المجلة العراقية للبحوث الانسانية والاجتماعية والعلمية
Iraqi Journal of Humanitarian, Social and Scientific Research
Print ISSN 2710-0952 Electronic ISSN 2790-1254
العدد 12 A آذار 2024
No.12A March 2024

تأثير الأمن السيبراني على فاعلية نظام الرقابة الداخلية (نموذج مقترح)

د. أسامة زيد محمد منوخ
كلية الإمام الأعظم الجامعة – قسم المالية والمصرفية

المستخلص

هدف البحث إلى توضيح اهمية الامن السيبراني من خلال تأثيره على الرقابة الداخلية وقيمة الوحدة الاقتصادية، وذلك من خلال بناء نموذج مقترح على وفق مقاييس عالمية من شأنه أن يعزز الأمن السيبراني لزيادة فاعلية عمل الرقابة الداخلية، وقد توصل البحث عدة استنتاجات كان أهمها ، إن النموذج المقترح للأمن السيبراني يعزز فعالية نظام الرقابة الداخلية عن طريق تعزيز الحماية وتقليل المخاطر الإلكترونية، مما يساهم في تعزيز الأداء العام للشركة أو المؤسسة واستدامتها في البيئة التقنية المعقدة والمتغيرة باستمرار، وكذلك بين النموذج المقترح بأن إدارة الأمن السيبراني تتطلب توجهاً شاملاً يشمل التواصل الفعال، والتعاون، والتحسين المستمر، والتفاعل السريع مع التهديدات المتغيرة، وقد أوصى البحث ضرورة تحديث وتطوير سياسات الأمن السيبراني وضمان تطبيقها بشكل صارم للحماية ضد التهديدات الجديدة والمتطورة. وينبغي الاستثمار في أدوات الأمن السيبراني المتقدمة مثل أنظمة الكشف عن التسلل وحلول إدارة الهوية والوصول لتعزيز الحماية، وأيضاً تقييم ومراجعة نظام الأمن السيبراني بشكل دوري للكشف عن النقاط الضعيفة وتحسين الإجراءات وفقًا لذلك.

الكلمات المفتاحية : الامن السيبراني / الرقابة الداخلية

The impact of cybersecurity on the effectiveness of the internal control system (proposed model)

Dr. Osama Zaid Muhammad Manoukh
Imam Al-A'zam University College - Department of Finance and Banking

Abstract

The research aimed to clarify the importance of cybersecurity through its impact on internal control and the value of the economic unit, by building a proposed model according to global standards that would enhance cybersecurity to increase the effectiveness of internal control work. The research reached several conclusions, the most important of which was that the proposed model Cybersecurity enhances the effectiveness of the internal control system by enhancing protection and reducing electronic risks, which contributes to enhancing the overall performance of the company or institution and its sustainability in the complex and constantly changing technical environment, as well as the proposed model that cybersecurity management requires a comprehensive approach that includes effective communication, cooperation, and improvement. Continuous, rapid reaction to changing threats, research has recommended the need to update and develop cybersecurity policies and ensure their strict application to protect against new and evolving threats. Invest in advanced cybersecurity tools such as intrusion detection systems and identity and access management solutions to enhance protection, and also periodically evaluate and review the cybersecurity system to detect weak spots and improve procedures accordingly.

Keywords: cybersecurity, internal control

مقدمة

لقد حددت تقرير مخاطر الأعمال المتوقعة الصادر عن معهد المدققين الداخليين الأمريكي خطراً يهدد منظمات الأعمال بمختلف أنواعها وأحجامها، ويأتي في مقدمتها مخاطر الأمن السيبراني، حيث تتزايد بشكل مستمر الهجمات السيبرانية المتنوعة والمعقدة وتحلق أضراراً بالغة بالعلامات التجارية وسمعة منظمات الأعمال، وينتج عن هذه الأضرار آثار مالية هائلة، واشار المعهد الوطني للمعايير والتكنولوجيا (NIST) إلى أن المخاطر السيبرانية تؤثر على صافي أرباح المنظمات ، حيث يمكن أن تؤدي إلى زيادة التكاليف وتخفيض الإيرادات، كما أنها قد تضر بقدرة المنظمة على الابتكار واكتساب الزبائن والحفاظ عليهم، فضلاً عن أن الأمن السيبراني يمكن أن يكون أحد المكونات الأساسية والهامة لإدارة المخاطر الشاملة.

ومن هنا تتأتى أهمية النماذج والأطر التي وضعتها المنظمات المهنية المعنية بالرقابة الداخلية ، كونه أطار مرجعي عالمي يمكن اعتماده في أي بيئة لدوره في تعزيز الرقابة الداخلية، ومن ثم المساهمة في إضفاء المصداقية على القوائم المالية. أن النموذج المقترح، يمكن أن يساعد الوحدات الاقتصادية من خلال زيادة فاعلية الرقابة الداخلية لإدارة تكنولوجيا المعلومات بشكل افضل لحل المشاكل الجديدة والناتجة عن استخدام تكنولوجيا المعلومات في عملياتها، وان وجود المخاطر الخاصة بأمن الحاسوب يستدعي توفير الدرجة المناسبة من امن المعلومات للحماية الالكترونية لأنظمة المعلومات بحيث نضمن ان تكنولوجيا المعلومات تساعد الوحدة الاقتصادية على تحقيق استراتيجياتها وبالتالي تحقيق اهدافها.

المبحث الأول

منهجية البحث

1- مشكلة البحث

يصاحب التطورات التقنية الحديثة المتسارعة مخاطر تتعرض لها الوحدات الاقتصادية التي بدورها تهدد امن المعلومات واغلب الانظمة والبرامج على شبكات الانترنيت، وهذا يتطلب الى وجود صمام امان لمواجهة تلك المخاطر والتي تتمثل بالأمن السيبراني الذي يعزز الرقابة الداخلية لتلك الوحدات، لذا يمكن صياغة مشكلة البحث كالآتي:-

- هل يدرك العاملون و يمتلكون المعرفة المهنية لتطبيق الاطر الحديثة لرقابة تقنية المعلومات والامن السيبراني؟
- هل يعزز الامن السيبراني قيمة الوحدة الاقتصادية من خلال تأثيره في الرقابة الداخلية؟

2- أهمية البحث

ان الاستخدام المتزايد لتكنولوجيا المعلومات في المجالات المحاسبية والمالية ادى الى زيادة الاهتمام بالأمن السيبراني والرقابة الداخلية على نظم المعلومات الالكترونية، وتنبع اهمية البحث من الاهمية التي يحظى بها كلا من الامن السيبراني والرقابة الداخلية على قيمة الوحدة الاقتصادية في ظل الاعتماد على الاطر الحديثة للرقابة الداخلية مما يتطلب التعرف على مفهوم الامن السيبراني ومتطلباته من خلال الحصول على مؤشرات تساعد على فهم الامن السيبراني في الرقابة الداخلية، وهذا ما تنطوي عليه اهمية البحث من تكاملية بالإجراءات والخصائص التي تحقق الاطر الحديثة للرقابة الداخلية في ظل التطورات الحديثة في بناء نموذج مقترح.

3- هدف البحث

يهدف البحث الى تحقيق الاتي:

أ- توضيح اهمية الامن السيبراني من خلال تأثيره على الرقابة الداخلية وقيمة الوحدة الاقتصادية.

ب- بيان نظري لتعزيز الرقابة على امن المعلومات بالاعتماد على الاطر الحديثة للرقابة الداخلية من خلال تكاملية الاجراءات والخصائص في ظل الاطر الحديثة.

4- فرضية البحث

يسعى البحث إلى فرضية رئيسية مفادها (أن تطبيق النموذج المقترح على وفق مقاييس عالمية من شأنه أن يعزز الأمن السيبراني لزيادة فاعلية عمل الرقابة الداخلية).

المبحث الثاني
مدخل مفاهيمي للأمن السيبراني

أولا: مفهوم الأمن السيبراني

يعد الأمن السيبراني من المفاهيم التي لاقت اهتماماً كبيرا في الآونة الأخيرة نظراً لظهور تقنيات وأدوات تكنولوجية جديدة واستخدامها بشكل واسع في كافة أنشطة معظم الشركات ، وقد عرفت دراسة (NIST, 2018: 12) الأمن السيبراني بأنه حماية الأصول المعلوماتية من خلال معالجة التهديدات التي تتعرض لها المعلومات التي تتم معالجتها وتخزينها ونقلها بواسطة أنظمة المعلومات المتداخلة بين الشبكات.

كما عرفته دراسة (ISACA, 2017 :57) بأنه عملية حماية مواقع تخزين البيانات والتقنيات المستخدمة لتأمينها كما يتضمن حماية تكنولوجيا المعلومات والإتصالات والأجهزة والبرمجيات .

وطبقا لما ورد في التقرير الصادر عن الاتحاد الدولي للاتصالات بشأن الامن السيبراني حول اتجاهات الإصلاح في الإتصالات للعام 2022 – 2023 حيث يمثل مجموعة من المهمات مثل تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية ومقاربات لإدارة المخاطر وتدريبات وممارسات فضلي وتقنيات يمكن إستخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين. (Florakis et al., 2023: 19)

وقد أكد (البغدادي ، 2021 ، 46) أن السيبراني يمثل النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات ويضمن إمكانات الحد من الخسائر والإضرار التي تترتب في حال تحقق المخاطر والتهديدات كما يتيح إعادة الوضع إلى ما كان عليه بأسرع ما يمكن بحيث لا تتوقف عجلة الإنتاج وبحيث لا تتحول الإضرار إلى خسائر دائمة .

أما (Eaton & Grenier, 2022: 102) فقد عرفه على أنه " هو مصفوفة من الأدوات التنظيمية والتقنية والإجرائية، والممارسات الهادفة إلى حماية الحواسيب والشبكات وما بداخلها من بيانات من الاختراقات أو التلف أو التغيير أو تعطل الوصول للمعلومات أو الخدمات، ويعد توجها عالميا سواء على مستوى الدول أو حتى المنظمات الحكومية أو الشركات.

ويرى الباحث وبناء على ما سبق أن الامن السيبراني يمثل عملية حماية المعلومات من خلال معالجة التهديدات التي تتعرض لها هذه المعلومات التي تتم معالجتها و تخزينها ونقلها بواسطة انظمة المعلومات المتداخلة بين الشبكات ، كما يؤكد الباحث على أن الأمن السيبراني يمتد ليشمل جميع المجالات الاقتصادية والاجتماعية والسياسية والقانونية لكافة المجتمعات المعاصرة ، كما أنه يرتبط إرتباطا وثيقا بسلامة مصادر الثروة والتقدم في الوقت الراهن والتي تشمل القدرة على الاتصال والتواصل والبيانات والمعلومات التي يستند عليها الإنتاج والإبداع والقدرة على المنافسة .

ثانيا: طبيعة المخاطر السيبرانية

في عالم يشوبه الكثير من التعرض للمخاطر على جميع المستويات وتزايد حدة اشكال الحرب السيبرانية تحتاج بيئة الأعمال إلى تكييف أدواتها في الحد من مخاطر الأمن السيبراني والاستجابة لها في مراحل مختلفة وأصبحت التغيرات والتحسينات التي تأتي مع التكنولوجيا الجديدة والابتكار واعتمادها من قبل الشركات أكثر تعقيدا عما سبق .

وفي سياق ذلك يتطلب الأمر بداية التعرف على طبيعة الجريمة السيبرانية التي تشكل الخطر الأساسي الواجب مكافحته واستنادا إلى مبدأ لا جريمة ولا عقاب دون نص عمدت العديد من الدول إلى وضع نصوص قانونية خاص بهذه الجرائم التي يمكنها أن تشمل قطاع واسع من الأعمال غير الشرعية كتلك التي تستخدم

أجهزة الكمبيوتر والشبكات كوسيلة لتنفيذ الجريمة أو كهدف لها بدءا من عمليات اختراق الأنظمة المعلوماتية وأنظمة الاتصالات وصولا إلى الهجمات التي تعطل الخدمات. (Florakis et al., 2023: 25)

وبناء على ما سبق فقد أكدت دراسة (Hartmann& Carmenate, 2021 : 128)، بأن المخاطر السيبرانية يقصد بها المخاطر التشغيلية على أصول المعلومات والتكنولوجيا التي لها عواقب تؤثر على سرية وسلامة ونظم المعلومات ومقارنة بفئات المخاطر التي يغطيها التأمين فإن المخاطر السيبرانية تتفق من حيث الخصائص والمسئولية مع مخاطر كل من الممتلكات والخصوم وكذلك المخاطر الكارثية والتشغيلية ، ومما لاشك فيه أن تكنولوجيا المعلومات والاتصالات تتيح إمكانات هائلة وغير مسبوقة لإنتاجية أفضل في جميع القطاعات وللتواصل عبر القارات إلا أن البنية التحتية لهذه التقنيات تمثل ارتباطاً بين مصالح متعددة وخدمات مختلفة ودول عديدة الأمر الذي يجعل من الأخطار في المجال السيبراني أخطار عالمية فلا يمكن لأي جهة أن تضمن بقاءها في منأى عن الأخطار ما دامت سلامة الأخرين معرضة للخطر

.

ثالثا: أنواع المخاطر السيبرانية

أن الهجمات السيبرانية تضم ثلاث أنواع يمكن بحسب الآتي:

(Shahimi & Mahzan, 2022: 212)

1. **مخاطر سيبرانية تتعلق بالسرية :** حيث تنشأ عندما يتم الكشاف عن المعلومات الخاصة داخل المنشأة إلى أطراف ثالثة كما في حالة حدوث اختراق البيانات مثل:

- اختراق أنظمة الكمبيوتر والشبكات للوصول إلى المعلومات السرية، مثل البيانات الشخصية، أو المعلومات الحساسة للشركات.
- البرمجيات الخبيثة مثل الفيروسات وأحصنة طروادة وبرامج التجسس التسبب في تسريب البيانات السرية أو سرقتها.
- الهجمات بواسطة الفدية من أخطر التهديدات، حيث يتم تشفير ملفات الضحية ويتم الابتزاز لفك تشفيرها بدفع فدية مالية.

2. **مخاطر سيبرانية تتعلق بالنزاهة :** والتي تتعلق بإساءة استخدام الأنظمة كما هو الحال بالنسبة للاحتيال، و من بين هذه المخاطر:

- يُمكن تغيير أو تعديل البيانات بطرق إلكترونية دون رصد، مما يؤثر على مصداقيتها ويؤدي إلى فقدان النزاهة.
- قد يؤدي اختراق الأنظمة الإلكترونية إلى تغيير البيانات أو سرقتها، مما يؤثر على دقتها ويخلق تشكيكًا في صحتها.
- هناك هجمات مستهدفة تهدف إلى الأفراد أو المؤسسات بهدف تدمير السمعة أو تشويه الصورة العامة، مما يؤدي إلى فقدان النزاهة والثقة في المعلومات المتعلقة بهم.

3. **مخاطر سيبرانية تتعلق باستمرارية الأداء :** والتي تتلخص في تعطل أو التوقف عن ممارسة الأعمال، وهناك بعض هذه المخاطر:

- يمكن أن تشمل مخاطر السيبرانية العمليات الداخلية غير المصرح بها أو الاستخدام غير القانوني للمعلومات، والتي يمكن أن تتسبب في توقف الخدمات أو تقليل استمراريتها.
- تصيب البرمجيات الضارة الأنظمة والبرمجيات، مما يؤدي إلى توقف أو تشويش في الأداء الطبيعي للأنظمة.

ويرى الباحث أن هذه الأنواع الثلاثة من المخاطر السيبرانية لها تأثيرات مباشرة ومختلفة على الأهداف حيث يؤده تعطل الأعمال إلى المنع من العمل مما ينتج عنه خسارة في الإيرادات بالنسبة للمنشآت أو تعطل في تحقيق الأهداف بالنسبة للأفراد كما يؤدي الاحتيال إلى خسائر مالية مباشرة في الوقت الذي يستغرق التحقيق في تأثيرات اختراق البيانات وقتا أطول الأمر الذي ينتج عنه أضرار معنوية تمس السمعة وفضلاً عن تكاليف التقاضي وبصفة عامة فإن خطر فقدان الثقة في أعقاب الهجمات الإلكترونية قد يكون عاليا

بالنسبة للقطاع المالي بالنظر إلى اعتماد المؤسسات المالية على ثقة عملائها مما يؤثر على قرارات المستثمرين .

لقد حددت دراسة (Wolden & Valverde, 2015: 214)، عدة أهداف للأمن السيبراني والتي تمثل المتطلبات الأساسية المتمثلة بسرية المعلومة المبنية على الممارسات والمعايير وتكاملية وسلامة المعلومة لتقليل المخاطر السيبرانية على الاصول المعلوماتية والتقنية لكافة الجهات من التهديدات الداخلية والخارجية مما يعني توافر المعلومة عند الحاجة اليها وتتحقق الاهداف في حال توافر عدة محاور تعتبر اساسية للحفاظ على امن المعلومات وتشمل المحاور:

1. **التكنولوجيا :** وهي ادوات الأمن اللازمة لحماية الانظمة من الهجمات الالكترونية المحتملة.
2. **الاشخاص :** متمثلة بالأشخاص والمنظمات من مستخدمي المعلومات والانظمة والبرامج.
3. **الانشطة والعمليات:** مجموعة من الاجراءات يتم من خلالها توظيف الأشخاص والتقنيات للقيام بالعديد من العمليات والأنشطة التي من شأنها التصدي للهجمات الالكترونية.

ويرى الباحث أن الامن السيبراني يشكل مجموعة من الاطر القانونية والتنظيمية واجراءات سير العمل بالاضافة الى الوسائل التقنية والتكنولوجية التي تهدف الى حماية الفضاء السيبراني، مع التركيز على ضمان توافر الحماية والسرية لتلك المعلومات.

المبحث الثالث

نظام الرقابة الداخلية

أولا: مفعوم نظام الرقابة الداخلية

تطور تعريف الرقابة الداخلية في وقتنا الحالي عما كان عليه في الماضي إذ اتسع نطاق هذه الرقابة وتشعبت اهدافها ، وقد كانت الرقابة الداخلية تهدف في بدايتها الى وضع مجموعة من الوسائل لمراقبة حركة النقدية والتقليل من الاخطاء والغش وحماية الاصول والموجودات، أما فقد أصبحت مفهوماً إدارياً شاملة، بمعنى أن الرقابة عنصر من عناصر نشاط الإدارة ، ويقسّم هذا النشاط الى أربعة عناصر : (KPMG, 2020: 55)

1. التخطيط ، ويشمل تحديد الأهداف ورسم السياسات ووضع البرامج والخطط .
2. التنظيم ، ويشمل تصميم الهيكل التنظيمي وتنمية الهيئة الإدارية .
3. التوجيه، ويشمل إرشاد المرؤوسين في تنفيذ أعمالهم .
4. الرقابة ، وتشمل التأكد من أن العمل المنجز يطابق ما متوقع أن يكون عليه ،وتحديد المعايير الرقابية وقياس النتائج وتحديد الإنحرافات .

وفيما يخص الرقابة الداخلية فقد صدرت عن اللجان والمنظمات والمعاهد المهنية المتخصصة في مجالات المحاسبة والتدقيق العديد من التعاريف التي تناولت مفهوم وأهداف الرقابة الداخلية ،ولعلّ أهم هذه التعاريف الاتي :-

عرفت نشرة معايير التدقيق رقم (1) الصادرة عن المعهد الامريكي للمحاسبين القانونيين AICPA الرقابة الداخلية بأنها "الخطة التنظيمية وكافة الطرق والاساليب التي تتبعها المؤسسة من أجل حماية أصولها ، والتأكد من دقة وإمكانية الاعتماد على بياناتها المحاسبية ، وتنمية الكفاءة التشغيلية وتشجيع الالتزام بالسياسات الادارية " (Saidin & Badara, 2013: 59)

وعرف معهد المحاسبين القانونيين في انكلترا وويلز ICAEW نظام الرقابة الداخلية على أنه "نظام يتضمن مجموعة عمليات مراقبة مختلفة مالية وتنظيمية ومحاسبية وضعتها الادارة ضمانا لحسن سير العمل في الوحدة الاقتصادية ، وتشمل نظام الضبط الداخلي والتدقيق الداخلي ورقابة الموازنة ووسائل أخرى مثل التكاليف المعيارية والتقارير الدورية "(Moeller, 2014: 2)

كما عرفت لجنة (COSO) المنبثقة عن لجنة المنظمات الراعية المعروفة بلجنة تريدواي Treadway الرقابة الداخلية بأنها : " عملية تنتج وتتأثر بمجلس ادارة الوحدة الاقتصادية وأدارتها وأفراد آخرين وتكون مصممة لتعطي تأكيداً معقولاً بخصوص تحقيق الاهداف في المجالات الاتية " : (Arens, 2018:144)

1- مقدار فعالية الاعمال وكفاءتها .
2- إمكانية الاعتماد على التقرير المالي .
3- الالتزام بالقوانين والانظمة المطبقة .

أما هيئة المعايير الرقابية (COCO) التابعة للمعهد لكندي للمحاسبين القانونيين (CICA) فعرفت الرقابة الداخلية بأنها : " العناصر الموجودة في الوحدة الاقتصادية والتي تتضمن المصادر ،الأنظمة ،العمليات ،الثقافة، والهيكل التي تدعم مجتمعة الأفراد في تحقيق أهداف الوحدة الاقتصادية " وهذه الأهداف تضم العناصر الآتية : (اليوسف، 2020: 65)

1- فاعلية وكفاءة عمليات الوحدة الاقتصادية .
2- المصداقية في التقارير الداخلية والخارجية .
3- الالتزام بالقوانين والأنظمة والسياسات الداخلية .

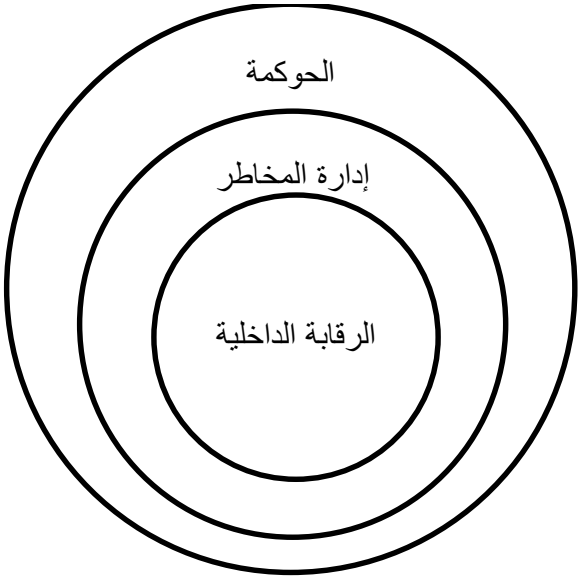
وعرفت المنظمة الدولية للأجهزة العليا للرقابة المالية INTOSAI الرقابة الداخلية بأنها " نظام شمولي للرقابة المالية أو غيرها من أنواع الرقابة بما تشمله من هيكل تنظيمي وأجراءات مالية داخلية ، أنشأتها الادارة ضمن أهدافها المحددة للمساعدة في عملية القيام بادارة أعمال الوحدة الاقتصادية بأسلوب منظم واقتصادي وفاعل وكفوء بحيث يضمن الالتزام بسياسات الادارة ويؤمن صحة السجلات المحاسبية وتقديم معلومات ادارية ومالية في حينها " .(حجازي، 2021: 69)

ويرى الباحث ومن خلال إستعراض التعاريف السابقة ، يمكن التوصل إلى أن نظام الرقابة الداخلية (نظام يتم إنشاؤه من قبل الإدارة تتم ممارسته من قبل كل المستويات داخل الوحدة الاقتصادية بصورة عملية من أجل تحقيق أهداف الوحدة الاقتصادية المتمثلة في حماية أصولها ، والتأكد من دقة وأمكانية الاعتماد على بياناتها المحاسبية ، وتنمية الكفاءة التشغيلية وتشجيع الالتزام بالسياسات الادارية والتي تسعى الإدارة الى تحقيقها بإستمرار عبر تطبيق النظام وتطويره وبما يتناسب مع التغيرات في بيئة الأعمال) .

ثانيا: أهمية الرقابة الداخلية للوحدات الاقتصادية

تعد الرقابة الداخلية الفاعلة (Effective) واحدة من أفضل الدفاعات ضد فشل الوحدات الاقتصادية ، إنّ الرقابة الداخلية هي محرك مهم لأداء الأعمال ، وإدارة المخاطر ، ويمكنها من إنشاء والحفاظ على قيمة الوحدة الاقتصادية ، وإنّ الرقابة الداخلية جزء لا يتجزأ من نظام الحوكمة والذي يمكن من إدارة المخاطر ، التي يتم فهمها وتفعيلها ومراقبة انشطتها من قبل مجلس الإدارة والإدارة ، وغيرهم من الموظفين العاملين في الوحدة للاستفادة من الفرص ومواجهة التهديدات لتحقيق أهداف الوحدة الاقتصادية بكفاءة. Moeller, (2014: 2)

الشكل (1)
الوحدة الاقتصادية والعلاقة بين الحوكمة وإدارة المخاطر والرقابة الداخلية



Moeller R. Robert, Executive's Guide to COSO Internal Controls Understanding and Implementing the New Framework, John Wiley & Sons, 2014: 2.

ويظهر من الشكل أعلاه أنّ الحوكمة تحيط بجميع الأنشطة في الوحدة الاقتصادية، وقد يكون إنشاء هيكل للحوكمة ليقابل الامتثال للقوانين واللوائح في البيئة التي تعمل فيها الوحدة والتي عادة ما يتم إصدار هذه القوانين واللوائح لحماية مصلحة الجمهور فضلا عن ذلك ، يجوز لمجلس إدارة الوحدة وإدارتها إنشاء هياكل حوكمة للوفاء باحتياجات أصحاب المصلحة الرئيسين، وأن الوحدة الاقتصادية تعمل ضمن الحدود والقيم التي تم وضعها من قبل مجلس الإدارة والإدارة العليا. (Kurt & et. al, 2009: 3-1)

إنّ إدارة المخاطر هي الطبقة الثانية في هيكل الحوكمة، وتهدف إدارة المخاطر إلى (Kurt & et. al, 2009: 3-2) :

(1) تحديد وتخفيف المخاطر التي تؤثر سلباً في نجاح الوحدة الاقتصادية.

(2) استغلال الفرص التي تمكن من إدارة النجاح بواسطة تطوير استراتيجيات حول كيفية إدارة المخاطر والضوابط الرئيسة، وينبغي أن تعمل أنشطة إدارة المخاطر ضمن التوجيه العام لهيكل الحوكمة.

كما يبيَّن الشكل السابق أنّ الرقابة الداخلية جزء من عملية إدارة المخاطر ومكون أساسي في الحوكمة ، إذ إنّ الرقابة الداخلية تشكل عنصراً حاسماً في نظام الحوكمة والقدرة على إدارة مخاطر الوحدة ، وكذلك عنصر أساسي في تحقيق أهداف الوحدة وإنشاء وتعزيز وحماية قيمة اصحاب المصلحة ، إذ إنّ الفشل يؤدي عادة إلى فرض قواعد ومتطلبات إضافية ، فضلاً عن الوقت الطويل والكلفة العالية للجهود اللاحقة اللازمة للامتثال. وهذا يؤكد على حقيقة لا يمكن حجبها أن نوع الرقابة الداخلية الصحيح يمكن الوحدة من الاستفادة من الفرص، في حين أن موازنة التهديدات يمكن أن يوافر الوقت والمال، وإنشاء وتعزيز والحفاظ على القيمة. وتنشأ الرقابة الداخلية الفاعلة أيضاً ميزة تنافسية، لأن الوحدة الاقتصادية التي لديها رقابة فاعلة يمكن أن تتحمل مخاطر إضافية، والرقابة الداخلية هي عملية تحاول من خلالها الوحدة تقليل احتمال حدوث أخطاء تتعلق بالمحاسبة ، والمخالفات، والأعمال غير المشروعة. إنّ الرقابة الداخلية تساعد على حماية الأموال . وتوافر إدارة كفؤة وفاعلة للأصول، والسماح بصحة معالجات المحاسبة المالية وسجلاتها. والرقابة الداخلية لا يمكنها القضاء على جميع الأخطاء والمخالفات، لكنها يمكن أن تنبه الإدارة للمشكلات المحتملة (Moeller:2014: 2-3)

ويرى الباحث أن تصميم الرقابة الداخلية بكفاءة وفاعلية يساعد الوحدة الاقتصادية في حماية أصولها من الفقدان أو سوء الاستخدام. وضمان أن تكون المعاملات مصرح بها بشكل سليم ، ودعم إدارة نظم تقنية المعلومات بشكل جيد ، وأن تكون المعلومات الواردة في التقارير المالية موثوق بها.

ثالثا: **مكونات الرقابة الداخلية على وفق إطار (COSO)** ***المحدث***

تشمل الرقابة الداخلية على وفق إطار COSO على خمسة مكونات يتم تصميمها وتنفيذها من قبل الإدارة لتوفير تأكيد معقول على تحقيق أهداف الرقابة، وهذه المكونات تظهر في الجدول (1) وهي: (لطفي، 2017: 67)

أ. بيئة الرقابة (Control Environment)
ب.تقدير المخاطر (Risk Assessment)
ج. أنشطة الرقابة (Control Activities)
د. المعلومات والتوصيل (Information & Communication)
ه. المتابعة (السيطرة) (Monitoring)

الجدول (1)
مكونات الرقابة الداخلية للجنة (COSO)

المكونات	وصف المكون	تقسيمات فرعية إضافية (في حالة القابلية للتطبيق)
بيئة الرقابة	التصرفات ، والسياسات ، والإجراءات التي تعكس الاتجاه العام للإدارة العليا ، وأعضاء مجلس الإدارة ، وملاك الوحدة عن الرقابة وأهميتها .	مكونات فرعية : • الأمانة والقيم الأخلاقية. • الالتزام بالأهلية والصلاحية. • مشاركة مجلس الإدارة أو لجنة التدقيق. • فلسفة الإدارة وأسلوب التشغيل. • تخصيص السلطة والمسؤولية. • سياسات وممارسات الموارد البشرية.
تقدير المخاطر	تحديد وتحليل الإدارة المناسب للمخاطر عند إعداد القوائم المالية بما يتفق مع مبادئ المحاسبة المتعارف عليها.	**عمليات تقدير المخاطر :** • تحديد العوامل المؤثرة على المخاطر. • تقدير أهمية المخاطر واحتمال حدوثه . • تحديد الإجراءات اللازم اتخاذها للسيطرة على المخاطر. فئات مزاعم الإدارة التي ينبغي تحقيقها : • التأكد من فئات العمليات والأحداث الأخرى. • التأكد من أرصدة الحسابات. • التأكد من العرض والإفصاح.

أنشطة الرقابة	السياسات والإجراءات التي تضعها الإدارة لتحقيق أهدافها من التقرير المالي .	فئات أنشطة الرقابة : • الفصل الملائم بين الواجبات. • الترخيص الملائم للعمليات المالية والأنشطة. • السجلات المستندات الملائمة. • الرقابة الفعلية على الأصول والدفاتر. • الفحص المستقل للأداء.
المعلومات والتوصيل	الطرق التي تستخدم لتعريف ، وتجميع ، وتبويب ، وتسجيل ، والتقرير عن العمليات المالية للوحدة والحفاظ على المسؤولية عن الأصول المرتبطة بها .	ينبغي تحقيق أهداف التدقيق المرتبطة بالعمليات المالي : الوجود ، الدقة ، الاكتمال ، التبويب ، الترخيص والتلخيص ، التوقيت.
المراقبة	تقدير الإدارة المستمر لجودة أداء الرقابة لتحديد ما إذا كانت الرقابة يتم تنفيذها طبقا للتصميم الموضوع لها ، أو يتم تحديد ما إذا كانت هناك ضرورة لتعديل الرقابة الداخلية	غير قابل للتطبيق

المصدر: (Gelinas, Dull, Wheeler, Accounting Information Systems, 10e, 2015: 234).

رابعاً: محددات الرقابة الداخلية

ينبغي معرفة إن الرقابة الداخلية ومهما بلغت قوتها ومتانة الإجراءات التي تضعها الإدارة فإنها لن تستطيع الحصول على تأكيد مطلق وإنما تأكيد معقول حول تحقيق الإدارة لأهدافها ويرجع ذلك إلى مجموعة من الأسباب منها : (Catton and Panavalli, 2020, 210)

1. وجود المحددات المتوارثة ، مثل الاعتماد على العنصر البشري والحكم المهني في الكثير من الأمور ، وما يعانيه من نواحي القصور فيما يتعلق بارتكاب الأخطاء أو عدم الكفاءة ، ومن ثم عدم فهم التعليمات بشكل مناسب ، فضلا عن نقص المعلومات ومحددات الوقت.
2. إمكانية التواطؤ بين الموظفين الذين يقومون بالوظائف المتعارضة بقصد التلاعب أو الاختلاس.
3. تخطي الإدارة للتعليمات التي قامت بوضعها ، والقيام بخرق الرقابة الداخلية ، ومن ثم فتح المجال أمام الآخرين لعدم الالتزام بالتعليمات.
4. التغييرات التقنية التي تحدث في بيئة العمل التي تجعل الرقابة الداخلية عاجزة عن توفير الرقابة المناسبة ما لم تُحَدث.
5. التكلفة مقابل المنفعة ، إذ إن تصميم الإجراءات الرقابية وشموليتها قد يصعب تحقيقهما في بعض الأحيان لاحتمال زيادة الكلفة على المنافع المتوقعة ويمكن ملاحظة ذلك في حالة الفصل المناسب بين الوظائف المتعارضة.

المبحث الرابع
النموذج المقترح وآليات تطبيقه

تواجه الوحدات الاقتصادية في مختلف القطاعات والانشطة تحديات كبيرة تحتم عليها ضرورة استخدام التقنيات الحديثة، اذ افرزت البيئة الجديدة للوحدات الاقتصادية العديد من المتغيرات التي لم تكن موجودة في ظل استخدام الاساليب التقليدية في الوحدات الاقتصادية التي تعتمد على النظم اليدوية آنذاك، حيث تؤدي التقنية في وقتنا الحاضر دوراً مهما نتيجة تقدمها وتطورها بشكل كبير إذ اصبحت متغلغلة في الوحدات الاقتصادية لذلك اصبح لزاما على تلك الوحدات بذل جهود كبيرة من اجل المحافظة على المعلومات من الاختراق او الدخول غير المصرح به من خلال تطوير آليات نظم الرقابة الداخلية، وان استخدام التقنيات الحديثة يتطلب وجود الرقابة والموائمة بين فوائد تقنية المعلومات ومخاطرها، وهذا يؤدي الى التوجه الاكاديمي والمهني نحو بناء نماذج للأمن السيبراني واخضاعها للرقابة لزيادة اداء هذه النماذج في الوحدات وفي جميع اعمالها .

أولا: المخاطر والتهديدات التي يستهدفها النموذج المقترح

يعبر التهديد عن أي حدث يمكن أن يتسبب بأثر سلبي على أعمال الوحدة الاقتصادية مثل توقف الاتصالات أو الخسائر المادية أو المعنوية ، أما الخطر فيعبّر عن نسبة احتمال استغلال التهديد لقابلية الإصابة بما يتسبب بآثار على الأصل، في حين أنّ التهديد يعني الخطر المحتمل الذي يمكن أن يتعرض له الامن السيبراني ويمكن أن يكون التهديد شخصا (المتجسس ، والمجرم المحترف ، والقرصان المحترف) أو شيئا يهدد الأجهزة أو البرامج ، أو حدثا (الحريق ، وانقطاع التيار الكهربائي ، والكوارث الطبيعية) ، أما المخاطر فإنّها تستخدم بشكل مترادف مع مصطلح التهديد في اغلب الأحيان ، إلا أن الحقيقة أن المخاطر تتعلق بأثر التهديدات عند حدوثها ، ويرتبط الخطر أساساً باحتمال تعرض الوحدة الاقتصادية لخسائر أو تلف في الموجودات نتيجة أخطاء محاسبية غير مقصودة أو نتيجة أعمال غير نظامية متعمدة . ويُعَدُّ الخطر من العناصر الملازمة لكافة أنشطة الوحدة فالأفراد يمكن أن يرتكبوا الأخطاء ، ويمكنهم استغلال الفرص للتلاعب والقيام بأعمال غير نظامية متعمدة ، والآلات يمكن أن تتعرض لكثير من أوجه القصور .

ويرى الباحث بأن المخاطر والتهديدات التي تواجه الامن السيبراني تقسم لعدة أقسام، فمن حيث مصدرها تقسم على مخاطر داخلية ، ومخاطر خارجية ، ومن حيث المتسبب بها تقسم على مخاطر ناتجة عن العنصر البشري ، ومخاطر ناتجة عن العنصر غير البشري، ومن حيث أساس العمدية تقسم على مخاطر ناتجة عن تصرفات متعمدة أو مقصودة، ومخاطر ناتجة عن تصرفات غير متعمدة أو غير مقصودة ، ومن حيث الآثار الناتجة عنها تقسم على مخاطر ينتج عنها أضرار مادية ، مخاطر فنية ومنطقية .

أما في النموذج المقترح فقد صنفت المخاطر من حيث علاقتها بمراحل النظام إلى الآتي:

1. **مخاطر المدخلات :** وهي المخاطر الناتجة عن عدم تسجيل البيانات في الوقت المناسب وبشكلها الصحيح أو عدم نقل البيانات بدقة خلال خطوط الاتصال، وتتمثل المخاطر المتعلقة بأمن المدخلات بأربعة أقسام أساسية وهي إنشاء بيانات غير سليمة، وتعديل أو تحريف بيانات المدخلات، حذف بعض المدخلات، إدخال البيانات أكثر من مرة.
2. **مخاطر تشغيل البيانات :** ويقصد بها المخاطر المتعلقة بالبيانات المخزنة في ذاكرة الحاسب والبرامج التي تقوم بتشغيل تلك البيانات وتتمثل مخاطر تشغيل البيانات في الاستعمال غير المصرح به لنظام وبرامج التشغيل وتحريف وتعديل البرامج بطريقة غير قانونية أو عمل نسخ غير قانونية أو سرقة البيانات الموجودة في الحاسب الآلي، ومثال على ذلك قيام الموظف بإعطاء أوامر للبرنامج بأن لا يسجل أي قيود في السجلات المالية تتعلق بعمليات البيع الخاصة بعميل معين من أجل الإفادة من مبلغ العملية لصالح المحرف نفسه.
3. **مخاطر المخرجات:** ويقصد بها المخاطر المتعلقة بالمعلومات والتقارير التي يتم الحصول عليها بعد عملية تشغيل ومعالجة البيانات، وقد تحدث تلك المخاطر من خلال طمس أو تدمير بنود معينة من المخرجات أو خلق مخرجات زائفة وغير صحيحة أو سرقة مخرجات الحاسب أو إساءة استعمالها أو عمل نسخ غير مصرح بها من المخرجات أو الكشف غير المسموح به للبيانات عن طريق عرضها على شاشات العرض أو طبعها على الورق أو طبع وتوزيع المعلومات بواسطة أشخاص غير مسموح لهم بذلك ، كذلك توجيه

تلك المطبوعات والمعلومات خطأ إلى أشخاص ليس لهم الحق في الاطلاع على تلك المعلومات أو تسليم المستندات الحساسة إلى أشخاص لا تتوافر فيهم الناحية الأمنية بغرض تمزيقها أو التخلص منها مما يؤدي إلى استعمال تلك المعلومات في أمور تسيئ إلى الوحدة الاقتصادية وتضر بمصالحها.

أما تصنيف المخاطر بالنموذج المقترح بحسب الغرض منها فقد قسمت إلى أربعة أنواع رئيسة وهي كالآتي:

1. خرق النظم الحاسوبية بهدف الاطلاع على المعلومات المخزنة فيها والوصول إلى معلومات شخصية أو أمنية عن شخص ما، أو التجسس الصناعي، أو التجسس المعادي للوصول إلى معلومات عسكرية سرية .
2. خرق النظم الحاسوبية بهدف التزوير أو الاحتيال(التلاعب بالحسابات في البنوك، والتلاعب بفاتورة الهاتف، والتلاعب بالضرائب، تغيير بيانات شخصية من السجل المدني أو السجل العام للموظفين، ...وغيرها).
3. خرق النظم الحاسوبية بهدف تعطيل هذه النظم عن العمل لأغراض تخريبية باستعمال ما يسمى البرامج الخبيثة (مثل الفيروسات، والدودة، وحصان طروادة، أو القنابل الإلكترونية)، أما من قبل الأفراد أو العصابات أو الجهات الأجنبية بغرض شلّ هذه النظم الحاسوبية (أو المواقع على الأنترنت) عن العمل لاسيما في ظروف خاصة أو في أوقات الحرب.
4. أخطار ناتجة عن فشل التجهيزات في العمل، وأعطال كهربائية، وحريق، وكوارث طبيعية(فيضانات، وزلازل) وتُعَدُّ التصنيفات السابقة لمخاطر نظم المعلومات المحاسبية الإلكترونية شاملة لجميع المخاطر التي تواجه نظم المعلومات المحاسبية.

أما التهديدات التي تواجه الامن السيبراني والتي يستهدفها النموذج المقترح فهي أربعة تهديدات، الكوارث الطبيعية والسياسية، والأخطاء البرمجية، وقصور المعدات والأفعال غير المقصودة، والأفعال المقصودة (الجرائم الحاسوبية)، والتي يوضحها الجدول الآتي:

جدول (2)

التهديدات التي تواجه تقنية المعلومات

التهديدات	الأمثلة
الكوارث الطبيعية والسياسية	- الحرائق أو الحرارة المفرطة - الفيضانات - الزلازل - الرياح العاتية - الحرب والهجمات الإرهابية
الأخطاء البرمجية وقصور المعدات	- تعطل المعدات والبرامجيات - الأخطاء أو الخلل في البرمجة - تحطم أنظمة التشغيل - أعطال وتقلبات الطاقة - الأخطاء غير المكتشفة في نقل البيانات
الأفعال غير المقصودة	- الحوادث الناجمة عن الإهمال البشري - الإخفاق في إتباع الإجراءات المؤسسية - ضعف التدريب والإشراف على الموظفين - الأخطاء غير المقصودة - الأخطاء المنطقية - الأنظمة التي لا تلبي احتياجات المنظمة أو التي ليس لديها قدرة على تحقيق المهام المطلوبة

الأفعال المقصودة (الجرائم الحاسوبية)	- التخريب - الفساد - سوء التمثيل ، الاستعمال الخاطئ ، الإفصاح غير المصرح به عن البيانات - اختلاس الموجودات - الاحتيال عند أعداد القوائم المالية

ويرى الباحث أن النوع الأخير من التهديدات والمتمثل بالجرائم المحوسبة يعد تحدياً كبيراً للأمن السيبراني لما يسببه من خسائر كبيرة ، ويمكن أن تتم الجرائم المحوسبة من قبل أشخاص من داخل الوحدة الاقتصادية يملكون صلاحيات الدخول إلى النظم أو أشخاص من خارج الوحدة ، وذلك باختراق نظم المعلومات باستعمال الحاسوب وفي الغالب يتم ذلك من خلال شبكات الاتصال.

ثانيا: مرتكزات النموذج المقترح للحفاظ على الامن السيبراني

يركز النموذج المقترح على ثلاثة مرتكزات ، البناء التنظيمي لوظائف تقنية المعلومات ، والرقابة على عمليات الحاسوب ، والتخطيط لمواجهة الكوارث:

1- البناء التنظيمي لوظائف تقنية المعلومات:

يتضمن البناء التنظيمي لتقنية المعلومات ، المواقع التنظيمية ، والمسؤوليات ذات العلاقة ، إذ يشمل هذا البناء خمسة مواقع رئيسة ذات مسؤوليات عديدة ، وهذه المواقع هي **مدير تقنية المعلومات** ، إذ يتولى فحص الرقابات كافة ، والمصادقة على النظم ، ووضع خطط قصيرة وطويلة الأمد ، والموقع الثاني هو **تطوير النظم** الذي يشتمل على محلل النظم الذي يتولى تقويم النظم الحالية ، وتصميم نظم جديدة ، ووضع خطط عامة للنظم ، ووضع مواصفات المبرمجين ، والمبرمجين الذين يقومون بتصميم وتوثيق البرامج ، وتصميم وتطوير خرائط تدفق البيانات عبر الحاسوب ، والموقع الثالث هو **تشغيل تقنية المعلومات** فهي تشتمل على مشغل الحاسوب الذي يقوم بتشغيل مكونات الحاسوب المادية ، وتنفيذ البرامج استناداً إلى تعليمات التشغيل ، وأمين المكتبة الذي يقوم بإدامة توثيق النظم والبرامج والملفات التي بعهدته ومدير شبكة الاتصالات الذي يقوم بتخطيط وإدامة مواقع للشبكة ذات صلة بالوحدة الاقتصادية، والموقع الرابع هو **رقابة البيانات** الذي يشتمل على فريق رقابة البيانات ويشمل رقابة تصاريح دخول المستخدمين، ومتابعة الدخول والرقابة على المعالجة والمخرجات، ومدير قاعدة البيانات الذي يقوم بتصميم وتنظيم قاعدة البيانات، وتحديد رقابات دخول واستعمال قاعدة البيانات، والموقع الخامس هو **مدير أمن المعلومات** الذي تقع على عاتقه إدارة أمن نظم تقنية المعلومات بضمنها أمن كل من المكونات المادية والبرمجيات، وملاحظة الوصول للبرامج والبيانات ومتابعة حالات الاختراق الأمني.

2- **الرقابة على عمليات تقنية المعلومات** وتتضمن الآتي:

أ- **فصل ملائم بين الوظائف** ، إذ تعمل الوحدة الاقتصادية على الفصل بين الوظائف المختلفة في تقنية المعلومات بهدف منع تجميع أو دمج وظائف المعالجة ، ومنح التفويض ، والتسجيل لدى شخص واحد فقط ، مثل الفصل بين وظيفة تطوير النظم عن المعالجة بالحاسوب ، وفصل وظيفة إدارة قاعدة البيانات عن الوظائف الأخرى لتقنية المعلومات ، وفصل وظيفة إدارة قاعدة البيانات عن مهام تطوير النظم.

ب- **رقابات مادية على الوصول**، وتتضمن :

1) وضع معدات الحاسوب في غرف يمكن إقفالها، وحصر الدخول إليها بالأفراد المصرح لهم.
2) وجود مدخل واحد أو مدخلين كحد أقصى إلى مركز تقنية المعلومات، مع جعل المداخل قابلة للمراقبة والأقفال.
3) تطبيق سياقات صحيحة لمطالبة المصرح لهم بدخول مركز تقنية المعلومات بهويات تعريفية.

4) إلزام المراجعين بالتوقيع في سجل الدخول عند دخولهم ومغادرتهم مركز تقنية المعلومات، وكتابة وصف مختصر عنهم ضمن سياسات الأمن للوحدة الاقتصادية، ووضع (بطاقات تعريفية) خاصة بهم ومرافقتهم للأماكن التي يقصدونها.
5) استعمال نظام الإنذار الأمني للكشف عن أي دخول غير مصرح به إلى نظام تقنية المعلومات.
6) نصب أقفال على الحواسيب الشخصية وبقية أجهزة الحاسوب.
7) تقييد الوصول من خارج الشبكة إلى البرامج والمعدات.
8) وضع معدات ومكونات أخرى مهمة للنظام بعيدا عن أية مواد قابلة للإشتعال.
9) نصب أجهزة الإنذار ضد الحرائق، واستعمال وسائل إطفاء للحريق لا تدمر معدات الحاسوب.

3- **الرقابة على الوصول المنطقي للبيانات:** ينبغي السماح للمستخدمين المصرح لهم فقط بالوصول إلى البيانات ، مما يعني أداءهم لوظائف معينة مصرح لهم بها من قبيل القراءة ، والنسخ ، والإضافة ، والحذف وغيرها. إذ من المهم حماية البيانات من الخارجيين بالنسبة للوحدة الاقتصادية ، كأن تخترق شركة منافسة النظام وتتصفح البيانات.

4- خطة التعافي من الكوارث :

تهدف خطة مواجهة الكوارث إلى تخفيض الأضرار والخسائر، فضلاً عن وضع وسائل بديلة مؤقتة لمعالجة المعلومات، ولمواصلة العمل الاعتيادي بأسرع وقت ممكن، وتدريب العاملين على كيفية التعامل مع الظروف غير الاعتيادية (حالات من قبيل الحرب، أو الفيضان، أو الزلزال)، والاختبار الدوري المناسب لخطط الطوارئ ، ومراجعة خطة التعافي من الكارثة تشتمل خطة التعافي من الكارثة على الخطوات الآتية تحديد أولويات التعافي. بموجبها تُحدَد التطبيقات والمكونات المادية والبرمجيات التي تضمن استمرار الوحدة الاقتصادية في العمل، في أثناء وبعد إنتهاء الكارثة.

أ- توفير غطاء تأميني للحصول على التمويل اللازم لاستبدال المعدات والبرمجيات المتضررة.
ب- الاحتفاظ المستمر بملفات إحتياطية من البيانات والبرامج (ملفات دعم)، تُخَزّن في مواقع آمنة بعيداً عن المركز الرئيس للحاسوب، لاستعمالها إذا ما أصيب النظام بأي كارثة.
ت- تحديد موظف تنسيق يكون مسؤولا عن التطبيق المُنسَق لخطة التعافي بكافة مراحلها، يحدد هذا الموظف مسؤوليات فريق العمل الذي تُناط به أنشطة مواجهة الكارثة والتعافي منها، يأخذ هذا الفريق على عاتقه إيجاد المواقع البديلة، وتحديد البرامج، والتسهيلات اللازمة لتوصيل البيانات واسترداد السجلات الحيوية.
ث- فحص ومراجعة خطة التعافي دوريا فضلاً عن اختبارها عن طريق محاكاة الكارثة.
ج- التوثيق الكامل لخطة التعافي من الكارثة والاحتفاظ بنسخ عديدة منها في مواقع بديلة آمنة.

ثالثا: الفعاليات الرئيسية للنموذج المقرح للأمن السيبراني لإدارة الرقابة الداخلية

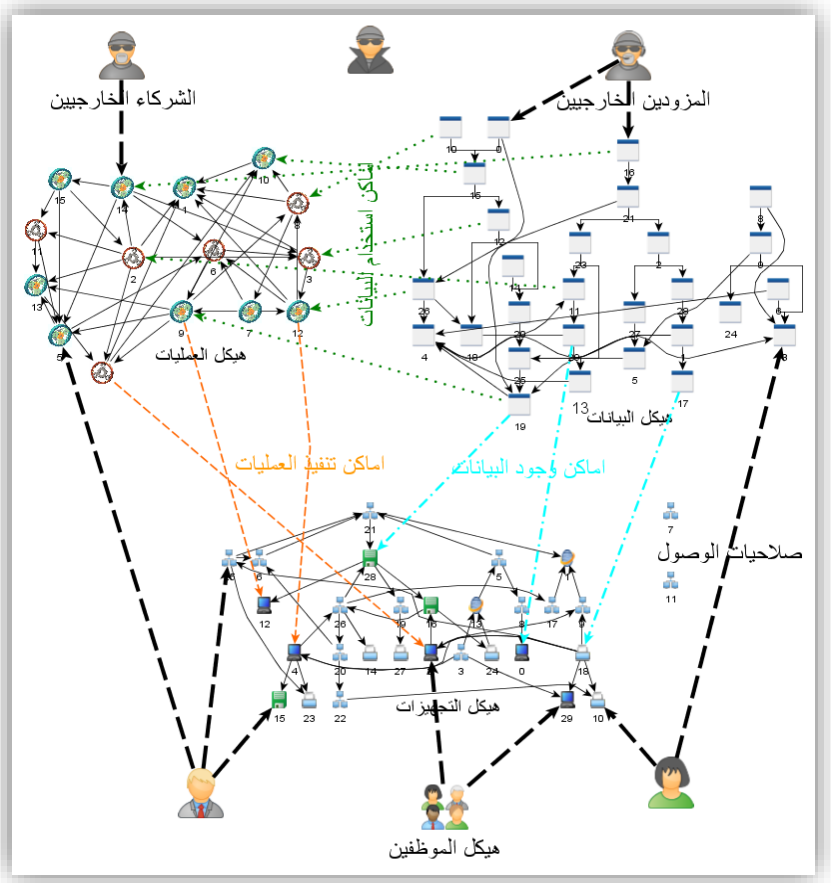
هناك عدة فعاليات ينبغي تطبيقها عند اعتماد النموذج المقترح لإدارة الامن السيبراني وهي :

1. **حدد وتعرف على البيئة :** وهي عملية تهتم بالتعرف على بيئة اعمال المؤسسات المالية والتجارية وتحديد الموجودات وكذلك اسلوب ادارة المخاطر و حوكمة الامن.
2. **احم البيئة :** وهي تهتم بالقيام بما يلزم لحماية الانظمة والمعلومات والموجودات في المؤسسات والمحافظة على هذه الاجراءات.
3. **اكتشف المشاكل الامنية والاختراقات:** وهي تهتم بالقيام بما يلزم لاكتشاف أي احداث غريبة واية عمليات اختراق وهجوم الكتروني.
4. **استجب لهذه المشاكل والاختراقات:** وهي تهتم بالقيام بما يلزم للاستجابة لأي حدث او عملية اختراق او هجوم.
5. **تعافى من هذه المشاكل والاختراقات** : وهي تهتم بالقيام بتنفيذ خطط التعافي من الاحداث.

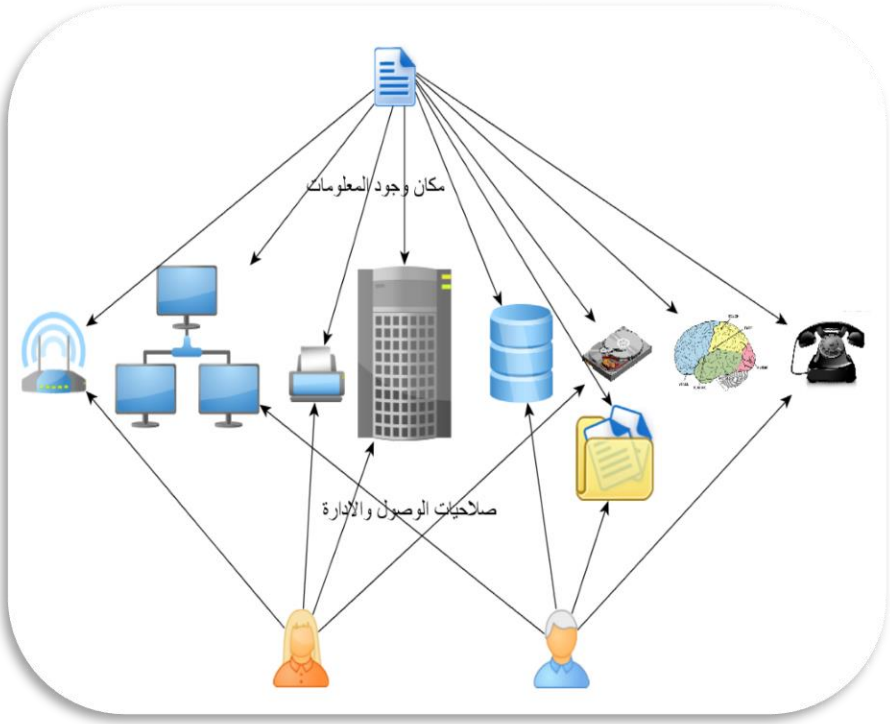
ويرى الباحث ولغرض تطبيق النموذج المقترح لزيادة فاعلية عمل الرقابة الداخلية للحفاظ على الامن السيبراني على وفق مقاييس عالمية يمكن بيانها من خلال شكل الآتي:

شكل (1)

هيكلية بناء الامن السبيراني في النموذج المقترح



الشكل (2) تحديد مكان وجود البيانات والمعلومات واساليب الحماية وصلاحيات الوصول وادارة البيانات في النموذج المقترح



يلزم لتطبق النموذج المقترح القيام بإنشاء واستحداث فعاليات وعمليات مستمرة لإدارة المعلومات من خلال حصر وادارة هيكل الاهداف وهيكل المعلومات والعمليات المرتبطة بها ، اضافة الى علاقة هذه المعلومات والعمليات بهيكل التجهيزات ووسائط نقل وتخزين البيانات وبيان صلاحيات وصول الموظفين لهذه المعلومات وذلك لكي يتم القيام بإدارة امن المعلومات والامن السيبراني بالشكل المطلوب. وفي مجال حماية المعلومات والامن السيبراني فانه ايضا يلزم استحداث عمليات مستمرة لإدارة امن ومخاطر المعلومات والفضاء الالكتروني ضمن السياسات والاستراتيجيات الخاصة بمتطلبات الاعمال وفق تصنيف المعلومات والعمليات المستخدمة بها، كما يلزم ايضا تطوير العمليات التقنية لحماية المعلومات والفضاء الالكتروني لتشمل متطلبات المقاييس الدولية بهذا المجال، وعلية فيمكن القيام بإنشاء وحدة تنظيمية مستقلة لتغطي هذه الفعاليات والخاص بالمتطلبات التقنية لحماية البيئة الحاسوبية.

المبحث الرابع

الاستنتاجات والتوصيات

أولا: الاستنتاجات

1. يترتب على أمان السيبراني تأثير كبير على فاعلية نظام الرقابة الداخلية في الشركات والمؤسسات فهو يوفر الأمان يعزز الحماية ضد التهديدات الإلكترونية المحتملة، مما يقلل من احتمالية حدوث انتهاكات أمنية داخلية أو خروج معلومات حساسة.
2. يؤثر الأمن السيبراني على نظام الرقابة الداخلية من خلال تحسين سرعة استجابة الشركة للتهديدات والتحقق من الوصول وإدارة الصلاحيات بشكل فعال. ويمكن تعزيز القواعد والسياسات الداخلية للشركة، مما يعني الامتثال بشكل أفضل للتشريعات واللوائح المتعلقة بالحماية الإلكترونية.
3. أن الحفاظ على الأمن السيبراني يقلل من المخاطر المالية المرتبطة بانتهاكات البيانات وتسرب المعلومات، مما يحافظ على سمعة الشركة وثقة العملاء. ويمكن أن يساهم في تعزيز الثقة بين العاملين داخل المؤسسة، مما يعزز الكفاءة ويزيد من إنتاجيتهم.
4. أن الفهم الصحيح للأمن السيبراني وتأثيره على الوحدة الاقتصادية يساعد في تطوير استراتيجيات أفضل للحماية وإدارة المخاطر في المؤسسة.
5. يتطلب الحفاظ على التوازن بين الأمن السيبراني والرقابة الداخلية التنوع في الأدوات والسياسات المستخدمة لضمان حماية البيانات والتحكم الفعال داخل الشركة.
6. إن النموذج المقترح للأمن السيبراني يعزز فعالية نظام الرقابة الداخلية عن طريق تعزيز الحماية وتقليل المخاطر الإلكترونية، مما يساهم في تعزيز الأداء العام للشركة أو المؤسسة واستدامتها في البيئة التقنية المعقدة والمتغيرة باستمرار.
7. بين النموذج المقترح بأن إدارة الأمن السيبراني تتطلب توجهاً شاملاً يشمل التواصل الفعال، والتعاون، والتحسين المستمر، والتفاعل السريع مع التهديدات المتغيرة.

ثانيا: التوصيات

1- يجب توفير تدريب مستمر وجلسات توعية للموظفين حول مخاطر الأمن السيبراني وأفضل الممارسات في استخدام التكنولوجيا وحماية المعلومات الحساسة.
2- تحديث وتطوير سياسات الأمن السيبراني وضمان تطبيقها بشكل صارم للحماية ضد التهديدات الجديدة والمتطورة.
3- الاستثمار في أدوات الأمن السيبراني المتقدمة مثل أنظمة الكشف عن التسلل وحلول إدارة الهوية والوصول لتعزيز الحماية.
4- تقييم ومراجعة نظام الأمن السيبراني بشكل دوري للكشف عن النقاط الضعيفة وتحسين الإجراءات وفقًا لذلك.

5- إعداد خطط استجابة واستعادة للحوادث الأمنية المحتملة لتقليل التأثيرات المحتملة في حالة وقوع هجمات سيبرانية.
6- التعاون مع مزودي الخدمات الأمنية والجهات الأمنية العامة والخاصة لتبادل المعلومات والتحديثات الأمنية.
7- تقييم أداء إجراءات الأمن السيبراني ونظام الرقابة الداخلية بشكل دوري للتأكد من فعاليتها واتخاذ التحسينات الضرورية.
8- ضمان الامتثال للقوانين واللوائح الخاصة بالأمن السيبراني والحفاظ على معايير الخصوصية والحماية.
9- جعل الأمن السيبراني جزءًا من ثقافة الشركة وتشجيع الموظفين على المساهمة في الحفاظ على الأمن.
10- في حالة الحاجة، اللجوء إلى خبراء الأمن السيبراني والمستشارين لتقديم المشورة والدعم في تحسين استراتيجيات الأمن.

المصادر

1. البغدادي، صلاح الدين أيوب، (2021)، مخاطر الهجمات الإلكترونية (السيبرانية) وآثارها الاقتصادية ، دارسة حالة دول مجلس التعاون الخليجي، سلسلة تنموية، المعهد العربي للتخطيط، الامارات .
2. حجازي ، رياض أحمد، (2021)، "حوكمة تكنولوجيا المعلومات : ميزة إستراتيجية في ظل اقتصاد المعرفة" الملتقى الوطني حول : حوكمة الشركات كآلية للحد من الفساد المالي والإداري جامعة بسكرة .
3. لطفي ، امين السيد احمد ، (2017)، "نظرية المحاسبة منظور التوافق الدولي" ، الدار الجامعية ، الاسكندرية ، جمهورية مصر العربية.
4. اليوسف، محمود عبد المجيد ، (2020)، "أثر فاعلية انظمة الرقابة الداخلية وفق إطار COSO على جودة التدقيق الخارجي/ دراسة ميدانية : على الشركات الصناعية المساهمة العامة الأردنية"، رسالة ماجستير غير منشورة ، ملية الاقتصاد والعلوم الادارية جامعة جرش، الأردن.
1. (NIST) (2018) , a Glossary of key information security terms National institute of standards and technology interagency or internal report available at http://csrc.nist.gov/publications.
2. (ISACA), (2017), Available at: https://www.isaca.org/en/resources/isaca-journal/issues/2017/volume-
3. Arens ،Alvin ،Randal J. Elder and Mark S. Beasley,(2018), "Auditing and Assurance Services: anintegrated Approach" ،Pearson Education. Inc. ،(14th ed.).
4. Catton, P. and Panavalli, P. (2020). Benefits of Utilizing Agile Internal Audit Methodology during COVID-19 Disruption. DHG. https://www.forvis.com/article/benefits-of-utilizing-agile-internal-audit-methodology-during-covid-19-disruption.
5. Eaton.T.V & Grenier, J.H (2022). Accounting and Cybersecurity Risk Management. Current Issues in Auditing, 13(2), C1-C9.
6. Florakis C.C. Louca R. Michaely and M Weber, (2023) ,Cybersecurity Risk, Pp. 1-73, Available at http://ssrn.com.
7. Gelinas, Dull, Wheeler, "**Accounting Information Systems**", 10e, 2015.
8. Hall-James A. ،"Introduction to Accounting information Systems", South Western ،(8th ed.) , 2013.
9. Hartmann C.C. and J. Carmenate, (2021) ,Academic Research on the Role of Corporate Governance and IT Expertise in Addressing Cybersecurity Breaches Implications for Practice Policy and Research, American Accounting Association, 15 (2) Pp. 9 - 23 .

10. KPMG (2020). Agile Internal Audit White paper on Working Agile within Internal Audit Functions Part II: Concrete Guidance for the set-up of the Agile Internal Audit Function and the Execution of Agile Audits.
11. Kurt F. Reding, Sobel, Paul J., Anderson, Urton L., Head, Michael J., Ramamoorti, Sridhar, Salamasick, Mark, Riddle, Cris, (2009), "Internal Auditing Assurance & Consulting Services", Second Edition, The Institute of Internal Auditors.
12. Moeller, M. S. (2014). Internal control quality and information asymmetry in the secondary loan market. Review of Quantitative Finance and Accounting, 43(4), 683-720.
13. Saidin, S. & Badara, M. (2013). Impact of the effective internal controlsystem on the internal audit effectiveness at local government level. Journal of Social and Development Sciences, 4(1), 16.
14. Shahimi S. and N. Mahzan, (2022) ,Building a research model and hypotheses development and findings of Exploratory Interviews International Journal of Management Excellence 10 (2) Pp. 1257 – 1283.
15. Wolden, M., Valverde, R., & Talla, M. (2015). The effectiveness of COBIT 5 information -9-IFAC security framework for reducing cyber attacks on supply chain management system, PapersOnLine.