model		R	R Square[b]	Adjusted R Square	F	Sig.
1		.943[a]	.891	.890	21.450	.000
Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
1		**B**	**Std. Error**	**Beta**		
	x_1	.159	.117	.171	1.363	.006
	x_2	.071	.091	.072	.783	.036
	x_3	.304	.280	.327	1.084	.022
	x_4	.086	.116	.091	.742	.040
	x_5	.182	.121	.070	1.502	.037
a. Dependent Variable: y						
b. Linear Regression through the Origin						

- الجدول من اعداد الباحث باستعمال برنامج (SPSS v.21).

<u>اختبار فرضيات البحث الفرعية</u>:-

اولا : دراسة فرضية العدم الاولى :-

لدراسة اثر **مخاطر الامن السيبراني من حيث الادوار والمسؤوليات على التقارير المالية** لابد من وضع الفرض الملائم لها والذي ينص على (**عدم وجود تأثير ذات دلالة معنوية عند مستوى معنويه (0.05) لمخاطر الامن السيبراني**

من حيث الادوار والمسؤوليات على التقارير المالية وانعكاسها على مسؤولية مراقب الحسابات) اذ تحتوي على ثلاث متغيرات والمتمثلة بـ (x_1، x_2، x_3) وهي متغيرات مستقلة اما بالنسبة للمتغير التابع والمتمثل (التقارير المالية) ولدراسة الفرضية لابد من وضع الانموذج الملائم للبيانات والذي يمثل مشكلة الدراسة تمثيلا دقيقا ، فمن خلال الجدول رقم (3) وبعد قياس التأثير واختيار الانموذج الافضل للبيانات تبين ان قيمة **(R^2 =0.818)** والذي يعني (معامل تحديد افضل نموذج) اي ان المتغيرات المستقلة تفسر (81%) تؤثر في المتغير التابع **(y_1)** اي ان ما تبقى يعدُّ من الاخطاء العشوائية في اختيار الاجابة المحددة او يعزى الى اخطاء غير معروفة اذ بلغت قيمتها (9%) اما بالنسبة لقياس دور العلاقة بين المتغيرات فقد بلغت قيمة (R=0.904) وهذا يدل على ان العلاقة قوية ،اما بالنسبة لقيمة اختبار (F=22.902) التي تدرس مدى ملائمة خط انحدار البيانات وفرضيته العدم الخاصة بأنموذج الانحدار اذ بلغ مستوى المعنوية (0.000) وهو اقل من (0.05) مما يدل عدم وجود فروق معنوية وان النموذج يمثل الظاهرة المدروسة ثميلا دقيقا وان خط الانحدار يلائم البيانات المعطاة اي رفض فرضية العدم وقبول الفرضية البديلة اي بمعنى وجود اثر **مخاطر الامن السيبراني من حيث الادوار والمسؤوليات على التقارير المالية** ، اما بالنسبة لمعامل (β) والذي يمثل تأثير كل متغير من المتغيرات المستقلة على المتغير التابع بمستوى معنوية اقل من (0.05) بعد اجتيازه اختبار (t). اي بمعنى ان العلاقة طردية وذات تأثير معنوي، وكما موضح بالجدول (3):-

جدول (3)

معامل تحديد افضل انموذج ومقدار التأثير للمتغيرات المستقلة لفرضية العدم الاولى

Model Summary						
Model		R	R Square[b]	Adjusted R Square	F	Sig.
1		.904[a]	.818	.782	22.902	.000
Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
1		**B**	**Std. Error**	**Beta**		
	x_1	.243	.155	.262	1.564	.024
	x_2	.298	.173	.326	1.719	.002
	x_3	.239	.147	.254	1.633	.009
a. Dependent Variable: y_1						
b. Linear Regression through the Origin						

- المصدر: من أعداد الباحث بالاعتماد على برنامج (SPSS v21).

ثانيا : دراسة فرضية العدم الثانية :.

اما من خلال الجدول (4) وبعد قياس تأثير مخاطر الامن السيبراني من حيث الحماية وحفظ البيانات المالية على التقارير المالية لا بد من وضع الفرض الملائم والذي ينص على **(عدم وجود تأثير ذات دلالة معنوية عند مستوى**

معنويه (0.05) لمخاطر الامن السيبراني من حيث الحماية وحفظ البيانات المالية على التقارير المالية وانعكاسها على مسؤولية مراقب الحسابات) اذ تحتوي على ثلاث متغيرات والمتمثلة بـ **(x_1، x_2، x_3)** وهي متغيرات مستقلة اما بالنسبة للمتغير التابع والمتمثل (التقارير المالية) **(y_2)** ولدراسة الفرضية لابد من وضع الانموذج الملائم للبيانات والذي يمثل مشكلة الدراسة تمثيلا دقيقا ، فمن خلال الجدول رقم (4) واختيار الانموذج الافضل للبيانات تبين ان قيمة (0.864= R^2) والذي يعني (معامل تحديد افضل نموذج) اي ان المتغيرات المستقلة تفسر (86%) تؤثر في المتغير التابع **(y_2)** اي ان ما تبقى يعدُّ من الاخطاء العشوائية في اختيار الاجابة المحددة او يعزى الى اخطاء غير معروفة اذ بلغت قيمتها (14%) اما بالنسبة لقياس دور العلاقة بين المتغيرات فقد بلغت قيمة (R=0.929) وهذا يدل على ان العلاقة قوية ، اما بالنسبة لقيمة اختبار (F=32.345) التي تدرس مدى ملائمة خط انحدار البيانات وفرضيته العدم الخاصة بأنموذج الانحدار اذ بلغ مستوى المعنوية (0.000) وهو اقل من (0.05) مما يدل عدم وجود فروق معنوية وان النموذج يمثل الظاهرة المدروسة تمثيلا دقيقا وان خط الانحدار يلائم البيانات المعطاة اي رفض فرضية العدم وقبول الفرضية البديلة اي بمعنى وجود تأثير مخاطر الامن السيبراني من حيث الحماية وحفظ البيانات المالية على التقارير المالية ، اما بالنسبة لمعامل (β) والذي يمثل تأثير كل متغير من المتغيرات المستقلة على المتغير التابع بمستوى معنوية اقل من (0.05) بعد اجتيازه اختبار (t). اي بمعنى ان العلاقة طردية وذات تأثير معنوي، وكما موضح بالجدول (4):-

جدول (4)

معامل تحديد افضل انموذج ومقدار التأثير للمتغيرات المستقلة لفرضية العدم الثانية

Model Summary						
Model		R	R Square[b]	Adjusted R Square	F	Sig.
1		.929[a]	.864	.837	32.345	.000
Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
1	**X**	**B**	**Std. Error**	**Beta**		
	x_1	.070	.157	.065	.449	.006
	x_2	.242	.175	.226	1.380	.004
	x_3	.022	.148	.020	.150	.002
a. Dependent Variable: y_2						
b. Linear Regression through the Origin						

- المصدر: من أعداد الباحث بالاعتماد على برنامج (SPSS v21).

ثالثا : دراسة فرضية العدم الثالثة :-

اما من خلال الجدول (5) والذي يبين قياس اثر مخاطر الامن السيبراني من حيث مراقبة الانظمة والشبكات وتطويرها على التقارير المالية لابد من وضع الفرض الملائم والذي ينص على **(عدم وجود تأثير ذات دلالة معنوية عند مستوى معنويه (0.05) لمخاطر الامن السيبراني من حيث مراقبة الانظمة والشبكات وتطويرها على التقارير المالية وانعكاسها على مسؤولية مراقب الحسابات)** اذ تحتوي على ثلاث متغيرات والمتمثلة بـ **(x_1، x_2، x_3)** وهي

متغيرات مستقلة اما بالنسبة للمتغير التابع والمتمثل (التقارير المالية) (y_3) واختيار الانموذج الافضل للبيانات تبين ان قيمة (0.825= R^2) والذي يعني (معامل تحديد افضل نموذج) اي ان المتغيرات المستقلة تفسر (85%) تؤثر في المتغير التابع (y_3) اي ان ما تبقى يعدُّ من الاخطاء العشوائية في اختيار الاجابة المحددة او يعزى الى اخطاء غير معروفة اذ بلغت قيمتها (15%) اما بالنسبة لقياس دور العلاقة بين المتغيرات فقد بلغت قيمة (R=0.908) وهذا يدل على ان العلاقة قوية ،اما بالنسبة لقيمة اختبار (F=24.102) التي تدرس مدى ملائمة خط انحدار البيانات وفرضيته العدم الخاصة بأنموذج الانحدار اذ بلغ مستوى المعنوية (0.000) وهو اقل من (0.05) مما يدل عدم وجود فروق معنوية وان النموذج يمثل الظاهرة المدروسة تمثيلا دقيقا وان خط الانحدار يلائم البيانات المعطاة اي رفض فرضية العدم وقبول الفرضية البديلة اي بمعنى وجود تأثير ذات دلالة معنوية عند مستوى معنويه (0.05) لمخاطر الامن السيبراني من حيث مراقبة الانظمة والشبكات وتطويرها على التقارير المالية ،اما بالنسبة لمعامل (β) والذي يمثل تأثير كل متغير من المتغيرات المستقلة على المتغير التابع بمستوى معنوية اقل من (0.05) بعد اجتيازه اختبار (t)، اي بمعنى ان العلاقة طردية وذات تأثير معنوي وكما موضح بالجدول (5):-

جدول (5)

معامل تحديد افضل انموذج ومقدار التأثير للمتغيرات المستقلة لفرضية العدم الثالثة

Model Summary						
Model		R	**R Square**[b]	**Adjusted R Square**	**F**	Sig.
1		.908[a]	**.825**	**.791**	**24.102**	.000
Model			**Unstandardized Coefficients**	**Standardized Coefficients**	**T**	Sig.
1	X	B	**Std. Error**	**Beta**		
	x_1	.165	**.152**	**.177**	**1.079**	.016
	x_2	.121	**.170**	**.132**	**.710**	.031
	x_3	.070	**.144**	**.075**	**.490**	.026
a. Dependent Variable: y_3						
b. Linear Regression through the Origin						

- المصدر: من أعداد الباحث بالاعتماد على برنامج (SPSS v21)

دراسة فرضية العدم الرابعة :.

اما من خلال الجدول رقم (6) وبعد قياس التأثير لإدارة الوحدة الاقتصادية للمخاطر السيبرانية من حيث القوانين والتشريعات على التقارير المالية لابد من وضع الفرض الملائم لها والذي ينص على **(عدم وجود تأثير ذات دلالة معنوية عند مستوى معنويه (0.05) لمخاطر الامن السيبراني عند ادارة الوحدة الاقتصادية من حيث القوانين والتشريعات على التقارير المالية وانعكاسها على مسؤولية مراقب الحسابات)** اذ تحتوي على ثلاث متغيرات والمتمثلة بـ **(x_1، x_2، x_3)** وهي متغيرات مستقلة اما بالنسبة للمتغير التابع والمتمثل (التقارير المالية) (y_4) واختيار الانموذج الافضل للبيانات تبين ان قيمة (0.863= R^2) والذي يعني (معامل تحديد افضل نموذج) اي ان المتغيرات

المستقلة تفسر (86%) تؤثر في المتغير التابع (y_4) اي ان ما تبقى يعدُّ من الاخطاء العشوائية في اختيار الاجابة المحددة او يعزى الى اخطاء غير معروفة اذ بلغت قيمتها (14%) اما بالنسبة لقياس دور العلاقة بين المتغيرات فقد بلغت قيمة (R=0.929) وهذا يدل على ان العلاقة قوية ،اما بالنسبة لقيمة اختبار (F=32.081) التي تدرس مدى ملائمة خط انحدار البيانات وفرضيته العدم الخاصة بأنموذج الانحدار التي تنص (خط الانحدار يلائم البيات المعطاة) اذ بلغ مستوى المعنوية (0.000) وهو اقل من (0.05) مما يدل عدم وجود فروق معنوية وان النموذج يمثل الظاهرة المدروسة ثميلا دقيقا وان خط الانحدار يلائم البيانات المعطاة اي رفض فرضية العدم وقبول الفرضية البديلة اي بمعنى وجود تأثير ذات دلالة معنوية عند مستوى معنويه(0.05) لإدارة الوحدة الاقتصادية للمخاطر السيبرانية من حيث القوانين والتشريعات على التقارير المالية ،اما بالنسبة لمعامل (β) والذي يمثل تأثير كل متغير من المتغيرات المستقلة على المتغير التابع بمستوى معنوية اقل من (0.05) بعد اجتيازه اختبار (t). اي بمعنى ان العلاقة طردية وذات تأثير معنوي، مما يدل على ان جميع الابعاد ذات تأثير معنوي، وكما موضح بالجدول (6):-

جدول (6)

معامل تحديد افضل انموذج ومقدار التأثير للمتغيرات المستقلة لفرضية العدم الرابعة

Model Summary						
Model		**R**	**R Square[b]**	**Adjusted R Square**	**F**	**Sig.**
1		**.929[a]**	**.863**	**.836**	**32.081**	**.000**
Model			**Unstandardized Coefficients**	Standardized Coefficients	**T**	**Sig.**
1	**X**	**B**	**Std. Error**	**Beta**		
	x_1	**.252**	**.148**	**.247**	**1.699**	**.005**
	x_2	**.082**	**.166**	**.081**	**.495**	**.023**
	x_3	**.223**	**.140**	**.215**	**1.594**	**.017**
a. Dependent Variable: y_4						
b. Linear Regression through the Origin						

- المصدر: من أعداد الباحث بالاعتماد على برنامج (SPSS v21).

خامسا: دراسة فرضية العدم الخامسة:-

لدراسة اثر مخاطر الامن السيبرانية من ناحية البعد الاقتصادي والاجتماعي والسياسي على التقارير المالية لابد من وضع الفرض الملائم لها والذي ينص على (**عدم وجود تأثير ذات دلالة معنوية عند مستوى معنويه (0.05) لمخاطر الامن السيبرانية من ناحية البعد الاقتصادي والاجتماعي والسياسي على التقارير المالية وانعكاسها على مسؤولية مراقب الحسابات**) اذ تحتوي على ثلاث متغيرات والمتمثلة بـ (x_1، x_2، x_3) وهي متغيرات مستقلة اما بالنسبة للمتغير التابع والمتمثل (التقارير المالية) ولدراسة الفرضية لابد من وضع الانموذج الملائم للبيانات والذي يمثل مشكلة

الدراسة تمثيلا دقيقا ، فمن خلال الجدول (7) وبعد قياس التأثير واختيار الانموذج الافضل للبيانات تبين ان قيمة **(R^2 =0.850)** والذي يعني (معامل تحديد افضل نموذج) اي ان المتغيرات المستقلة تفسر **(85%)** تؤثر في المتغير التابع **(y_5)** اي ان ما تبقى يعدُّ من الاخطاء العشوائية في اختيار الاجابة المحددة او يعزى الى اخطاء غير معروفة اذ بلغت قيمتها **(15%)** اما بالنسبة لقياس دور العلاقة بين المتغيرات فقد بلغت قيمة **(R=0.921)** وهذا يدل على ان العلاقة قوية ،اما بالنسبة لقيمة اختبار **(F=24.718)** التي تدرس مدى ملائمة خط انحدار البيانات وفرضيته العدم الخاصة بأنموذج الانحدار اذ بلغ مستوى المعنوية (0.000) وهو اقل من (0.05) مما يـــدل عدم وجود فروق معنوية وان النموذج يمثل الظاهرة المدروسة تمثيلا دقيقا وان خط الانحدار يلائم البيانات المعطاة اي رفض فرضية العدم وقبول الفرضية البديلة اي بمعنى وجود تأثير ذات دلالة معنوية على التقارير المالية ، اما بالنسبة لمعامل **(β)** والذي يمثل تأثير كل متغير من المتغيرات المستقلة على المتغير التابع بمستوى معنوية اقل من (0.05) بعد اجتيازه اختبار **(t)**. اي بمعنى ان العلاقة طردية وذات تأثير معنوي، وكما موضح بالجدول (7):-

جدول (7)

معامل تحديد افضل انموذج ومقدار التأثير للمتغيرات المستقلة لفرضية العدم الخامسة

Model Summary						
Model		**R**	**R Square[b]**	**Adjusted R Square**	F	Sig.
1		**.921[a]**	**.850**	**.782**	24.718	.000
Model		**Unstandardized Coefficients**		**Standardized Coefficients**	T	Sig.
1	**X**	B	**Std. Error**	**Beta**		
	x_1	.249	**.118**	**.222**	2.108	.037
	x_2	.202	**.098**	**.179**	2.068	.041
	x_3	.163	**.101**	**.143**	1.611	.000
a. Dependent Variable: y_5						
b. Linear Regression through the Origin						

- المصدر: من أعداد الباحث بالاعتماد على برنامج (SPSS v21).

المحور الرابع: الاستنتاجات والتوصيات

اولا: الاستنتاجات

1. لقد آدي التطور التكنولوجي إلى مجموعة من النتائج الإيجابية التي انعكست على تحسين اقتصاديات الدول و الحياة العامة للأفراد، ولكن الاستغلال السلبي للتكنولوجيا أفرز مجموعة من المفاهيم، من بينها ما يعرف بمخاطر الامن السيبراني و تسبب أضرار للآخرين، تمس بخصوصياتهم وسرقة الهوية الرقمية والبيانات المالية.
2. الأمن السيبراني يعني اتخاذ التدابير اللازمة لحماية الوحدة الاقتصادية من الهجمات السيبرانية، وذلك من خلال مجموعة من الوسائل المستعملة قانونيا وتقنيا وتنظيميا وإداريا وتوعويا في منع الوصول غير المشروع للبيانات والمعلومات الإلكترونية ومنع استغلالها بطريقة غير قانونية.
3. تؤثر المخاطر السيبرانية على دقة ومصداقية التقارير المالية، مما قد يؤدي إلى انخفاض ثقة المستثمرين والمستخدمين بهذه التقارير، الأمر الذي ينعكس سلبًا على سمعة الوحدة الاقتصادية.
4. هناك توافق شبه كامل بين أفراد عينة البحث على أن الأمن السيبراني يلعب دورًا أساسيًا في حماية الأنظمة المحاسبية والشبكات والبيانات المالية من الهجمات الإلكترونية مما يعزز موثوقية التقارير المالية، وهذا يتطلب من مراقب الحسابات أخذ مخاطر الأمن السيبراني بعين الاعتبار عند تقييم البيئة الرقابية ونظم المعلومات، لضمان دقة وسلامة البيانات المالية وحمايتها من أي اختراق قد يؤثر على مصداقية التقارير.

ثانيا: التوصيات

1. وضع التشريعات التي تساهم في تطبيق الأمن السيبراني داخل الوحدة الاقتصادية، إصدار اللوائح التي تضمن سرية تبادل المعلومات المحاسبية، وتطبيق برامج الامن السيبراني التي تعمل على حماية أمن نظام المعلومات داخل الوحدات الاقتصادية.
2. لابد من تكاتف الجهود الداخلية والدولية لحماية أسرار البيانات والمعلومات الشخصية، وإدراج الجرائم السيبرانية في إطار معاهدات تسليم المجرمين المعتادين مثل هذا النوع من الجرائم وإنشاء منظمات دولية وإقليمية، وإبرام اتفاقيات ثنائية وجماعية تكون متخصصة مهمتها الأساسية التنسيق بشأن مواجهة الجرائم السيبرانية واحتوائها ومحاولة التخفيف منها.
3. ضرورة تعزيز دور ومسؤولية مراقب الحسابات في تقييم المخاطر السيبرانية التي قد تؤثر على دقة ومصداقية التقارير المالية من خلال مراجعة أنظمة الأمن السيبراني للوحدة، وتقييم مدى تأثير هذه على البيانات المالية، والإفصاح عن المخاطر المحتملة في التقارير المالية. وتوفير برامج تدريبية لمراقبي الحسابات لرفع مستوى الوعي لديهم حول التهديدات السيبرانية.
4. تحديث المعايير والإرشادات المتعلقة بمراقبة الحسابات ليشمل هذا التحديث تقييم مخاطر الأمن السيبراني، و كيفية التعامل مع هذه المخاطر، مما يضمن حماية البيانات المالية من أي تهديدات سيبرانية قد تؤثر على مصداقية التقارير المالية ودقة الإفصاح المحاسبي في ظل بيئة رقمية تتزايد تعقيدًا.

المصادر والمراجع

1)- المصادر العربية

أولاً- الكتب

1- ديري، زاهد محمد (2010) " الرقابة الادارية "، دار المسيرة للنشر والتوزيع، عمان.

2- سواد، زاهرة توفيق، (2009) " مراجعة الحسابات والتدقيق "، الطبعة الاولى، دار الراية للنشر والتوزيع، عمان – الاردن.

ثانياً - البحوث

1. ابو العلا، محمد عبد العزيز محمد، (2018) " اثر درجة التخصص الصناعي لمراجع الحسابات على جودة التقارير المالية بالتطبيق على الشركات المقيدة بالبورصة المصرية "، مجلة المحاسبة والمراجعة، العدد 2 ، كلية التجارة، جامعة بني سويف، مصر.
2. اميرهم، جيهان عادل، (2022)، " أثر جودة المراجعة في الحد من مخاطر الأمن السيبرانية وانعكاساته على ترشيد قرارات المستثمرين "، دراسة ميدانية، مجلة البحوث المالية والتجارية، كلية التجارة – جامعة بورسعيد، المجلد (23)- العدد الثالث .
3. الحسيني، هدى خليل ابراهيم، (2011) " مسؤولية مراقب الحسابات " مجلة كلية بغداد للعلوم الاقتصادية، العدد (28).
4. السيد، عادل محمد علي، (2024)، " الحماية الدستورية للأمن السيبراني ودوره في حماية الحق في الخصوصية المعلوماتية " مجلة روح القوانين، كلية القانون، بجنا كليس- بحيرة، العدد (106) – (1)، (1- 185).
5. عبد الجواد، أميرة عبد العظيم، (2020)، " المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام " *مجلة البحوث الفقهية والقانونية ، جامعة القاهرة*, *32*(35), 1–131.
6. عبد الوهاب نصر، اسماء احمد الصيرفي، (2020)، " اثر مستوى الالتزام الاخلاقي للمحاسبين الماليين على جودة التقارير المالية بالتطبيق على الشركات المقيدة بالبورصة المصرية "، مجلة المحاسبة والمراجعة، كلية التجارة، جامعة دمنهور، مصر.
7. القاضي، عبد الامير نجم، (2017) " مسؤولية مراقب الحسابات عن تقييم نظام الرقابة الادارية " المجلة العراقية للعلوم الادارية، كربلاء.
8. المرداس، ندى بنت خالد، (2023)، "الأمن السيبراني في المملكة السعودية بين الواقع والمأمول، دراسة نظرية تحليلية" المجلة الدولية لنشر البحوث والدراسات، العدد(49)، المجلد (5)، 2709-7064.
9. المري، راشد محمد، (2023)، " الأمن السيبراني وحماية الأنظمة الإلكتروني " دراسة تحليلية تأصيلية ، مجلة الدراسات القانونية والاقتصادية, الأردن، 9(1), 959-1008.
10. يوسف بوغرارة، (2018)، "الأمن السيبراني، الاستراتيجية الجزائرية للأمن السيبراني والدفاع في الفضاء السيبراني "، مجلة الدراسات – الجزائر المجلد (1)، العدد (3).

ثالثاً – الرسائل والاطاريح

1. احمد، محمد صديق عبد العزيز (2019)، " حوكمة المراجعة ودورها في تقليل مخاطر المراجعة وتحسين جودة التقارير المالية، جامعة االنيلين، اطروحة دكتوراه.
2. حكيمة مناعي، (2009)، " تقارير المراجعة الخارجية في ظل حتمية تطبيق المعايير المحاسبية الدولية في الجزائر "، رسالة ماجستير، كلية العلوم الاقتصادية والتسيير، جامعة الحاج لخضر- باتنة، الجزائر.
3. الدحدوح ، حازم فهمي عادل ، (2014) " العوامل المؤثرة على توقيت اصدار التقارير المالية للشركات المدرجة في بورصة فلسطين " ، الجامعة الاسلامية - غزة ، رسالة ماجستير.
4. الرشيدي، طارق عبد العظيم يوسف، (2019)، " أثر الإفصاح عن مخاطر الأمن السيبراني في التقارير المالية على أسعار الأسهم وأحجام التداول"، دراسة مقارنة في قطاع تكنولوجيا المعلومات، رسالة ماجستير، كلية التجارة، جامعة دمياط – مصر.
5. الشورة، إيمان محمد (2020) " الامن السيبراني في البنوك الاسلامية الاردنية "، رسالة بكالوريوس، كلية الشريعة، جامعة الاردن .
6. الشورة، إيمان محمد (2020) " الامن السيبراني في البنوك الاسلامية الاردنية "، رسالة بكالوريوس، كلية الشريعة، جامعة الاردن .
7. طه، عبدالله الامام ادم واخرون، (2017) " دور نظم المعلومات المحاسبية في جودة التقارير المالية" بحث تكميلي لنيل شهادة البكالوريوس في المحاسبة والتمويل، جامعة السودان للعلوم والتكنولوجيا.
8. عبادي، دعاء سرحان، (2023)، " أثر تطبيق تكنولوجيا الأمن السيبراني علي جودة التقارير المالية "، دراسة استطلاعية لعينة من المدققين الداخليين والخارجيين، جامعة الفرات الاوسط التقنية، العراق.
9. قرفي، عبد العال، شيماء ، (2019) " دور محافظ الحسابات في مراجعة حسابات الشركات " رسالة ماجستير، كلية العلوم الاقتصادية، قسم العلوم المالية والمحاسبية، جامعة العربي التبسي.
10. وفقان، حسام محمد، (2021) " أثر تؤخُّر نشر التقارير المالية على القيمة السوقية لاسهم الشركات العراقية المدرجة في سوق العراق للأوراق المالية " دراسة تطبيقية، رسالة ماجستير، كلية الادارة والاقتصاد، جامعة القادسية.

2) – المصادر الأجنبية

First- Books:

1. Arens, A. A., Elder, R. J., & Beasley, M. S. (2013). Auditing and assurance services (16th ed.). United States: Pearson.
2. Basu, S. K. (2016). Auditing and assurance (2nd ed.). Pearson India Education Services Pvt. Ltd.
3. Ghelani, D. (2022). Cyber security, cyber threats, implications and future perspectives.
4. Johnstone, K. M., Gramling, A. A., & Rittenberg, L. E. (2013). Auditing: A risk-based approach to conducting a quality audit (9th ed.). South-Western, Cengage Learning.

Second - Scientific research and articles:-

1. Al Shamsi, A. (2019). Effectiveness of cyber security awareness program for young children: A case study in UAE. International Journal of Information Technology and Language Studies, 3(2), 1–9.
2. Barry, T., Jona, J., & Soderstrom, N. (2022). The impact of country institutional factors on firm disclosure: Cybersecurity disclosures in Chinese cross-listed firms. Journal of Accounting and Public Policy.
3. Bicak, A., Liu, X. M., & Murphy, D. (2015). Cybersecurity curriculum development: Introducing specialties in a graduate program. Information Systems Education Journal, 13(3), 99–106.
4. Catota, F. E., Morgan, M. G., & Sicker, D. C. (2019). Cybersecurity education in a developing nation: The Ecuadorian environment. Journal of Cybersecurity, 5(1), tyz001.
5. Cheong, A., Yoon, K., & Cho, S. (2021). Classifying the contents of cybersecurity risk disclosure through textual analysis and factor analysis. Journal of Information Systems, 35(2), 179–194.
6. Eaton, T. V., Grenier, J. H., & Layman, D. (2019). Accounting and cybersecurity risk management. Current Issues in Auditing, 13(2), A1–A39.
7. Eling, M., & Wirfs, J. H. (2016). Cyber risk: Too big to insure. Risk transfer options for a mercurial risk class. Institute of Insurance Economics, University of St. Gallen, 20–58.
8. Haapamäki, E., & Sihvonen, J. (2019). Cyber security in accounting research. Managerial Auditing Journal, 34(7), 808–834.
9. Hilary, G., Segal, B., & Zhang, M. H. (2016). Cyber-risk disclosure: Who cares, Georgetown McDonough School of Business Research Paper.
10. Jayakumar, S. (2020). Cyber attacks by terrorists and other malevolent actors: Prevention and preparedness. In A. P. Schmid (Ed.), Handbook of terrorism prevention and preparedness (pp. 871–930). ICCT Press.
11. Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2018). What is the impact of successful cyberattacks on target firms? National Bureau of Economic Research Working Paper No. 24409.
12. Mohammad, N., & Hamed, K. (2013). Impact of conservatism on the accounting information quality and decision making of the shareholders and the firms listed on the Tehran Stock Exchange. International Journal of Academic Research in Accounting, Finance and Management Sciences, 3(3), 186–197.

13. Raigen, D., Diakun, N., & Purse, R. (2014). Defining cyber security. Technology Innovation Management Review, 4(10), 13–22.
14. Waxman, M. C. (2011). Cyber-attacks and the use of force: Back to the future of Article 2(4). Yale Journal of International Law, 36, 421–459.