

أهمية تبني اطار COSO المحدث ودوره في تحقيق الامن السيبراني لإدارة المخاطر المؤسسية في الوحدات الاقتصادية - دراسة استطلاعية

إعداد الباحثة م.م. منال ظاهر رشاد

قسم الشؤون المالية في الجامعة المستنصرية

manal76.mr@gmail.com

المستخلص :

تهدف هذه الورقة البحثية لبيان أهمية تبني إطار COSO المحدث في ظل نظام البيئة الرقابية الداخلية للوحدات الحكومية للمحافظة على امن وسلامة البيانات والمعلومات في تلك الوحدات والحد من المخاطر المحيطة بها أو تقليلها لاقبل حد ممكن في ظل بيئة رقابية متطورة نتيجة اعتماد الانظمة والوسائل الحديثة في تلك الوحدات عن طريق البرامج والمواقع الالكترونية المعتمدة في تبادل وارشفة المعلومات . وتوصلت الباحثة الى أن هناك دور فعال للوسائل التي يتبعها المدقق الداخلي من خلال تطبيق اطار COSO المحدث عند تدقيقه للبيانات والمعلومات والوثائق المؤرشفة الكترونيا وللمواقع الالكترونية المعتمدة لحماية الوحدات الاقتصادية من المخاطر المؤسسية ودعم أمن وسلامة البيانات والمعلومات.

وكانت ابرز التوصيات هي أن حوكمة الادارة متمثلة بفلسفتها واسلوبها بالتعامل مع تدقيق البيانات والاوليات المرسله والمؤرشفة إلكترونيا وموقفها الداعم لذلك وكفاءة الافراد العاملين سواء مدخلي البيانات أو مدققيها والقيم الاخلاقية التي يتمتع بها هؤلاء العاملين تتأثر ببيئة الوحدة الاقتصادية وتحد من المخاطر المؤسسية التي تتعرض لها تلك الوحدة وتحافظ على أمن وسلامة المعلومات من التلاعب والتزوير والاختراق.

:Abstract

This research paper aims to demonstrate the importance of adopting the updated COSO framework in light of the internal control environment system of government units to maintain the security and integrity of data and information in those units and reduce the risks surrounding them or reduce them to the lowest

possible extent in light of an advanced control environment as a result of adopting modern systems and means in those units Through approved programs and websites for exchanging and archiving information.

The researcher concluded that there is an effective role for the methods used by the internal auditor through the application of the updated COSO framework when auditing data, information, electronically archived documents and approved websites to protect economic units from institutional risks and support the security and integrity of data and information.

The most prominent recommendations were that the administration's governance is represented by its philosophy and method of dealing with auditing data and priorities sent and archived electronically and its supportive position for that and the efficiency of the working individuals, whether data entry or auditors, and the moral values enjoyed by these workers are affected by the environment of the economic unit and reduce the institutional risks to which that unit is exposed and maintains On the security and safety of information from manipulation, forgery and penetration.

المقدمة :

في ظل التطورات التكنولوجية واعتماد الوسائل الالكترونية الحديثة في الوحدات الحكومية في تعاملاتها سواء على الصعيد الداخلي او الخارجي وكيفية الحفاظ على الوثائق والبيانات الهامة وحمايتها من الاختراق لاسيما بعد انتشار وباء كورونا وما القى بظلاله على العمليات المالية وكيفية تداولها وتدقيقها يبرز أهمية اتباع وسائل وانظمة رقابية حديثة تحد من مشاكل ضياع او اختراق البيانات والمعلومات الهامة والسرية الخاصة بالوحدة الاقتصادية لتقليل المخاطر المحتملة او الحد منها وذلك بتبني الاهداف الرئيسية لاطار COSO المحدث ، ولتحقيق ذلك تقدم الباحثة توضيحاً لهذا الموضوع المهم في هذه الورقة البحثية من خلال ثلاثة مباحث يتناول المبحث الاول الاطار المنهجي

للبحث وبعض الدراسات السابقة، أما المبحث الثاني فيسلط الضوء على الاطار النظري للبحث فيما يبين المبحث الثالث الاطار العملي للبحث.

حيث يستوجب ذلك تطبيق اطار رقابي يحدد كيفية الوصول واحكام الرقابة والسيطرة على تلك المواقع والبرامج والبيانات المؤرشفة الكترونيا والحد من مخاطر الاختراق والتلاعب والسرقة سواء على صعيد المعلومات المالية أو المعلومات غير المالية .

الاطار المنهجي للبحث والدراسات السابقة

أولاً : مشكلة البحث

تتمحور مشكلة البحث في ظل حدوث الازمة العالمية (وباء كورونا) وما نتج عنه من اعتماد مواقع التواصل الالكترونية لادارة أعمال الوحدات الحكومية وضرورة الحاجة في معظم تلك الوحدات ولاسيما عينة البحث المتمثلة بقسم الرقابة والتدقيق في كل من رئاسة الجامعة المستنصرية والمراكز التابعة للجامعة وشعب التدقيق في الكليات الموجودة في موقع الجامعة بالاضافة الى الموظفين العاملين في ديوان الرقابة المالية العاملة في الجامعة المستنصرية التابع لوزارة المالية ، وتتمثل مشكلة البحث بالآتي :

- تساهم المبادئ المتضمنة في اطار COSO عند تبنيتها من قبل موظفي الرقابة والتدقيق الداخلي في دعم الامن السيبراني في الوحدات الاقتصادية التي تستخدم الوسائل التكنولوجية في عملها للسيطرة على المخاطر المؤسسية المحتملة وادارتها بكفاءة .

ثانياً : أهمية البحث

ان اعتماد الوسائل التكنولوجية في معالجة البيانات المالية وغير المالية وأرشفة المعلومات الهامة لاستردادها عند الحاجة والمخاطبات الهامة والسرية في الوحدات الحكومية وبين بعضها البعض يستدعي كل ذلك ضرورة التأكد من صحتها لاعتمادها والمحافظة على تلك البيانات والمعلومات من الاختراق والضياع والتلف ، لذا جاء هذا البحث ليسلط الضوء على أهمية تبني أنشطة التدقيق الحديثة المطبقة في الوحدات الحكومية لمواجهة مخاطر استخدام التكنولوجيا والحفاظ على أمن وسلامة المعلومات السرية من الاختراق والتزوير .

ثالثاً : أهداف البحث

يسعى هذا البحث لتحقيق الاهداف الآتية :

- 1- بيان أهمية تبني أطر جديدة للتدقيق الداخلي في الوحدات الحكومية من خلال تسليط الضوء على مفهوم إطار COSO المحدث والمبادئ المرتكز عليها .
- 2- تحديد مفهوم الأمن السيبراني والمبادئ والمتطلبات اللازمة لدعمه .
- 3- التعريف بدور أنشطة المدقق الداخلي المتبعة لإدارة مخاطر اختراق وضياع البيانات والمعلومات المؤرشفة إلكترونياً

رابعاً : فرضية البحث

يسعى البحث لإثبات مدى صحة الفرضية الآتية :

- 1 – ان مكونات أنشطة COSO المتبعة والمتعلقة بمبادئ المعلومات وبالمتابعة أو المراقبة لها تأثير معنوي على درء المخاطر المتعلقة بالأمن السيبراني في الوحدات الاقتصادية .

*بعض الدراسات السابقة

- 1- دراسة (Beasley,Branson&Hancock,2010) ، "How Key Risk Indicators can Sharpen Focus on Emerging Risks" – كيف يمكن لمؤشرات المخاطر الرئيسية أن تزيد من حدة المخاطر الناشئة . بينت هذه الدراسة أن هناك العديد من المنظمات التي تتبنى نهج للإشراف على المخاطر على مستوى المؤسسة من خلال الاطار المتكامل COSO لمساعدة الادارة التنفيذية في عملية ادارة المخاطر بشكل أوسع .

- 2- (Gaaligan&others,2019) ، "Managing Cyber Risk in A Digital Age" – هدف الدليل الى تقديم نظرة عامة للمديرين التنفيذيين واعضاء مجلس الادارة حول ادارة المخاطر الالكترونية من خلال المبادئ المحددة في اطار عمل COSO لادارة المخاطر المؤسسية .

- 3-دراسة بدوي ،عبد السلام خميس،2011 "أثر هيكل نظام الرقابة الداخلية وفقاً لاطار COSO على تحقيق أهداف الرقابة"

هدفت الدراسة الى التعرف على اثر عناصر هيكل الرقابة الداخلية بموجب اطار COSO على تحقيق اهداف الرقابة في المنظمات الاهلية العاملة في قطاع غزة والتعرف على تطور بناء هياكل لانظمة الرقابة الداخلية في هذه المنظمات

4-Mulyandani,Vina,2022 ,”Evaluation Internal Control System of Cash Spending Based on the Framework COSO”

يهدف هذا البحث تقييم تطبيق نظام الرقابة الداخلية على الصرف النقدي باستخدام المنهج الوصفي التحليلي حيث توصلت الدراسة الى ان تطبيق هذا النظام جيد ومناسب مع اطار COSO .

5-Antonio,Rossella,2021 “The WorldCom fraud under the COSO framework analysis”

6-Shafqat N. & Masood A.,2016 “Comparative Analysis of Various National Cyber Security Strategies”

هدفت الدراسة الى بيان نقاط الضعف الجوهرية في الفضاء السيبراني والهجمات التي يتعرض لها باستمرار وما يؤدي الى تهديد الامن القومي والاقتصاد و حياة المواطنين اليومية ووضع استراتيجيات لامن السيبراني للتصدي لهذه التهديدات المتنوعة .

7-Al-Fatlawi,Qaayssar & Al- Ramaahi ,Athraa,2021 “The relationship between internal censorship components by the existing coso framework and the performance of the external Auditor ”

هدف البحث الى تعزيز المعرفة الفكرية بطار الرقابة الداخلية الذي يجمع مكونات COSO المحدث وتقييم اطار الرقابة الداخلية وفق اطار COSO المحدث في المصارف العراقية الخاصة حيث بينت نتيجة البحث بان هناك تباين بين البنوك الخاصة في تطبيق مكونات الرقابة الداخلية وفق اطار COSO المحدث .

8- الجوهر والعيدي ، 2019 ، "نموذج مقترح لاستمارة فحص الرقابة الداخلية في ضوء مبادئ اطار COSO المتكامل المحدث"

اوضحت الدراسة التعرف على اطار COSO للرقابة الداخلية المحدث لسنة 2013 والمبادئ الجديدة التي تم اضافتها ضمن المكونات الخمسة للاطار والتعرف على مدى

امكانية تطبيق هذا الاطار من خلال تصميم استمارة فحص تغطي مبادئه ومكوناته والتعرف على نقاط ضعف الرقابة الداخلية .

9-كاظم ونصيف ، 2019 ، "العلاقة بين حوكمة الشركات وادارة مخاطر مشروع (ERM) دراسة استطلاعية لاراء عينة من الاكاديميين والمهنيين"

بينت الدراسة تاثير اعتماد اطر الرقابة الداخلية بصورة واسعة في عملية تقييم الرقابة الداخلية في مساعدة الوحدات الاقتصادية في عملية تحسين القرارات المتخذة وتطوير القيمة الاجمالية لها وتقليل ارتكاب الاحتيال والكشف المبكر عن حالات التلاعب والغش وارتكاب الاحتيال .

10-Wideman,R.,1992” Project and Program RISK MANAGEMENT ”

هدف هذا الكتيب الى توفير فهم مبسط عن طبيعة مخاطر المشروع ونظرة ثاقبة في عملية ادارة مخاطر المشروع لاي شخص يفكر في تأسيس مشروعه سواء كان صغيراً أم كبيراً .

ثانياً : الجانب النظري للبحث

1- مفهوم إطار COSO المتكامل المحدث للرقابة الداخلية : إن مصطلح COSO

يمثل اختصاراً للعبارة (Committee Of Sponsoring Organizations) والتي يقصد بها لجنة دعم او رعاية المنظمات التابعة للجنة Tread way Commission حيث كان جيمس جيم تريدواي الابن العضو لهيئة الاوراق المالية وأول رئيس ل COSO التي نشأت في الولايات المتحدة عام 1985 لرعاية اللجنة الوطنية لاعداد التقارير المالية الاحتياطية ، وتعد لجنة قطاع خاص غير هادفة للربح وتتألف من :معهد المحاسبين الاداريين (IMA) ،معهد المدققين الداخليين (IIA) ، المعهد الامريكي للمحاسبين القانونيين (AICPA) ،الجمعية الامريكية للمحاسبة (AAA) ، معهد المدراء الماليين (FEI) (العبيدي والجوهر، 2019: 5) وقد عرفت لجنة COSO الرقابة الداخلية بأنها عملية تتأثر بالإدارة وبجميع المعنيين بإدارة الوحدة الاقتصادية وتصمم من أجل الحصول على تأكيد مناسب حول تحقيق الاهداف التالية :

- فاعلية وكفاءة العمليات التشغيلية.
- مدى مصداقية البيانات المالية.
- كيفية الالتزام بالسياسات والانظمة والقوانين .(بدوي ، 2011: 29)

وأشار (Mulyandani,2022:22) الى أن تعريف الرقابة الداخلية بموجب هذه اللجنة بأنها عملية يتأثر بها مجلس الادارة والادارة والموظفون الآخرون في كيان مصمم لتقديم تأكيد معقول بخصوص تحقيق الاهداف حول الكفاءة والفعالية التشغيلية، ومستوى الموثوقية بالتقارير المالية، والامتثال للقوانين واللوائح المعمول بها وذلك بهدف حماية الاصول من سوء الاستخدام و انتاج معلومات وبيانات محاسبية دقيقة والالتزام بالقوانين والانظمة داخل الوحدة الاقتصادية، كما بينت لجنة COSO مكونات الرقابة الداخلية بالنقاط الخمسة الآتية:

- 1- بيئة الرقابة .
- 2- تقييم المخاطر.
- 3- أنشطة الرقابة.
- 4- الاتصالات والمعلومات.
- 5- أنشطة المراقبة (المتابعة).

كما ذكر (Antonio,2021:60; 65) الى أن الاطار المتكامل لإدارة المخاطر المؤسسية (ERM) لا يجب اعتباره بديلاً عن الاطار المتكامل للرقابة الداخلية COSO لان الاثنين متوافقان تماماً ويستندان الى نفس الاساس المفاهيمي ولكن ادارة المخاطر المؤسسية تمثل إطاراً أوسع من ضمنه نظام الرقابة الداخلية. لهذا السبب تعد تقارير COSO في الوقت الحالي الحل الأمثل للتعامل مع الرقابة الداخلية وادارة المخاطر وتحظى بقبول واسع من قبل المنظمات المهنية.

كما أوضح بأن أهم الاسباب التي دفعت هيئة COSO الى تحديث إطار الرقابة الداخلية لعام 1992 هو التغييرات التي طرأت كظهور الاسواق المعولمة والتحولت في نماذج الاعمال التجارية وكثرة استخدام مقدمي الخدمات الخارجيين لذلك تم إصدار إطار COSO المحدث لعام 2013 حيث يتكون هذا الاطار من سبعة عشر مبدأً مرتباً بالمكونات الخمسة للرقابة الداخلية .

حيث لخص (الجوهر والعيدي، 2019: 15-16) المكونات الخمسة للرقابة الداخلية وما يتضمنه من مبادئ سبعة عشر وفق إطار COSO المتكامل المحدث لعام 2013 بالجدول الآتي :

جدول رقم (1)

عدد خاص لوقائع الندوة العلمية السنوية لقسم الدراسات الاقتصادية في مركز المستنصرية
لدراسات العربية والدولية للعام 2023

يبين أبرز مكونات الرقابة الداخلية الخمسة والمبادئ السبعة عشر التابعة لها وفق إطار
COSO المتكامل المحدث

ت	المكونات	المبادئ
1	بيئة الرقابة: وهو اساس جميع المكونات الاخرى للرقابة الداخلية ويتضمن النزاهة والقيم الاخلاقية والكفاءة والبيئة الرقابية التي تعد محرك يدفع الوحدة بالاتجاه الصحيح.	1- الالتزام بالاخلاق والنزاهة 2- الاشراف على الرقابة الداخلية من قبل مجلس الادارة وبشكل مستقل عن الادارة . 3- الهياكل وخطوط التقارير والمسؤوليات المناسبة لتحقيق اهداف الادارة والتي يشرف عليها المجلس . 4- جذب الافراد ذوي الكفاءة وتطويرهم 5- محاسبة الافراد عن مسؤولياتهم في الرقابة الداخلية لتحقيق الاهداف.
2	تقدير المخاطر: يتوجب على الوحدة الاقتصادية تحديد المخاطر وتحليلها وادارتها إذ تعد ادارة المخاطر عملية مستمرة نظراً لتغيرات البيئة الخارجية والداخلية باستمرار التي قد تشكل عقبة أمام الوحدة.	6- تحديد الاهداف بشكل واضح للتمكن من تحديد المخاطر وتقييمها . 7- بعد تحديد وتحليل المخاطر يتم تحديد كيفية ادارتها. 8- النظر فيما اذا كان هناك احتيال 9- تحديد التغيرات وتقييمها والتي قد تؤثر على نظام الرقابة الداخلية
3	أنشطة الرقابة: وتتمثل بالسياسات والاجراءات الرقابية التي تساعد على ضمان تنفيذ الاجراءات المحددة لمعالجة المخاطر وتحقيق الاهداف بفاعلية بضمنها أنشطة التحكم على مراحل العمال المختلفة والتكنولوجيا.	10- تطوير واختيار الضوابط التي تساعد على تخفيف المخاطر لمستوى مقبول. 11- تطوير واختيار أنشطة رقابية على التقنية . 12- نشر أنشطة الرقابة على السياسات والاجراءات ذات العلاقة.

4	المعلومات والاتصال :بضمناها نظم المعلومات والاتصالات وتبادل المعلومات داخليا وخارجيا لتنفيذ أنشطة الرقابة الداخلية اليومية وفهم المسؤوليات لكل موظف .	13- الحصول على معلومات ذات صلة وجودة عالية لدعم الرقابة الداخلية . 14- ابلاغ المعلومات داخليا بضمناها الاهداف والمسؤوليات لدعم عناصر الرقابة الداخلية الاخرى. 15- نقل مسائل الرقابة الداخلية الى الاطراف الخارجية ذات الصلة .
5	المتابعة أو المراقبة : من خلال رصد جميع العمليات وجراء التعديلات والابلاغ عن اوجه القصور بالوقت المناسب وابلاغ الادارة العليا بالمسائل الخطيرة .	16- تطوير واختيار واجراء التقييمات بشكل دوري او مستمر لعناصر الرقابة الداخلية . 17- الابلاغ عن اوجه القصور للمسؤولين (الادارة العليا) وتقييمها لوضع الاجراءات التصحيحية .

المصدر : (الجوهر والبيدي، 2019: 15 – 16)

وترى الباحثة من خلال هذه المبادئ السبعة عشر أنها تركز على عدة أمور ليس فقط
كيفية منع التزوير والتلاعب المالي وإنما تذهب لابعاد من ذلك نظراً للتحديثات التي
ضمّنها اطار COSO المتكامل والتحديات الجديدة لمخاطر التدقيق فهي تتضمن التركيز
على درء المخاطر عن الوحدة الاقتصادية بما يحقق أهدافها ويضمن المحافظة على
جميع الامور المالية وغير المالية من معلومات سرية ومنع التلاعب والتزوير والغش
في تلك التعاملات في ظل استخدام الارشفة الالكترونية للمعاملات وحفظ البيانات من
خلال الحاسوب الالكتروني .

2- مفهوم الأمن السيبراني **Cyber Security** : يعتمد الاقتصاد العالمي بشكل
عام على استراتيجيات الامن السيبراني الفعالة لضمان حماية اصول الوحدات
الاقتصادية بكافة انواعها وحماية البيانات والمعلومات من الاختراق والهجمات
الالكترونية والذي يشكل تهديد لمعظم هذه الوحدات في ظل اعتمادها الكبير على
التبادل الالكتروني للبيانات والتعاملات التجارية ، حيث يقوم قرصنة الانترنت
باستغلال تعطش المجتمع للتكنولوجيا للتخطيط لجرائمهم من خلال السيطرة على
المعلومات هامة والسرية لتهديد الأمن القومي بشكل واسع وأمن الوحدات
الاقتصادية الكبرى بشكل خاص من أجل ذلك لا بد من توضيح هذا المفهوم وكما
يأتي :

الامن السيبراني أو أمن تكنولوجيا المعلومات هو عبارة عن مجموعة من الاجراءات والعمليات التي تسعى لتأمين وحماية الشبكات واجهزة الحاسوب والبرامج والمعلومات من الهجمات الالكترونية أو السرقة أو التلف والوصول غير المصرح به للمعلومات. (المنيع،2022: 163) في حين عرفه (Cook,2017:32-33) "القدرة على حماية الفضاء الالكتروني أو الدفاع عنه من الهجمات الالكترونية بما في ذلك القدرة على الكشف عن الهجمات المحتملة وتقييمها واستغلال ذلك في التصدي لها من خلال المبادئ الاساسية الامان،السرية، النزاهة ويؤثر الامن السيبراني المتبع على الامن القومي والازدهار الاقتصادي والشخصي".

وقد تطرق الى الجريمة السيبرانية ووصفها بأنها اختراق البيانات والتلاعب بها بشكل اجرامي أو ضار من خلال استخدام أجهزة الحاسوب المتصلة بالشبكة للمساعدة على ارتكاب الجرائم كالارهاب والتجسس واساءة استخدام الحاسوب والاحتيال عبر الشبكات المحلية أو الدولية .

يتبين من خلال التعاريف السابقة للأمن السيبراني بأنه معني بالحفاظ على أمن وسلامة البيانات والمعلومات وحمايتها من الاختراق والمخاطر الناشئة عن بيئة تقنية المعلومات سواء ما كان متعلق بالحماية المادية للاجهزة والبرامجيات من سوء الاستخدام أو التخريب بالإضافة الى مشاكل واطء التطبيقات وكيفية تأمين حمايتها من التلاعب والتزوير والهجمات الالكترونية ، كما أشار (Cook,2017:18) أن أهم عنصر في مكافحة التهديدات السيبرانية هو الناس حيث هم من يُنشئوا التقنيات والبرامج وبإمكانهم فهم ومعرفة كيفية حمايتها من الهجمات في الفضاء السيبراني حيث يساعد التطوير وتعزيز الوعي والتدريب للقوى العاملة والتعاون مع الجهات الخارجية سواء كانت حكومية ام خاصة في تعزيز حماية مستخدمي تلك البرامج والمواقع الالكترونية .

وغالبا ما تحدث الجريمة الالكترونية بشكل غير منظم من الناحية الزمانية والمكانية في البيئة الافتراضية حيث هناك مجرمين متحمسين يسعون لاقتناص الفرص لارتكاب الجرائم الالكترونية فقد يستمر الجناة في الفضاء السيبراني انتظار النقر على اي اداة مصابة من قبل الاشخاص المستخدمين من اجل غزو أجهزتهم بالبرامج الضارة أو سرقة الملفات السرية سواء كانت شخصية أو تتعلق بالوحدة الاقتصادية. (علي،2022: 119)

أهم المبادئ والمتطلبات المتعلقة بالأمن السيبراني : تم الاتفاق على تقسيم مبادئ الامن السيبراني والادارة الالكترونية للبيانات والبرمجيات الى خمسة مبادئ ومتطلبات كما يأتي : (العقابي والربيعي،2018: 65)

- 1- المبادئ والمتطلبات الادارية : تساهم هذه المتطلبات في التطوير والتغيير ودعم الاساليب الادارية الحديثة من خلال وضع الاستراتيجيات وخطط التأسيس وتطوير التنظيم الاداري بالكفاءات والمهارات المتخصصة التي تتولى مهمة تشكيل لجان تتولى مشروع الادارة الالكترونية لتحديد المنافذ الالكترونية وكيفية ادارتها من قبل الادارة العليا في الوحدة الاقتصادية.
- 2- المبادئ والمتطلبات التقنية : وتتمثل بكافة المكونات المادية التي من خلالها يتم تنفيذ التطبيقات الالكترونية عن طريق الحواسيب الالكترونية ونظم المعلومات والهواتف والفاكسات لتوفير التقنية المناسبة لطبيعة عمل الوحدة الاقتصادية لتطوير اداءها ويشترط هذا المبدأ توفر البنى التحتية من أجهزة ومعدات وبرمجيات .
- 3- المبادئ والمتطلبات البشرية : وتعد الاساس الذي يمكن استثماره لتحقيق النجاح في تطبيق ودعم الامن الالكتروني بإعتباره رأس مال فكري تستند عليه الوحدات الاقتصادية من خلال اعداد الكوادر المختصة بإنشاء وبرمجة المواقع الالكترونية وبرامج الارشفة الالكترونية والمخاطبات عبر المواقع الرسمية بين مختلف الوحدات الاقتصادية وهذا يتطلب التدريب المستمر لمواكبة الحركة السريعة في تطور مجال التكنولوجيا والاتصالات .
- 4- المبادئ والمتطلبات المالية : تعد من المبادئ المهمة والاساسية التي تعوق مشاريع الادارة الالكترونية والمحافظة على أمن وسلامة المعلومات حيث تتطلب الادارة الالكترونية في المشاريع الكبيرة أموال طائلة مقارنة بالمشاريع المتوسطة والصغيرة ، من توفير الاجهزة والمعدات الالكترونية الحديثة الى اقامة البرامج التدريبية المختصة وتوفير البرامج الحديثة وتطويرها بشكل مستمر.
- 5- المبادئ والمتطلبات الأمنية : تتعلق هذه المتطلبات بأمن وحماية قواعد البيانات لحماية المعلومات من المخاطر الداخلية والخارجية التي من الممكن أن تتعرض لها الوحدات الاقتصادية من خلال تشريع القوانين والانظمة لسلامة وصول المعلومات للمستفيدين على سبيل المثال تنصيب جدار ناري لحماية البرامج والمعلومات من الاختراق والتلف ، تشفير المعلومات والوثائق السرية برمز دخول خاص بالمستخدم لايسمح لغيره الوصول اليها مثل كلمات المرور التي تتكون من ست خانات على الاقل من حروف وارقام ، التحديث المستمر للبرامج المضادة للفايروسات ، عمل نسخ احتياطية للبرامج والمعلومات الهامة وحفظها في أماكن آمنة .

مصادر التهديد السيبراني : تتمحور مصادر التهديد السيبراني بمايأتي :
(منشور مستشارية الامن الوطني ، بدون سنة: 5)

1- الدول الاجنبية

2- الارهابيين والجماعات المتطرفة

3- النقابات الجنائية المنظمة

4- الشركات

5- الهاكرز

3- مفهوم إدارة المخاطر المؤسسية : تعد ادارة المخاطر جزء من حوكمة الشركات

وقضية مهمة في مسائل المحاسبة الادارية والمراقبة في الوحدات الاقتصادية إذ تسهل عملية صياغة الاهداف ورسم الفرص والمخاطر المحتملة وكيفية تحقيق الاهداف ، ويمكن تعريف المخاطر وفقاً لمعيار آيزو 31000 بأنها حالة من عدم اليقين التي من الممكن ان تؤثر على اهداف المنظمة الاستراتيجية فالتأثير الناتج من المخاطر قد يكون سلبي متمثلاً بالتهديدات أو إيجابي متمثلاً بالفرص ، وقد عرف (Sudaryono&others,2022:180) ادارة المخاطر المؤسسية بانها "قدرة المنظمات على فهم والتحكم في مستوى المخاطر التي يتم التعرض لها في ادارة استراتيجيات الاعمال والفائدة الرئيسية منها التركيز على ادارة المخاطر عبر جميع خطوط الشركة " ، في حين عرفها (كاظم ونصيف،2019: 632) بأنها عبارة عن عملية يقوم بها مجلس الادارة والموظفين الآخرين في إعداد وتطبيق استراتيجيات واضحة من خلال الوحدة الاقتصادية تهدف لتحديد الاهداف المحتملة والتي قد تؤثر على الوحدة وادارة المخاطر المطلوبة لتوفير تأكيدات معقولة وكافية فيما يتعلق بتحقيق أهداف الوحدة الاقتصادية ككل .

وأشار اليها(Boon& other,2022:3) بأنها إطار عمل متكامل تستخدمه المؤسسات بشكل واسع لتقليل المخاطر إذ تدعو لجنة COSO المنظمات للتركيز على ادارة المخاطر المؤسسية ودمجها لتحديد المخاطر وادارتها بشكل صحيح في الوحدات الاقتصادية كما إنها ليست مجرد مسألة داخلية حيث يرغب أصحاب المصلحة الخارجيون في معرفة المخاطر التي يستثمرون فيها كما تطرق (Sudaryono&others,2022:181)الى أن تطبيق ادارة المخاطر المؤسسية في العديد من الصناعات لاكثر من عقد من الزمان نتيجة للتغيرات في القوانين البيئية والاضطرابات الاقتصادية التي ساهمت في تعقيد المنتجات والادوات والمخاطر المحيطة بها وان الوعي بتلك المخاطر هو المفتاح لممارسات ادارة المخاطر الفعالة والتشجيع على اتخاذ القرارات اكثر جودة ، وقد تضمن اطار Coso مبادئ توجيهية لتنفيذ ادارة تلك المخاطر .

فوائد ادارة المخاطر المؤسسية

توفر ادارة المخاطر في المؤسسات الفوائد الآتية:
(Sudaryono&others,2022:182-183)

- جعل القرارات أسهل وخاصة في الامور المعقدة .
- يساعد على إجراء تقديرات دقيقة للتكلفة .
- إعطاء أهمية وألوية للقرارات المهمة والفعالة .
- إعطاء إشارة للأطراف ذات العلاقة لإحتمالية حدوث المخاطر وجوانب عدم اليقين الذي يعيق تحقيق الاهداف الاستراتيجية .
- توفير أدوات تحليل شاملة والنظر في البدائل المتاحة وكشف وصياغة المشكلة المطروحة .

وذكر (Sitompul,2022:52) بأن الوحدات الاقتصادية تواجه حقيقة دائمة هي أنه اذا أرادت تلك الوحدة تحقيق نتائج كبيرة فإنها تواجه مخاطر أكبر وإذا لم تتم ادارة مخاطرها بشكل صحيح فسوف يتسبب ذلك بخسائر كبيرة للوحدة ولأصحاب المصلحة فيها .

أنواع المخاطر :

يتم تقسيم المخاطر التي قد تواجهها الوحدات الاقتصادية الى الانواع الآتية : (قادري ورحال ، 2020 : 12-13)

- 1- المخاطر الاستراتيجية / وتشمل المخاطر الكبيرة والهامة والمؤثرة على تحقيق الاهداف واتخاذ القرارات .
- 2- المخاطر التشغيلية / وهي مخاطر الخسارة المباشرة وغير المباشرة الناتجة عن فشل أو عدم كفاية العمليات الداخلية والافراد والانظمة أو الاحداث الخارجية .
- 3- المخاطر المالية / وتشمل الخسائر بسبب الظروف الاقتصادية مثل تقلبات الاسعار في صرف العملات الاجنبية وأسعار الفائدة بالإضافة لمخاطر السيولة والسوق .
- 4- مخاطر المعلومات / وهي المخاطر الناجمة عن عدم دعم تكنولوجيا المعلومات لاحتياجات قطاع الاعمال وكذلك المخاطر الناتجة عن عدم توفر معلومات دقيقة وصحيحة تساعد على اتخاذ القرارات سواء كانت متعلقة بالنشاط أو العمل في البيئة الداخلية او الخارجية .

- 5- مخاطر السمعة / والناجمة عن فقدان الشهرة أو العلامة التجارية بسبب الانطباع السلبي المتكون عن الوحدة الاقتصادية الناجم عن سلوكيات غير أخلاقية وغير مقبولة من قبل الإدارة أو العاملين فيها .
- 6- مخاطر قانونية / وتنشأ بسبب عدم الالتزام أو الاخلال بالانظمة والقوانين أو الممارسات المعتمدة في الوحدة الاقتصادية .
- 7- المخاطر الخارجية / تتمثل بالمخاطر الناشئة عن عوامل خارجية كالتغيرات التكنولوجية ، المنافسة ، الاقتصادية ، تغيرات الانظمة والقوانين وغيرها .
- 8- المخاطر الاخرى / وتتعلق بالظروف الطبيعية وبيئة الاعمال والتطورات التكنولوجية المتسارعة والاحداث العرضية .

يتبين مما سبق عرضه أن الغرض من سعي الوحدات الحكومية لإدارة مخاطرها المؤسسية بشكل فعال ليس فقط كونه مسألة داخلية خاصة بها بل قد يرغب أصحاب المصلحة الخارجيون أيضاً في معرفة مخاطر الوحدة التي يستثمرون فيها كون هذه المخاطر قد تكون بيئية أو سوقية وتكون خارج سيطرة تلك الوحدة عندما يكون كفاءة ادارة المخاطر دليلاً هاماً للإدارة وأصحاب المصلحة خارج الوحدة الاقتصادية .

وأشار (Poon.A.,et.al,2022:4) الى أن إدارة المخاطر المؤسسية للمتغيرات الداخلية أكثر أهمية للوحدة الاقتصادية وذلك كونها لديها القدرة على معالجة المتغيرات الداخلية للحصول على مزايا تنافسية التي تؤثر على كفاءة الوحدة الاقتصادية ولاسيما في الوحدات الصغيرة والمتوسطة الذي يحسن من ربحيتها ويخفض من تكلفة تمويلها. يتبين مما سبق أن هناك ترابط بين ادارة مخاطر الوحدات الاقتصادية ولاسيما تلك المخاطر الناجمة عن اعتماد الوسائل الألكترونية الحديثة في أرشفة البيانات والمعلومات الخاصة بالوحدة وإرسال وإستلام الملفات والوثائق السرية والهامة التي تخص تلك الوحدة وبين كيفية الحفاظ عليها من الاختراق والتزوير والتلف من خلال اعتماد وسائل وقائية لمنع حدوث المخاطر والتحوط لها قبل وقوعها وذلك بإعتماد التدقيق الإلكتروني لتلك البيانات والمعلومات و تخزينها في أماكن خاصة يصعب إختراقها أو العبث بها من خلال عمل نسخ احتياطية للرجوع الى المعلومات والوثائق الهامة عند تعرضها للتلف أو التلاعب وعمل رموز سرية للبيانات والمعلومات السرية سواء كانت خاصة بالموظفين أو الوحدة الاقتصادية .

يتجسد ذلك من خلال إنشاء برامج رصينة وتصميم مواقع رسمية يصعب إختراقها وإعتماد وسائل تدقيقية تساعد على إختبار مدى كفاءة وفاعلية تلك البرامج والمواقع الإلكترونية والحفاظ على أمن وسلامة المعلومات فيها وتتبع مسار إدخال المعلومات

وتصريح الدخول إليها وتنصيب برامج التنبيه والحماية من مخاطر الاختراق والتلاعب بالبيانات الخاصة بالوحدة أو فقدانها .

ثالثاً: الجانب العملي للبحث

يتكون مجتمع البحث من موظفي التدقيق الداخلي ، حيث تم توزيع 75 استبانة في قسم الرقابة والتدقيق الداخلي في رئاسة الجامعة المستنصرية من اختصاصات ودرجات وظيفية مختلفة ، كما شملت الدراسة موظفي شعبة التدقيق الداخلي في كلية الآداب وكلية العلوم كما تضمنت العينة موظفي ديوان الرقابة المالية ، وتم قبول 59 منها بعد استرداد 68 استبانة حيث تم رفض 9 منها لعدم تكامل المعلومات فيها .

وان المقياس المستخدم لتحليل البيانات وهو مقياس SPSS 28 الاحصائي ومعاملات الثبات فيه كما يأتي :

أولاً: معاملات الثبات

معامل ألفا كرونباخ	المقياس
0.711	مبادئ إطار COSO المحدث
0.726	مبادئ ومتطلبات دعم الأمن السيبراني
0.818	المجموع

المصدر: إعداد الباحثة بالاعتماد على مخرجات برنامج SPSS 28.

إذ يتبين من الجدول أعلاه أن المتغير المستقل هو مبادئ إطار COSO المحدث في حين يمثل المتغير التابع هو مبادئ ومتطلبات دعم الامن السيبراني ، حيث تم التحقق من ثبات أداة البحث باستخدام معادلة كرونباخ ألفا (Cronbach – Alpha) لقياس الاتساق الداخلي لمتغيرات مجال اذ بلغ ثبات المقياس الكلي 0,818 ويعد هذا الثبات مقبولاً لأغراض هذا البحث .

ثانياً: وصف عينة البحث:

1- متغير الجنس

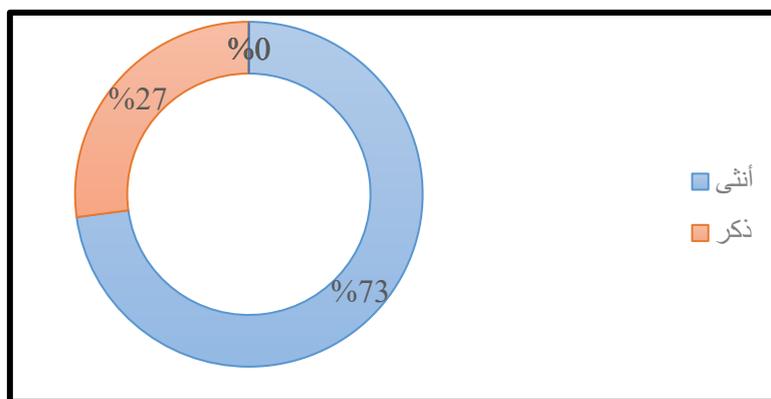
جدول (1)

توزيع افراد عينة الدراسة حسب الجنس

النسبة	العدد	الجنس
72.9%	43	أنثى
27.1%	16	ذكر
100.0%	59	المجموع

المصدر: إعداد الباحثة بالاعتماد على مخرجات برنامج SPSS 28.

يتضح من الجدول رقم (1) أن عدد الاناث في عينة البحث قد بلغ 43 موظفة مايمثل نسبة 73% كما هو موضح في شكل رقم (1) في حين بلغ عدد الذكور 16 فقط والذي نسبته 27% من اجمالي العينة.



شكل (1)

توزيع افراد عينة الدراسة حسب الجنس

المصدر: إعداد الباحثة بالاعتماد على مخرجات برنامج Microsoft Excel 2019

متغير الفئات العمرية

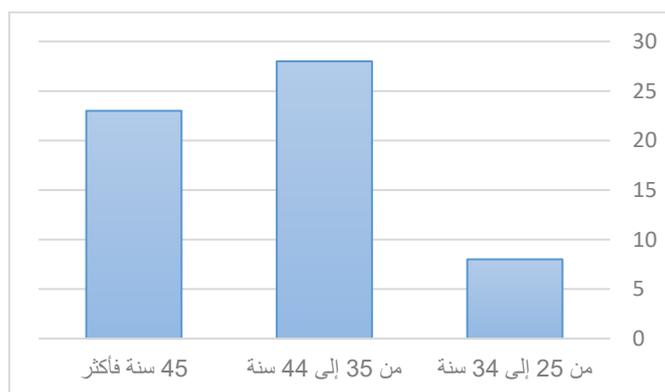
جدول (2)

توزيع افراد عينة الدراسة حسب الفئات العمرية

النسبة	العدد	العمر
13.6%	8	من 25 إلى 34 سنة
47.5%	28	من 35 إلى 44 سنة
39.0%	23	45 سنة فأكثر
100.0%	59	المجموع

المصدر: إعداد الباحثة بالاعتماد على مخرجات برنامج SPSS 28.

يمثل متغير الفئات العمرية الموضح بالجدول رقم (2) توزيع عينات البحث حسب الفئات العمرية المختلفة والذي تبين من خلاله أن معظم هؤلاء الموظفين تتراوح أعمارهم بين 35 و 44 سنة إذ تشكل نسبة 47,5% من مجموع عدد المستجيبين مقارنة بالفئات العمرية الأخرى وذلك بقسمة عدد الموظفين المستجيبين في هذه الفئة نسبة إلى مجموع عدد المستجيبين الكلي ، في حين تبلغ أقل نسبة والبالغة 13,6% للفئات العمرية من 25 إلى 34 سنة وهذا يتضح بالشكل الآتي :



شكل (2)

توزيع افراد عينة الدراسة حسب الفئات العمرية

المصدر: إعداد الباحثة بالاعتماد على مخرجات برنامج Microsoft Excel 2019

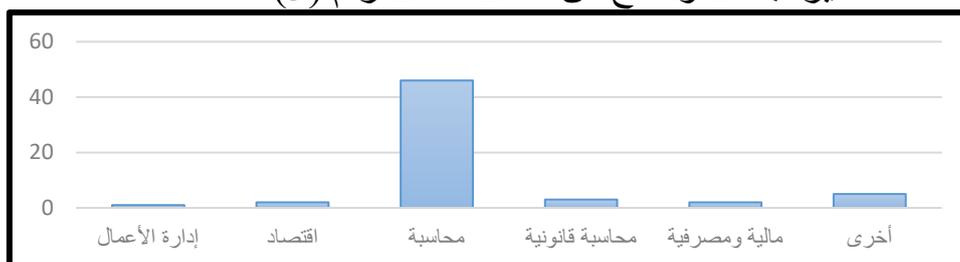
2- متغير التخصص

جدول (3)

توزيع افراد عينة الدراسة حسب التخصص
التخصص العدد النسبة

التخصص	العدد	النسبة
إدارة الأعمال	1	1.7%
اقتصاد	2	3.4%
محاسبة	46	78.0%
محاسبة قانونية	3	5.1%
مالية ومصرفية	2	3.4%
أخرى	5	8.5%
المجموع	64	100.0%

المصدر: إعداد الباحثة بالاعتماد على مخرجات برنامج SPSS 28. وفق متغير التخصص يتوزع افراد العينة على ستة مجاميع يبلغ أعلى نسبة منهم في تخصص المحاسبة إذ بلغ عدد المستجيبين على استبانة البحث 78% من إجمالي العدد الكلي حيث تمثل هذه النسبة 46 مستجيب من أصل 64 وهذا يعطي إنطباعاً عن طبيعة تخصص الموظفين المتواجدين في قسم الرقابة والتدقيق الداخلي في عينة البحث والذي يمكن ملاحظة تأثيره بشكل واضح من خلال الشكل رقم (3)



شكل (3)

توزيع افراد عينة الدراسة حسب التخصص

المصدر: إعداد الباحثة بالاعتماد على مخرجات برنامج Microsoft Excel 2019

المؤهل العلمي

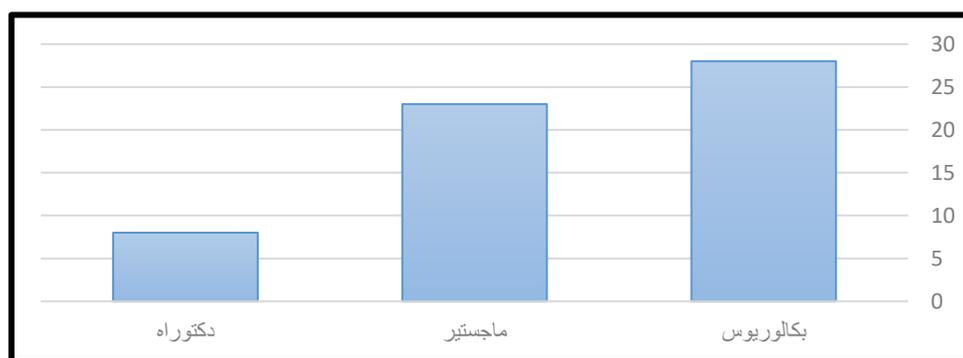
جدول (4)

توزيع افراد عينة الدراسة حسب المؤهل العلمي

النسبة	العدد	المؤهل العلمي
47.5%	28	بكالوريوس
39.0%	23	ماجستير
13.5%	8	دكتوراه
100.0%	59	المجموع

المصدر: إعداد الباحثة بالاعتماد على مخرجات برنامج SPSS 28.

بموجب نتائج متغير المؤهل العلمي لافراد عينة البحث يتم ملاحظة أن الغالبية العظمى لعدد المستجيبين من موظفي قسم الرقابة والتدقيق الداخلي هم من حملة شهادة البكالوريوس اذ بلغت نسبتهم 47.5% من اجمالي العينة ويأتي من بعد ذلك حملة شهادة الماجستير أما حملة شهادة الدكتوراه فتبلغ نسبتهم 13.5% من اجمالي العدد الكلي وذلك يعطي انطباعا عن طبيعة موظفي قسم الرقابة والتدقيق الداخلي المتوفر في عينة البحث ومدى تأثيره في تحقيق فرضية البحث من حيث تطبيق الاساليب الحديثة في أعمال التدقيق الداخلي وتأثيرها في دعم الامن السيبراني في الوحدات الحكومية ويمكن توضيح نسبة المستجيبين وفق مؤشر المؤهل العلمي بالشكل التكراري رقم (4)



شكل (4)

توزيع افراد عينة الدراسة حسب المؤهل العلمي

المصدر: إعداد الباحثة بالاعتماد على مخرجات برنامج Microsoft Excel 2019.

3- العنوان الوظيفي

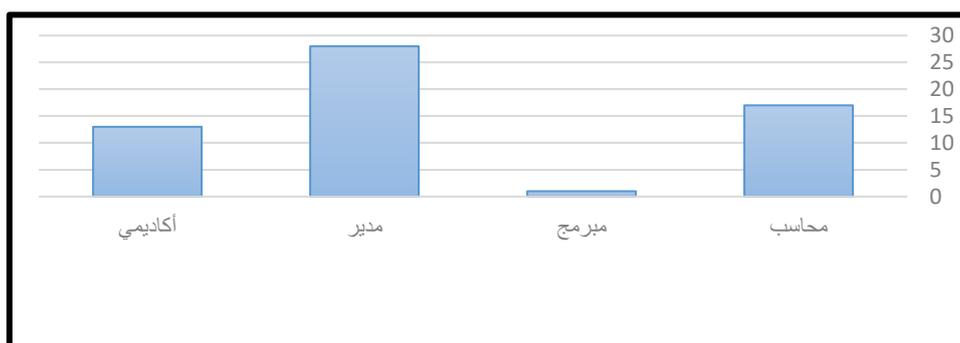
جدول رقم (5)

توزيع افراد عينة الدراسة حسب العنوان الوظيفي

النسبة	العدد	العنوان الوظيفي
28.8%	17	محاسب
1.7%	1	مبرمج
47.5%	28	مدير
22.0%	13	أكاديمي
100.0%	59	المجموع

المصدر: إعداد الباحثة بالاعتماد على مخرجات برنامج SPSS 28.

وفق هذا المتغير يتضح ان من هم بدرجة مدير يمثلون اعلى نسبة من العينة والذي يتضح من خلاله الخبرة الوظيفية التي يتمتع بها موظفوا التدقيق الداخلي في عينة البحث ويولي هذه النسبة من هم بدرجة محاسب اذ بلغت نسبتهم 28,8 % ثم من هم حملة الشهادات العليا (أكاديمي) بينما أقل نسبة 1,7% كانت لمن هم بدرجة مبرمج وهذا يوضح إفتقار أنظمة التدقيق في عينة البحث في الاعتماد على الانظمة الحديثة للتدقيق الالكتروني .



شكل رقم (5)

توزيع افراد عينة الدراسة حسب العنوان الوظيفي

المصدر: إعداد الباحثة بالاعتماد على مخرجات برنامج Microsoft Excel 2019.

ثالثاً: تحليل علاقات الارتباط

1. علاقة الارتباط بين محاور مبادئ COSO ومحاور الأمن السيبراني
جدول رقم (6)

معاملات الارتباط بين محاور مبادئ COSO ومحاور الأمن السيبراني

دعم الأمن السيبراني في ظل المبادئ والمتطلبات			متغيرات الدراسة		
الأمنية	البشرية والمالية والتقنية	الإدارية والتشريعية	مبادئ COSO المتعلقة		
0.415	0.252	0.088	معامل الارتباط	بتقدير المخاطر وإدارتها	
0.001	0.054	0.506	مستوى الدلالة		
0.135	0.318	0.128	معامل الارتباط	بأنشطة الرقابة	
0.307	0.014	0.333	مستوى الدلالة		
0.397	0.311	0.200	معامل الارتباط	بمجال المعلومات والاتصالات	
0.002	0.017	0.129	مستوى الدلالة		
0.558	0.471	0.427	معامل الارتباط	بمجال المتابعة أو المراقبة	
0.000	0.000	0.001	مستوى الدلالة		

المصدر: إعداد الباحثة بالاعتماد على مخرجات برنامج SPSS 28.

نلاحظ من الجدول السابق ما يأتي:

عدم وجود علاقة دالة إحصائياً بين مبادئ COSO المتعلقة بتقدير المخاطر وإدارتها مع دعم الأمن السيبراني في ظل المبادئ والمتطلبات الإدارية والتشريعية وكذلك البشرية والمالية والتقنية، ولكن العلاقة دالة إحصائياً وموجبة بين مبادئ COSO المتعلقة بتقدير المخاطر وإدارتها مع دعم الأمن السيبراني في ظل المبادئ والمتطلبات الأمنية.

عدم وجود علاقة دالة إحصائياً بين مبادئ COSO المتعلقة بأنشطة الرقابة مع دعم الأمن السيبراني في ظل المبادئ والمتطلبات الإدارية والتشريعية وكذلك الأمنية، ولكن العلاقة دالة إحصائياً وموجبة بين مبادئ COSO المتعلقة بأنشطة الرقابة مع دعم الأمن السيبراني في ظل المبادئ والمتطلبات البشرية والمالية والتقنية.

عدم وجود علاقة دالة إحصائياً بين مبادئ COSO المتعلقة بمجال المعلومات والاتصالات مع دعم الأمن السيبراني في ظل المبادئ والمتطلبات الإدارية والتشريعية، ولكن العلاقة دالة إحصائياً وموجبة بين مبادئ COSO المتعلقة بأنشطة الرقابة مع دعم الأمن السيبراني في ظل المبادئ والمتطلبات البشرية والمالية والتقنية وكذلك الأمنية.

وجود علاقة ارتباط دالة إحصائياً وموجبة بين مبادئ COSO المتعلقة بمجال المتابعة والمراقبة مع كل من دعم الأمن السيبراني في ظل المبادئ والمتطلبات الإدارية والتشريعية وكذلك البشرية والمالية والتقنية بالإضافة إلى الأمنية.

2. العلاقة بين مبادئ إطار COSO المحدث ومبادئ ومتطلبات دعم الأمن السيبراني
جدول رقم (7)

معاملات الارتباط بين مبادئ إطار COSO المحدث ومبادئ ومتطلبات دعم الأمن السيبراني

مبادئ ومتطلبات دعم الأمن السيبراني		متغيرات الدراسة
0.625	معامل الارتباط	مبادئ إطار COSO المحدث
0.000	مستوى الدلالة	

المصدر: إعداد الباحثة بالاعتماد على مخرجات برنامج SPSS 28.

ونلاحظ من الجدول السابق وجود علاقة ارتباط موجبة دالة إحصائياً بين مبادئ إطار COSO المحدث ومبادئ ومتطلبات دعم الأمن السيبراني؛ وذلك بسبب أن مستوى الدلالة أقل من مستوى المعنوية 0.05.

رابعاً: تحليل علاقات الأثر

جدول رقم (8)

أثر مبادئ إطار COSO المحدث في مبادئ ومتطلبات دعم الأمن السيبراني

المتغير التابع (مبادئ ومتطلبات دعم الأمن السيبراني)						
R ²	Sig	F	Sig	T	المعامل	المتغيرات المستقلة
39%	0.000	36.457	0.007	2.808	15.090	الثابت
			0.000	6.038	0.418	مبادئ إطار COSO

المصدر: إعداد الباحثة بالاعتماد على مخرجات برنامج SPSS 28.

نلاحظ من الجدول (8) ما يأتي:

هناك أثر دال إحصائياً لمبادئ إطار COSO المحدث في مبادئ ومتطلبات دعم الأمن السيبراني لأن قيم Sig أقل من مستوى الدلالة 0.05.

مبادئ إطار COSO المحدث تفسر 39% من التغيرات الحاصلة في متغير مبادئ ومتطلبات دعم الأمن السيبراني وذلك لأن قيمة معامل التحديد (R²=39%).

رابعاً : الاستنتاجات والتوصيات

الاستنتاجات

استناداً لما سبق عرضه من نتائج التحليل الإحصائي لاستجابات أفراد عينة البحث نستنتج ما يأتي :

هناك تأثير للأنشطة الرقابية المتبعة في وحدات عينة البحث على تحقيق المتطلبات الامنية للحفاظ على البيانات والمعلومات السرية في الوحدات الاقتصادية المختلفة .

يؤيد أفراد عينة البحث من موظفي شعب التدقيق الداخلي في الجامعة المستنصرية ووزارة المالية إتباع أنظمة التدقيق الحديثة في الحفاظ على سلامة وأمن المعلومات والاوليات الهامة والسرية والتحقق من عدم اختراق تلك المعلومات والوثائق والولوج غير المصرح به .

يمثل تطبيق مبادئ COSO المحدث أساساً لدرء المخاطر المؤسسية التي تتعرض لها الوحدات الاقتصادية كالمخاطر التشغيلية لتجنب الخسائر المباشرة وغير المباشرة ومخاطر المعلومات الناجمة عن دعم تكنولوجيا المعلومات بالإضافة للمخاطر المالية الناجمة الخسائر بسبب الظروف الاقتصادية .

من خلال تنوع التخصصات في قسم الرقابة والتدقيق الداخلي في عينة البحث يتبين ضرورة اشراك عناصر تحمل تخصصات تقنية تقوم بتوثيق وأرشفة البيانات واعداد برامج تدقيقية خاصة بكل وحدة للمحافظة على أمن وسلامة المعلومات والاجهزة والمواقع الالكترونية المختلفة .

يوفر إطار COSO لإدارة المخاطر المؤسسية أساسًا يمكنه من بناء برنامج للأمن السيبراني ، ودمج مفاهيم إدارة المخاطر الإلكترونية مع عناصر الاستراتيجية وأهداف العمل والأداء ، والتي يمكن أن تؤدي إلى زيادة قيمة الأعمال.

التوصيات

توصي الباحثة بما يأتي :

ضرورة اتباع أنظمة تدقيق حديثة وأنشطة تساهم في حماية الوحدات الاقتصادية من مخاطر اختراق البيانات أو ضياعها وتعرضها للتلف وحمايتها من التلاعب والتزوير .

تطوير الكوادر الرقابية من خلال إشراكها بدورات تتضمن اعتماد التدقيق على أنظمة حاسوبية متطورة وتزويد هذه الوحدات ببرامج تدقيقية خاصة للمحافظة على سرية المعلومات وحمايتها من التزوير والتلاعب .

ضرورة الدمج بين الأنشطة الرقابية التقليدية والحديثة للتوصل الى أفضل النتائج لضمان أرشفة المعلومات والتعامل معها بشكل آمن والحفاظ على سلامة الاجهزة الحاسوبية وأجهزة الاتصال من الاختراق والتلف .

يمكن للوحدات الاقتصادية المختلفة أن تكون مستعدة بشكل أفضل لإدارة المخاطر السيبرانية في هذا العصر الرقمي من خلال تطبيق مبادئ COSO المحدث في الأنشطة الرقابية المتبعة في تلك الوحدات .

المصادر

المصادر العربية :

- 1- قادري، زين الدين و رحال، مهدي معمر (2020)، "دور التدقيق الداخلي في تقييم إدارة المخاطر وفق إطار COSO"، رسالة ماجستير محاسبة وتدقيق، جامعة قاصدي مرباح، ورقلة - الجزائر .
- 2- منشور مستشارية الامن الوطني "استراتيجية الامن السيبراني العراقي"، أمانة سر اللجنة الفنية العليا لأمن الاتصالات والمعلومات، بدون سنة، 1-10 .
- 3- العموش، آية والطراونة، اخليف، (2022)، "واقع القيادة الافتراضية في الجامعات الاردنية بالاستناد الى أسس الادارة الالكترونية"، المجلة العلمية لكلية التربية - جامعة اسيوط، المجلد الثامن والثلاثون، العدد السابع، يوليو، (ص: 1-30).
- 4- الصانع، نورة والسواط، حمد وأبو عيشة، زاهدة و سليمان، إيناس وعسران، عواطف، (2020)، "وعي المعلمين بالامن السيبراني وأساليب حماية الطلبة من مخاطر الانترنت وتعزيز القيم والهوية الوطنية لديهم"، المجلة العلمية لكلية التربية، جامعة اسيوط، المجلد السادس والثلاثون - العدد السادس، يونيو .
- 5- كاظم، تيسير جواد و نصيف، أحمد حسين (2019)، "العلاقة بين حوكمة الشركات وادارة مخاطر مشروع ال (ERM) دراسة استطلاعية لآراء عينة من الاكاديميين والمهنيين"، مجلة كلية الادارة والاقتصاد م جامعة الكوفة، العدد (54)، ص (619 - 667) .
- 6- الجوهر، كريمة علي و العبيدي، أحمد جاسم، (2019)، "إنموذج مقترح لاستمارة فحص الرقابة الداخلية في ضوء مبادئ إطار COSO المتكامل المُحدث " بحث منشور ، ص (41 - 48)
- 7- بدوي، عبد السلام خميس، (2011)، "أثر هيكل نظام الرقابة الداخلية وفقاً لإطار COSO على تحقيق أهداف الرقابة"، دراسة حالة المنظمات الاهلية في قطاع غزة، رسالة ماجستير في المحاسبة والتمويل، كلية التجارة الجامعة الاسلامية / غزة .
- 8- المنيع، الجوهرة بنت عبد الرحمن، (2022) "متطلبات تحقيق الأمن السيبراني في الجامعات السعودية في ضوء رؤية 2030"، جامعة الأميرة نورة بنت عبد الرحمن، جامعة أسيوط، المجلة العلمية، المجلد 38، العدد الأول - يناير 2022 م، ص (156 - 194)

المصادر الاجنبية

- 1- Poon A.,Roslan N.,Othman J.,Anuar A.,Nejad M.,(2022),”The Effect of Enterprise Risk Management (ERM)Implementation onSMEs Performance in Malaysia”,Malaysian Journal of Social Sciences and Humanities (MJSSH),Vol 7,Issue 4,P:1-13.
- 2- Sitompul S.,(2022),”FACTOR ENTERPRISE RISK MANAGEMENT PADA INDUSTRI BARANG KONSUMSI DI BEI”Sintaksis:Jurnal Ilmiah Pendidikan,Vol2 No 2Juni,p:52-61.
- 3- Sudaryono D.,Sudibyoy Y.,Sadaryono B.,(2022)”DETERMINANTS OFENTERPRISEMANAGEMENT(ERM)EFFECTIVENESS”,Jurnal Akuntansi Trisakti ,Vol 9 NOMOR,2 SEPTEMBER,p :179-204.
- 4- Backman,Sarah,(2022),”Risk vs. threat-based cybersecurity:the case of the EU”,European Security ISSN:Print online Journal homepage:p:1-19.
- 5- Ghelani,Diptiben,(2022),”Cyber Security,Cyber Threats,Implications and Future Perspectives:A Review”,American Journal of Science,Engineering and Technology,Vol.3,No.6,pp12-19.
- 6- Cook,Kimberly,(2017),”Effective Cyber Security Strategies for Small Businesses”, Doctor of Business Administration,Waden University.
- 7- Antonio,Rossella D.,(2021),”The WorldCom fraud under the COSO framework analysis”,Universita Ca foscari Venezia.thesis and Dissertations
- 8- Mulyandani,Vina Citra,(2022),”Evaluation Internal Control System of Cash Spending Based on the Framework COSO”,International Journal of Arts and Social Science , ISSN:2581-7922,vol 5,Issue 10,Oct.p (21-29).