Tikrit Journal of Administrative and Economic Sciences, Vol. 19, No. 63, Part (2): 94-112
Doi: www.doi.org/10.25130/tjaes.19.63.2.5

Tikrit Journal of Administrative and Economics Sciences
مجلة تكريت للعلوم الإدارية والاقتصادية
ISSN: 1813-1719 (Print)

Internal Audit Requirements to Enhance Cybersecurity in Economic Units in considering the Institute of Internal Auditors (IIA) Guidelines

Suha Younis Ali AL Braznji*, Zeyad Hashim Yahya Al-Saqa
Department of Accountancy, College of Administration and Economics, University of Mosul

Keywords:
Internal Audit, Cybersecurity, Internal Audit Requirements, Cybersecurity Enhancement, Risk Management

A R T I C L E I N F O

Article history:
Received 13 May. 2023
Accepted 19 Jun. 2023
Available online 30 Sep. 2023

*Corresponding author:
Suha Younis Ali AL Braznji
Department of Accountancy, College of Administration and Economics, University of Mosul

Abstract: The study aimed to identify a set of requirements that are supposed to be met in a way that enables the internal auditor to perform his role effectively as an independent guarantee provider for the Board of Directors for a set of controls and measures for cybersecurity and what can contribute to achieving its efficiency and effectiveness, through auditing the operations carried out by the first and second lines responsible for developing and implementing these controls, based on the instructions issued by the Institute of Internal Auditors (IIA), and the study found the need to meet a set of requirements It is to provide the internal auditor with advanced knowledge of information technology and work with high professional care and maintain his independence, and that the internal auditors receive sufficient support from the Board of Directors by allowing time, providing the necessary financial resources, supporting their participation in developing the cybersecurity strategy in economic units and granting them sufficient powers for that, updating the internal audit approach and planning for the cyber audit process on an annual and flexible basis and on a risk-based basis using an appropriate methodology, as well as strengthening the relationships between the internal audit function and technical functions. Information, cybersecurity, and work collaboratively to enhance cybersecurity in economic units.

Tikrit Journal of Administrative and Economic Sciences, Vol. 19, No. 63, Part (2): 94-112
Doi: www.doi.org/10.25130/tjaes.19.63.2.5

متطلبات التدقيق الداخلي لتعزيز الأمن السيبراني في الوحدات الاقتصادية في ضوء إرشادات معهد المدققين الداخليين (IIA)

سهى يونس علي البرزنجي **زياد هاشم يحيى السقا**
قسم المحاسبة، كلية الإدارة والاقتصاد، جامعة الموصل

المستخلص

هدفت الدراسة إلى تحديد مجموعة من المتطلبات التي يفترض توافرها بالشكل الذي يمكن المدقق الداخلي من أداء دوره بشكل فاعل كمقدم ضمانات مستقلة لمجلس الادارة لمجموعة الضوابط والتدابير الخاصة بالأمن السيبراني وبما يمكن أن يسهم في تحقيق كفاءتها وفاعليتها, من خلال تدقيق العمليات التي يقوم بها الخطان الأول والثاني المسؤولين عن وضع وتنفيذ هذه الضوابط، وذلك بالاستناد على الارشادات الصادرة من معهد المدققين الداخليين (IIA)، وقد توصلت الدراسة إلى ضرورة توافر مجموعة من المتطلبات المتمثلة بتزود المدقق الداخلي بمعرفة متطورة بتقنية المعلومات والعمل بعناية مهنية عالية والحفاظ على استقلاليته, وأن يتلقى المدققون الداخليون الدعم الكافي من مجلس الادارة بإتاحة الوقت وتوفير الموارد المالية اللازمة ودعم مشاركتهم في تطوير استراتيجية الأمن السيبراني في الوحدات الاقتصادية ومنحهم الصلاحيات الكافية لذلك، وتحديث منهج التدقيق الداخلي والتخطيط لعملية التدقيق السيبراني بشكل سنوي ومرن وعلى أساس المخاطر باستخدام منهجية ملائمة، فضلاً عن تعزيز العلاقات بين وظيفة التدقيق الداخلي ووظائف تقنية المعلومات والأمن السيبراني ومشاركتهم في رعاية مشاريع بحثية مشتركة او المشاركة في استضافة دورات تدريبية متعلقة بالأمن السيبراني والعمل بشكل تعاوني لتعزيز الأمن السيبراني في الوحدات الاقتصادية.

الكلمات المفتاحية: التدقيق الداخلي، الأمن السيبراني، متطلبات التدقيق الداخلي، تعزيز الأمن السيبراني، أدارة المخاطر.

المبحث الأول: منهجية البحث ودراسات سابقة

اولاً. منهجية البحث:

1. المقدمة

أدى التطور في بيئة الأعمال بسرعة وبصورة غير مسبوقة إلى اتجاه العديد من الوحدات الاقتصادية نحو مواكبة استخدامات التقنية الحديثة، حيث تطبق تقنيات وأدوات تقنية متطورة في مباشرة أعمالها لجعلها أكثر كفاءة، فضلا عن القيام بتخزين بياناتها الهامة والحساسة على الشبكات وفي الحوسبة السحابية Computing Cloud وفي الوقت نفسه تتطلب بيئة الأعمال العالمية الوحدات الاقتصادية على الحفاظ على بنية تحتية رقمية آمنة لأجراء معاملاتها التجارية وهذه البنية التحتية الرقمية العالمية المترابطة تسمى بالفضاء السيبراني، وللوقاية من مخاطر هذا الفضاء دائم التوسع والنمو يقع على المختصين في الأمن السيبراني الأخذ بعين الاعتبار كل التدابير اللازمة للوقاية من مخاطر هذا الفضاء الافتراضي الرقمي وبما يتطلب ضرورة توافر تشكيلة متنوعة من الضمانات الآمنة التي تتناسب وطبيعة البيئة الرقمية الجديدة أطلق عليها "الامن السيبراني cyber security".

واستناداً إلى تطور دور التدقيق الداخلي في أدارة المخاطر والرقابة والحوكمة في الوحدات الاقتصادية التي يعمل فيها بشكل عام وأثرها البالغ في الحد من المخاطر التي يتعرض لها بيئة العمل السيبراني وتعزيز الأمن فيها بشكل خاص يتطلب الالتزام بمجموعة من الارشادات الصادرة من معهد المدققين الداخليين (IIA) بغرض حماية الموارد البشرية والمالية المرتبط عملها بتقنيات المعلومات من مخاطر الأمن السيبراني والحفاظ على المعلومات وكل ما يرتبط ببيئة العمل السيبراني

2. **مشكلة الدراسة:** أن الالتزام بإرشادات معهد المدققين الداخليين يعني ضرورة العمل على توفير مجموعة من المتطلبات المرتبطة بعمل التدقيق الداخلي التي تساهم في تعزيز الأمن السيبراني في الوحدات الاقتصادية، لذا فإن السؤال الذي يمكن من خلاله أن تتبلور **مشكلة البحث** هو: ماهي متطلبات التدقيق الداخلي اللازمة لتعزيز الأمن السيبراني التي أشارت إليها إرشادات معهد المدققين الداخليين في الوحدات الاقتصادية وهل تمكن هذه الارشادات المدقق الداخلي من أداء دوره في تعزيز الأمن السيبراني وكيف؟
3. **أهمية الدراسة:** يستمد البحث أهميته من أهمية المتغيرات التي يحويها وتتلخص بما يأتي:

أ. تناول موضوع على قدر كبير من الأهمية والمتمثل بكيفية تأمين حماية الموارد البشرية والمالية المرتبط عملها بتقنيات المعلومات من المخاطر التي يتعرض لها الفضاء السيبراني وكيفية ادارتها من قبل خطوط الدفاع الثلاثة (وظائف تقنية المعلومات والأمن السيبراني والتدقيق الداخلي).

ب. ابراز الدور المنوط للمنظمات المهنية الدولية وعلى وجه الخصوص معهد المدققين الداخليين في عصر تسوده العولمة الالكتروني في التصدي للمخاطر التي يمكن أن تتعرض لها البيئة السيبرانية للوحدات الاقتصادية من قبل التدقيق الداخلي وتوفير الحماية الكافية للمعلومات والشبكات والبرامج بتحقيق الأمن السيبراني.

ج. تزويد المدققين الداخليين بآلية مناسبة تمكنهم من التصدي للهجمات السيبرانية وتوسيع نطاق المعرفة بالسلامة السيبرانية من أجل تحقيق كفاءة التدقيق الرقمي.

4. **أهداف الدراسة:** *يهدف البحث إلى:*

أ. التعرف على مفهوم الأمن السيبراني وأهميته في الوحدات الاقتصادية.

ب. توضيح أهمية التدقيق الداخلي في تحقيق أهداف الأمن السيبراني.

ج. تحديد متطلبات التدقيق الداخلي الواجب توافرها في سبيل تعزيز الأمن السيبراني والحد من المخاطر السيبرانية وتحقيق أمن المعلومات في ضوء إرشادات معهد المدققين الداخليين.

5. **فرضيات الدراسة:** يعتمد البحث على فرضية رئيسية مفادها:

إن الالتزام بإرشادات معهد المدققين الداخليين يمكن المدقق الداخلي من تعزيز الأمن السيبراني في الوحدات الاقتصادية.

وقد تضمن البحث المباحث الآتية:

المبحث الأول: الإطار النظري للأمن السيبراني.

المبحث الثاني: أهمية التدقيق الداخلي لأغراض الأمن السيبراني.

المبحث الثالث: متطلبات تطبيق إرشادات معهد المدققين الداخليين لتعزيز الأمن السيبراني.

Tikrit Journal of Administrative and Economic Sciences, Vol. 19, No. 63, Part (2): 94-112
Doi: www.doi.org/10.25130/tjaes.19.63.2.5

ثانياً. دراسات سابقة:

1. دراسة (Islam, et al., 2018):

عنوان الدراسة	العوامل المؤثرة في تدقيق الامن السيبراني
هدف الدراسة	تحديد العوامل المؤثرة في الامن السيبراني التي لها علاقة بالمراجعة الداخلية من خلال استطلاع اراء 970 مراجع داخلي في 166 دولة
نتائج الدراسة	1. ان قيام المراجعين الداخليين بالتقييم الشامل للمخاطر له تأثير ايجابي كبير في مراجعة الامن السيبراني 2. أن كفاءة المراجعين الداخليين تؤثر على مراجعة الامن السيبراني.

2. دراسة (آمنة، 2021) بحث:

عنوان الدراسة	تأثير الامن السيبراني على الرقابة الداخلية وانعكاسها على الوحدة الاقتصادية: دراسة استطلاعية لارا عينة من المدققين الداخليين والمحاسبين في وزارة التعليم العالي والبحث العلمي.
هدف الدراسة	التعرف على أهمية الامن السيبراني من خلال تأثيره على الرقابة الداخلية وقيمة الوحدة الاقتصادية باعتماد إطار حوكمة تقنية المعلومات 5COBIT باستخدام المنهج الوصفي التحليلي.
نتائج الدراسة	وجود تقبل واتفاق بشكل عام بين ابعاد ومتطلبات الامن السيبرانية على الأطر الحديثة للرقابة الداخلية.

3. دراسة (الزيود، 2021) رسالة ماجستير:

عنوان الدراسة	أثر المراجعة الداخلية في الحد من مخاطر السيبرانية في البنوك التجارية الاردنية
هدف الدراسة	التعرف على أثر التدقيق الداخلي المتمثل بـ (كفاءة التدقيق الداخلي، وحيادية التدقيق الداخلي، والمركز التنظيمي للتدقيق الداخلي وتخطيط التدقيق الداخلي) في الحد من المخاطر السيبرانية في البنوك التجارية الاردنية باعتماد المنهج الوصفي والتحليلي
نتائج الدراسة	أن كفاءة المراجعة الداخلية وموقعها التنظيمي وتخطيط عملية التدقيق في البنك يؤثر في الحد من مخاطر الامن السيبراني بالبنوك التجارية الاردنية وعدم وجود أثر لحيادية التدقيق الداخلي في الحد من المخاطر السيبرانية في البنوك التجارية الاردنية.

4. دراسة (George, et al., 2021):

عنوان الدراسة	التدقيق الداخلي والامن السيبراني: دور التدقيق والمساهمة الإجرائية
هدف الدراسة	فحص العوامل التي تؤثر على امن الانترنت وفي نفس الوقت التي تكون ذات صلة بالتدقيق الداخلي من خلال استمارة الاستبيان تم توزيعها على الوحدات الاقتصادية المدرجة في بورصة أثينا للأوراق المالية موجهة الى المدققين الداخليين

نتائج الدراسة	اظهرت العوامل الرئيسية التي توثر على الامن السيبراني بما في ذلك درجة وطبيعة التعاون بين موظفي تقنية المعلومات والمدققين والتدريب المتعلق بتقنية المعلومات، وفيما يتعلق بالتدقيق السيبراني وسبل البحث المستقبلي هناك ضرورة لأجراء مسح في المستقبل لعينة أكبر للسماح بمزيد من الدقة في الاستنتاجات ودرجة أكبر من التعميم.

5. دراسة (محروس وصالح، 2022) بحث

عنوان الدراسة	استخدام المنهجية الرشيقة في تطوير اداء المراجعة الداخلية في الأمن السيبراني.
هدف الدراسة	1. تطوير أداء المراجعة الداخلية في منظمات الاعمال المصرية لمواجهة مخاطر الامن السيبراني باستخدام المنهجية الرشيقة. 2. تقديم مجموعة من المقترحات توضح طريقة ومراحل تطبيق المراجعة الداخلية الرشيقة لمواجهة مخاطر الامن السيبراني.
نتائج الدراسة	1. أن المنهجية الرشيقة هي إحدى المناهج الملائمة لتطوير اداء المراجعة الداخلية وبشكل خاص في مواجهة مخاطر الأمن السيبراني كونها تتيح درجة عالية من المرونة في خطط التدقيق وتعتمد على فرق العمل متعددة المهام والتخصصات وتطبق الاسلوب الاستباقي في التعامل مع المخاط ركما انها تستخدم دورات المراجعة قصيرة الاجل والتي تساعد على تقديم خدمات المراجعة في أسرع وقت ممكن وهذا يناسب مع دور المراجعة الداخلية في مواجهة مخاطر الامن السيبراني. 2. توافر مجموعة من ارشادات التطبيق التي يمكن استخدامها في مجال دور المراجعة الداخلية في مواجهة مخاطر الامن السيبراني ومنها على المستوى الدولي إطار عمل COBIT وإطار تحسين البنية الاساسية الحيوية الصادر عن NIST وكذلك مقترحات SEC ومحلياً تتوافر الاستراتيجية الوطنية للأمن السيبراني ومبادرات البنك المركزي المصري في مجال الأمن السيبراني.

من خلال ما تقدم يتضح أن الدراسات السابقة ركزت على أهمية الأمن السيبراني بصورة نظرية وفق ما يمكن أن يقوم به المدققين الداخليين من مهام وواجبات في سبيل تحقيق أهداف الأمن السيبراني. أما الدراسة الحالية فقد تميزت عن الدراسات السابقة من حيث:

1. تتطرق لموضوع الأمن السيبراني على وفق ما تم تحديده من إرشادات صادرة عن معهد المدققين الداخليين وضرورة الالتزام بها من قبل الوحدات الاقتصادية بصورة عامة وصولاً إلى تحقيق أهداف الأمن السيبراني.
2. إن الدراسات المحلية (في العراق) التي تطرقت لموضوع الأمن السيبراني قليلة جدا فاستكملت الدراسة الحالية الجهود البحثية لأثراء الأدب النظري ودعم التوجهات البحثية في المجالات البحثية، كما إنها تمثل أول دراسة محلية تطرقت لأهمية ودور التدقيق الداخلي في الأمن السيبراني (حسب علم الباحثان).

المبحث الثاني: الإطار النظري للأمن السيبراني

أولاً. مفهوم الأمن السيبراني: لقد برز مفهوم الأمن السيبراني في المقدمة في السنوات القليلة الماضية عندما كان العلماء والمتخصصين في الحاسوب وتقنية المعلومات يبحثون عن الحلول والاجراءات الممكنة للحد من التهديدات والمخاطر التي تتعرض لها الحواسيب إلا أنه وبمرور الوقت وبعد تزايد الهجمات الالكترونية وتطور تأثيرها وحجمها اتضح أن مصطلح الأمن السيبراني أبعد من كونه مجرد مفهوم يرتبط بشكل فني بتقنية المعلومات. (الشهراني وفلمبان، 2020: 622) مصطلح السيبرانية الآن هو واحد من أكثر المصطلحات تردداً في معجم الأمن الدولي، وتشير المقاربة الإيتيمولوجية لكلمة "cyber" إلى أنها لفظة يونانية الأصل مشتقة من كلمة "kybernetes" بمعنى الشخص الذي يدير دفة السفينة، حيث تستخدم مجازاً للمتحكم "governor"وتجدر الإشارة إلى أن العديد من المؤرخين يرجعون أصلها إلى عالم الرياضيات الأمريكي norbert wieners 1894-1964 وذلك للتعبير عن التحكم الآلي، فهو الأب الروحي المؤسس للسبرنيتيقية من خلال مؤلفه الشهير Cybernetics or control and communication in" the Animal and the machine وأشار في كتابه إلى أن السبرنتيقية هي التحكم والتواصل عند الحيوان والآلة والإنسان والآلة ليستبدل مصطلح الآلة بعد الحرب العالمية الثانية بالحاسوب أما الأمن لغوياً: هو نقيض الخوف، أي بمعنى السلامة. والأمن مصدر الفعل أَمِنَ أَمْناً وأَمَاناً وأَمَنَةً :أي اطمئنان النفس وسكون القلب وزوال الخوف (الموسوعة السياسية، 2019) ومفهوم الأمن بصورة عامة يطال جميع عمليات الدخول والخروج والبقاء أو التصرف في مكان ما، أما في الفضاء السيبراني فهو يشمل مختلف قواعد وأصول ضبط الاتصال ونقل المعلومات وتخزينها وحفظها وأمن الموقع وأمن النظم الالكترونية واستثمارها وأمن الاتصالات (عبد الرضا والمعموري، 2015: 153).

مفهوم الأمن السيبراني يعد من المفاهيم المعقدة التي قدمت لها العديد من التعريفات المختلفة (العمارات والحمامضة، 2022: 13) وقد احاطت بتعريف الأمن السيبراني الكثير من الجهود الرامية إلى وضع تعريف جامع ومحدد له وذلك لأنه يرتكز على مفاهيم ذات نطاق وطني وإقليمي وعالمي، ومفاهيم أخرى ذات أبعاد أمنية وتقنية واقتصادية واجتماعية وعسكرية وسياسية (عبد الرضا والمعموري، 2015: 152) ومن هذه التعريفات هي تعريف الاتحاد الدولي للاتصالات في تقريره (اتجاهات الاصلاح في الاتصالات للعام 2010-2011) هو" مجموعة من المهمات، مثل تجميع وسائل وسياسات واجراءات امنية، ومبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريبات وممارسات فضلى وتقنيات يمكن استخدامها لحماية البيئة السيبرانية وموجودات الوحدات الاقتصادية والمستخدمين " (الاتحاد الدولي للاتصالات،2011) وعرفت جمعية تدقيق ومراقبة نظم المعلومات (ISACA) الأمن السيبراني بكونه " حماية الأصول المعلوماتية من خلال معالجة التهديدات التي تتعرض لها المعلومات التي يتم معالجتها وتخزينها ونقلها من خلال نظم معلومات متصل بشبكات بينية "(ISACA, 2016)ويشير الأمن السيبراني إلى التقنيات والعمليات المصممة لحماية موارد المؤسسة معلومات - أجهزة الكمبيوتر وأجهزة الشبكة والبرامج والبيانات - من الوصول غير المصرح به أو التعطيل أو التدمير (IIA, 2022C) كما عرفت AICPA الأمن السيبراني بأنه عملية تطبيق التدابير الأمنية لضمان سرية البيانات وسلامتها وتوافرها (AICPA, 2017)

ووفقاً لما سبق يعرف الباحثان الأمن السيبراني بأنه كافة الاجراءات التقنية والادارية المتخذة بغرض حماية النظم والشبكات المعلوماتية والبيانات والمعلومات من المخاطر الناتجة عن استخدام تقنيات المعلومات (اختراق أو تعطيل أو تعديل أو دخول أو استخدام غير مصرح به) مهما كانت طبيعتها والهدف من ورائها من خلال تحقيق الأهداف وضوابط المعايير المحددة لتشخيص الثغرات والتهديدات والمخاطر ومن ثم العمل على التخفيف من آثارها عند حدوثها والتعافي منها.

ثانياً. العلاقة بين أمن المعلومات والأمن السيبراني: من أهم التحديات التي تواجه مصطلح الأمن السيبراني هي الاستخدام غير الدقيق للمصطلح حيث لا يوجد تعريف واحد متفق عليه للأمن السيبراني فهناك من يعده متداخلاً مع أمن المعلومات مدعيا أن الأمن السيبراني هو فرع من أمن المعلومات وهناك من يربط بين الأمن السيبراني والخاصية العالمية للأنترنت على أساس أنه أوسع من أمن المعلومات الذي يهتم أساسا بالسرية (Schatz, et al., 2017: 202) حيث يعرف أمن المعلومات بأنه حماية بيانات الوحدة الاقتصادية بالاعتماد على ثلاثة محاور رئيسية ويرمز لها "CIA" وهي السرية Confidentiality سلامة المعلومات Integrity اتاحة المعلومة في أي وقت Availability (السمحان، 2020: 11) أما الأمن السيبراني أتى من كلمتين (cyber security) والسيبرانية (cyber) تعني فضاء الانترنت والذي يشير إلى النظم والشبكات والأجهزة والبيانات ومعناها الفضاء المعلوماتي وبما ان كلمة security تشير الى الحماية فيصبح المقصود بالأمن السيبراني أمن الفضاء المعلوماتي وهو تعبير أوسع وأعم من أمن المعلومات (الرشيد، 2022: 14) كما كانت وجهة نظر(العمارات والحمامضة) مؤيدة لما سبق بأن الأمن السيبراني مفهوم أوسع من أمن المعلومات من حيث إن الأمن السيبراني يهتم بكل ماهو موجود على السايبر من غير أمن المعلومات بينما أمن المعلومات لا يهتم بذلك كما إن أمن المعلومات يهتم بأمن المعلومات الفيزيائية "الورقية " في حين الأمن السيبراني لا يهتم بذلك (العمارات والحمامضة، 2022: 19) وبنفس التوجه أوضحت الهيئة الوطنية السعودية للأمن السيبراني مفهوم الأمن السيبراني بكونه "حماية الشبكات ونظم تقنية المعلومات ونظم التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحتويه من بيانات من أي اختراق أو تعطيل أو دخول استخدام أو استغلال غير مشروع، ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الالكتروني والأمن الرقمي ونحو ذلك " (الضوابط الاساسية للأمن السيبراني، 2018).

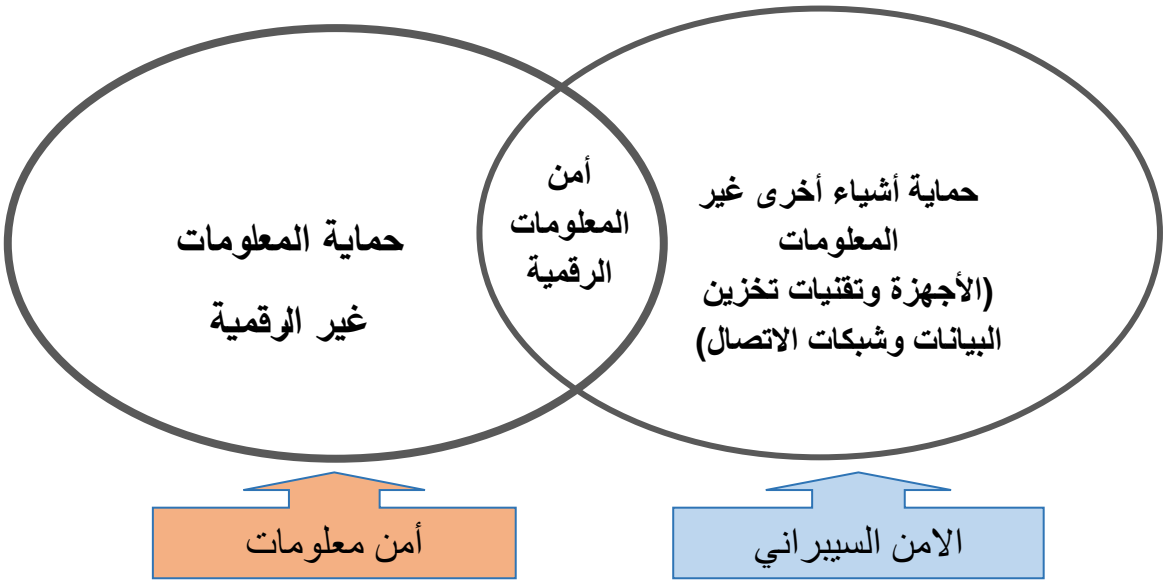
أما الرأي القائل بأن أمن المعلومات اشمل من الأمن السيبراني تبناه (بوقرص) فقد عدّ الأمن المعلوماتي أشمل من الأمن السيبراني من حيث إن أمن المعلومات يهتم بالأمن السيبراني فضلا عن تأمين كل ما هو مادي من مبانٍ وأجهزة من السرقة والتخريب والولوج غير المرخص له والكوارث الطبيعية والغبار والرطوبة وما إلى ذلك محددا أربعة أهداف رئيسية للأمن المعلوماتي السلامة، السرية، التوافر، وعدم النكران، والتنصل (بوقرص، 2022: 67) كما عدّ Couto متطلبات الأمن السيبراني مجموعة فرعية من المتطلبات العامة لأمن المعلومات وإن سياسات ومعايير الأمن السيبراني تتكامل وتتماشى مع مجموعة السياسات العامة لأمن المعلومات (Couto, 2018: 71).

التوجه الثالث هو استخدام مصطلح" أمن المعلومات "ومصطلح "الامن السيبراني" كمصطلحين مترادفين كما هو الحال في دراسة قامت بها جامعة الملك سعود بالمملكة العربية السعودية بهدف التعرف على المخاطر والتحديات التي تواجه تقنية المعلومات في الوطن العربي مبرراً ذلك بانتشار مفهوم الفضاء السيبراني الذي يرتبط ارتباطً وثيقاً بالأنترنت وبتقنية الاتصالات

والمعلومات عبر البنى التحتية المختلفة للاتصالات والنظم المعلوماتية فضلاً عن العديد من الخدمات المعلوماتية التي لم يكن ليتم الحصول عليها من دونه (Arishee, 2019: 66)

أما مؤسسة التدقيق الداخلي (Internal Audit foundation) التابع لمعهد المدققين الداخليين الدولي فقد أكدت في دراسة أجرته مع شركة المحاسبة (Crowe Horwath) على ضرورة اجراء تمييز بين وظيفة أمن المعلومات وفريق الأمن السيبراني، من حيث إن غالبا ما يتم اعتبار الأمن السيبراني مجموعة فرعية من وظيفة أمن المعلومات الأوسع المسؤول عن العديد من المجالات التي لا تكون بالضرورة مهتمة بقضايا التكنولوجيا في عالم مثالي فيه موارد غير محدودة أي إن مسؤوليات هاتين الوظيفتين يجب ان تكون مميزة بوضوح ومحددة بعناية، بالرغم من وجود تقاطع كبير بين هاتين الوظيفتين من حيث غالباً ما يكون أعضاء فريق أمن المعلومات مسؤولون عن واجبات ومخاوف محددة تتعلق بالأمن السيبراني اضافة الى قيام العديد من الوحدات الاقتصادية بتخويل جزء من برنامج الأمن السيبراني الخاص بها إلى عملاء الجهات الخارجية بما في ذلك الأمان المدار (Jamison, et al., 2018: 8).

بالاستناد لما تقدم يرى الباحثان أن مفهوم الأمن السيبراني أوسع وأشمل من مفهوم أمن المعلومات باعتباره المجال الذي يعنى بأمن كل ما هو موجود في السايبر ومن ضمنه أمن المعلومات فهو يحمي الفضاء الالكتروني نفسه وكل من يستخدمه من أفراد ومنظمات ودول وحماية تقنية الاتصالات والمعلومات الإلكترونية. ومما يعني بذات الوقت وجود علاقة تقاطع بين المفهومين من حيث الاهتمام بالمعلومات الرقمية الموجودة في السايبر، فأمن المعلومات له دور في حماية كافة البيانات والمعلومات اينما وجدت أما الأمن السيبراني يشار إليه بكونه حماية الأجهزة وتقنيات تخزين البيانات وشبكات الاتصال الالكترونية وبما يعمل على حماية البيانات المتواجدة في الفضاء السيبراني كما هو موضح بالشكل الآتي:



الشكل (1): العلاقة بين الأمن السيبراني وأمن المعلومات

المصدر: من إعداد الباحثان.

ثالثاً. أهداف الأمن السيبراني: للأمن السيبراني أهداف عدة ومن أهمها هي (المنتشري والحريري، 2020: 104):

1. سد الثغرات في أمن نظم المعلومات وتعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من اجهزة وبرمجيات وما تقدمه من خدمات وما تحويه من بيانات.
2. التصدي لهجمات وحوادث أمن المعلومات التي تستهدف الأجهزة الحكومية ومؤسسات القطاع العام والخاص والحد من التجسس والتخريب الإلكتروني على مستوى الحكومة والأفراد.
3. توفير المتطلبات اللازمة للحد من المخاطر والجرائم السيبرانية التي تستهدف مستخدمي تقنية المعلومات والاتصالات وصمود البنى التحتية الحساسة للهجمات الالكترونية.
4. تدريب الأفراد على إجراءات وآليات جديدة تمكنهم من مواجهة التحديات الخاصة باختراق اجهزتهم التقنية بقصد سرقة او اتلاف معلوماتهم الشخصية.
5. مقاومة البرمجيات الخبيثة التي تستهدف أحداث أضرار بالغة للمستخدمين ولنظم المعلومات.
6. التخلص من نقاط الضعف في نظم الحاسب الآلي والأجهزة المحمولة باختلاف أنواعها.

واضاف الشهراني الهدفين الآتيين (الشهراني وفلمبان، 2020: 623):

1. اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حد سواء من المخاطر المحتملة الناتجة عن سوء استخدام الانترنت
2. حماية خصوصية البيانات السرية والشخصية

ويعد الهدف الأسمى للأمن السيبراني من وجهة نظر الباحثان وبالاستناد لما سبق هو القدرة على مقاومة التهديدات والجرائم السيبرانية والتخفيف من آثارها واعادة الوضع إلى ما كان عليه بأسرع وقت بضمان الاستجابة المناسبة للحوادث السيبرانية والتعافي منها للمحافظة على سمعة الوحدات الاقتصادية وتوفير بيئة أمنة موثوق بها في التعاملات التي تجري فيها بالتقليل من عمليات الاختراق والتجسس لشبكاتها الالكترونية وغيرها من المخاطر السيبرانية والتخلص منها بأقل ضرر.

رابعاً. اهمية الامن السيبراني: يعد الأمن السيبراني جزءاً مهماً للأفراد والمنظمات والحكومات والمؤسسات التعليمية، حيث أصبح من الضرورة للعائلات حماية أفراد الأسرة من الاحتيال عبر الانترنت ومن الناحية المالية ضرورة تأمين المعلومات المالية التي يمكن أن تؤثر على الوضع المالي الشخصي، هناك حاجة حيوية لمستخدمي الانترنت لفهم كيفية حماية انفسهم من الاحتيال عبر الانترنت وسرقة الهوية ويؤدي التعلم المناسب عن السلوك عبر الانترنت وحماية النظام الى تقليل نقاط الضعف وجعل بيئة الانترنت أكثر أماناً ولقد واجهت المنظمات الصغيرة والمتوسطة تحديات أمنية مختلفة بسبب محدودية موارد ومهارات الأمن السيبراني (Goutam, 2015: 14) فالأمن السيبراني له أهمية كبيرة في كافة المجالات التي يتم فيها استخدام تقنيات المعلومات وتكمن هذه الأهمية بما يأتي (السمحان، 2020: 12):

1. توفير الحماية الفائقة لخصوصية المعلومات والابقاء على سريتها، وذلك بعدم السماح بالوصول إليها واستخدامها لغير المخولين بذلك ووفرة البيانات وجاهزيتها عند الحاجة اليها.
2. الحفاظ على سلامة المعلومات وتجانسها بكف الأيادي العابثة فيها.
3. تعمل على توفير بيئة عمل آمنة جداً عند العمل عبر الشبكة العنكبوتية.

أضاف العمارات والحمامضة إلى أهمية الامن السيبراني الاتي (العمارات والحمامضة، 2022: 36):

1. حماية كافة الشبكات والأجهزة من الاختراقات وذلك لتكون درع واقي للبيانات والمعلومات.
2. استخدام الادوات الخاصة بالمصادر المفتوحة والعمل على تطويرها وذلك لتحقيق مبادئ الأمن السيبراني وكشف نقاط الضعف والثغرات الموجودة في النظم ومعالجتها.

واستناداً لما سبق يرى الباحثان أن أهمية الأمن السيبراني تكمن في الاستفادة من برامج الدفاع السيبراني سواء كان على المستوى الفردي بالحفاظ على الهوية والبيانات المهمة من السرقة أو الفقدان أو على مستوى المجتمع بتأمين حماية البنية التحتية الحيوية كمحطات الطاقة والمستشفيات وشركات الخدمات المالية وغيرها من التهديدات السيبرانية وضمان عملها بطريقة آمنة وطبيعية.

يستخلص الباحثان مما تقدم أن الوحدات الاقتصادية بمختلف أنشطتها تواجه تحديات كبيرة تحتم عليها ضرورة استخدام التقنيات الحديثة، إذ أفرزت البيئة الجديدة لها العديد من المتغيرات التي لم تكن موجودة في ظل استخدام الأساليب التقليدية التي تعتمد على النظم اليدوية آنذاك حيث اصبحت التقنية في وقتنا الراهن متغلغلة في الوحدات وتؤدي دورا مهماً فيها، إلا أن نمو بيئة تقنية المعلومات والاتصالات مصحوب بتهديدات جديدة وخطيرة حيث تمتلك الهجمات السيبرانية الآن القدرة على إلحاق ضرر كبير بالمجتمع بطرق جديدة وحاسمة، وكنتيجة حتمية لحاجة بيئة الأعمال إلى تكيف أدواتها والساعي الدائم نحو الحد من المخاطر السيبرانية ظهرت الحاجة الملحة إلى اعتماد سياسات واجراءات أمنية والذي هو في الأساس عملية أمان وسلامة الفضاء السيبراني من التهديدات لضمان الحفاظ على البيانات الإلكترونية في مأمن من الوصول غير المصرح به أو الضرر والحفاظ على أنواع أخرى من معدات المعالجة الإلكترونية، وهنا يمكن أن تؤدي عملية التدقيق الداخلي دورا هاما فيها، فالتغييرات في بيئة الأعمال لها تأثير وبشكل كبير على التدقيق الداخلي وتحديدا الحاجة إلى تولي أدوار ومسؤوليات جديدة نحو دور استشاري إداري نتيجة للمعرفة الجيدة بنماذج الأعمال والعمليات داخل المنظمة، وبالتالي تقديم توصيات لتحسين الأمن السيبراني من خلال تقييم المخاطر السيبرانية وتوفير توكيد فيما يتعلق بأمن المعلومات.

المبحث الثالث: أهمية التدقيق الداخلي لأغراض الامن السيبراني

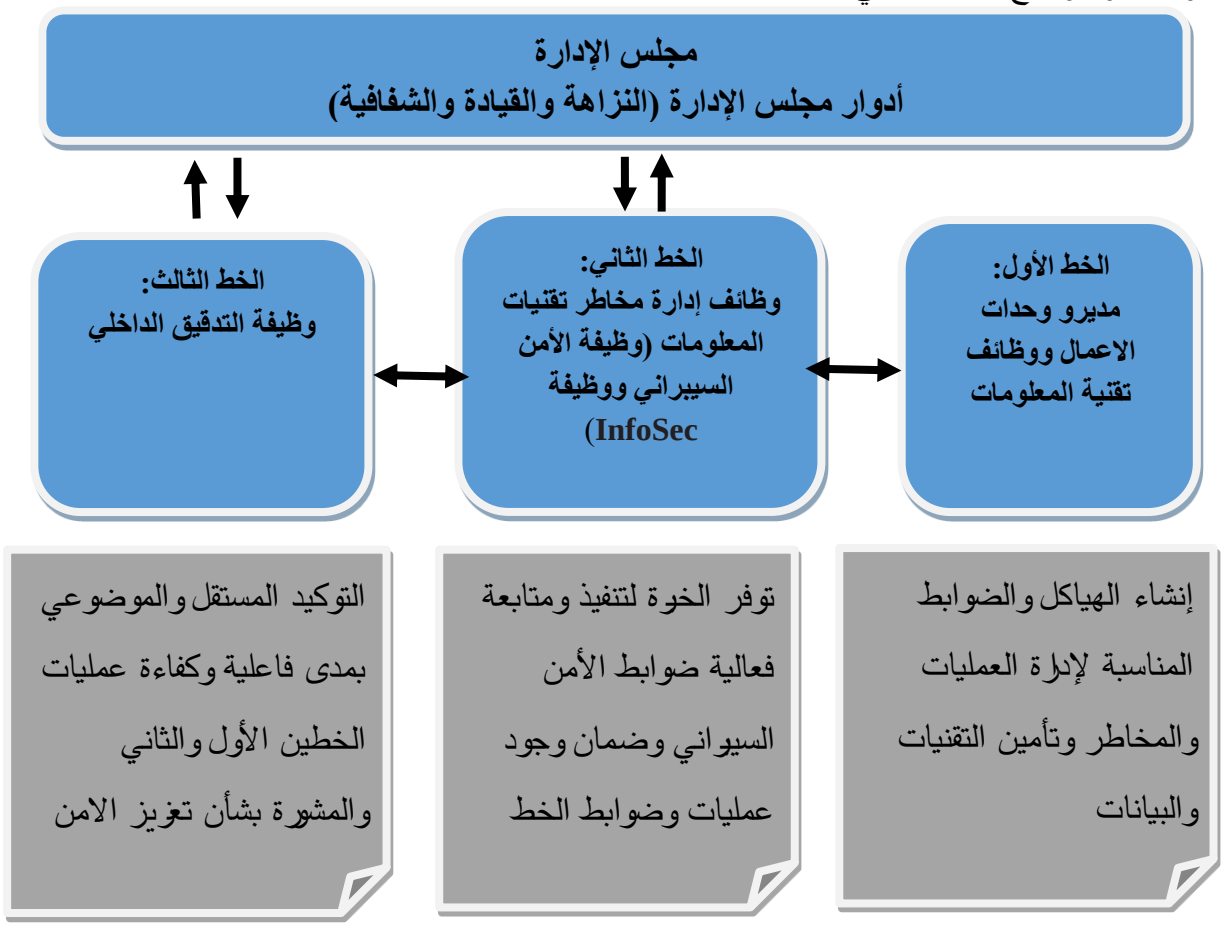
في السنوات الأخيرة كانت الوحدات الاقتصادية تسعى جاهدة لابتكار طرق أكثر فعالية لتحسين أدائها مع الحفاظ على حصتها في السوق وتحقيق ميزة تنافسية وهنا يؤدي نظام الرقابة الداخلية القوي والتي تشكل عملية التدقيق الداخلي أحد عناصره والمصمم لإضافة قيمة وتحسين الإجراءات دوًرا رئيسًيا في منع الهجمات الإلكترونية واكتساب مديري تنفيذيين مؤهلين للوقاية من هذه المخاطر(Lois, et al., 2020: 2).

وبما إن تحسين الأمن السيبراني يجب أن يحدث في أسرع وقت للبقاء على قيد الحياة ومواكبة التطور في التهديدات الالكترونية باعتماد سياسات أمنية واسعة النطاق ومتطورة يتم اتباعها من قبل كل موظف لتحسين اجراءات أمن المعلومات في الوحدة الاقتصادية والتي يجب أن تخضع وباستمرار للتقييم المستمر لمدى فعالية تنفيذها ومدى تماشيها مع أهداف العمل، فقد أدركت العديد من الوحدات الاقتصادية الحاجة إلى خط ثالث للدفاع السيبراني لتقديم مراجعة مستقلة للتدابير الأمنية والأداء من قبل وظيفة التدقيق الداخلي الذي يجب أن يؤدي دوًرا أساسياً في تقييم وتحديد الفرص لتعزيز أمن الوحدة الاقتصادية (Deloitte, 2017) فوفقاً لما جاء بتقرير IIA الصادر في ابريل 2022 أن

الهجمات السيبرانية تتزايد بشكل كبير نتيجة للعديد من الأزمات بما في ذلك أزمة اوكرانيا وتهديدات وباء كورونا التي لاتزال مستمرة اضافة الى التوترات بين الولايات المتحدة الامريكية والصين وإن هذه التوترات والأزمات اجتمعت مع متغيرات أخرى دفعت بمخاطر الأمن السيبراني إلى قمة أولويات التدقيق الداخلي (IIA, 2022a)

وتؤدي أجزاء كبيرة من الحوادث السيبرانية إلى اضطراب الأعمال وفقدان الدخل والتكاليف الإضافية والإضرار بالسمعة المنظمات تواجه عدداً مزعجًا من مشكلات الأمن السيبراني من مختلف الأنواع والأحجام والفشل في تحليل التحديات ومن الواضح أن أقسام تقنية المعلومات (IT) لديها التزامات حقيقية تتعلق بهذه المجالات، أن الهجمات الإلكترونية هي حقيقة الأعمال التجارية اليوم ولكن يمكن لوظيفة التدقيق الداخلي القوية أن توفر نهجًا شاملاً للأمن السيبراني الذي يحتاج إلى البقاء (Shamsuddin, 2018: 63)

وفي ظل البيئة المتغيرة والمليئة بالمخاطر يرى الباحثان ضرورة ادراج الأمن السيبراني ضمن استراتيجية ادارة المخاطر للمؤسسة واعتماد ضوابط وعمليات واضحة وقوية مبنية على اساسيات هامة للأمن السيبراني على مستوى الوحدة الاقتصادية ككل وتفعيل أدوار للخطوط الثلاثة وكما هو موضح بالشكل الآتي:



الشكل (2): من اعداد الباحثان اعتماداً على

(IIA,2020a) (Kahyaoglu, & Caliyurt 2018) (Slapnicar et al.: 2022)

ومن أحد الأخطاء الجسيمة لمجالس الادارة أن تفترض أن التدقيق الخارجي يوفر كل التأكيدات التي تحتاجها المنظمة فيما يتعلق بالأمن السيبراني والتقارير غير المالية والاستدامة حيث يوفر منظور التدقيق الداخلي رؤية أعمق وأشمل تنعكس من أهدافه كما يوفر التأكيد المستقل على المخاطر والضوابط قبل أن يتم ذلك من قبل التدقيق الخارجي (IIA,2022a)

فالمدققون الداخليون يوفرون ضماناً للأمن السيبراني من خلال استقلاليتهم في الوقت الذي يكون فيه معظم الموظفين في الوحدة الاقتصادية مثل قسم تقنية المعلومات والوظائف الامنية لا يمكنها ان توفر ضمان موضوعي ومستقل لمجلس الادارة فعندما يتعلق الأمر بالأمن السيبراني أعضاء مجلس الادارة يفضلون المدققون الداخليون كونهم يتمتعون بالاستقلالية، فخدمات التأكيد المقدمة من قبلهم تستخلص قيمتها وموثوقيتها من الافتراضات الرئيسية لـاستقلالية العقل والمظهر المعترف به في الأطر والمعايير العالمية (Simić, 2022: 14)

وإن حاجة أعضاء مجالس الادارة في بعض الوحدات الاقتصادية إلى فهم واضح للمخاطر السيبرانية التي تتعرض لها الوحدة والتي تكون الصورة فيها غير واضحة يجعل مجالس الادارة ولجان التدقيق والامتثال التابعة لها تطالب التدقيق الداخلي تقديم ضمانات بشأن ادارة الوحدة الاقتصادية للمخاطر الالكترونية فبالرغم من استفادة الهيئات الادارية هذه من تعليم الأمن السيبراني الذي يقدمه كبير مسؤولي المعلومات (CIO) وكبير مسؤولي التقنيات وكبير مسؤولي أمن المعلومات (CISO) إلا أن جهود التعليم هذه قد لا تفي باحتياجات مجالس الادارة للوضوح والفهم (Kahyaoglu, Caliyurt, 2018: 369).

تتداخل وظيفة التدقيق الداخلي مع الأمن السيبراني بطرق عدة حيث يؤدي متخصصو أمن المعلومات وقدرات التدقيق الداخلي دورا مهما في منع واكتشاف مخاطر الأمن السيبراني، أن التحكم في أمن المعلومات وتحسينه هو مسؤولية وظيفة تقنية المعلومات ووظيفة التدقيق الداخلي، ووظيفة التدقيق الداخلي مهمة للغاية لنجاح الوحدة الاقتصادية فهي تقدم تأكيدات موثوقة وموضوعية لمجلس الإدارة وكبار موظفي الإدارة المتعلقة بالحوكمة والمخاطر والرقابة (Simić, 2022: 7) فالعديد من لجان التدقيق ومجالس الإدارة لديها توقعات متزايدة لموظفي التدقيق الداخلي بفهم وتقييم قدرات الوحدة الاقتصادية في إدارة المخاطر المرتبطة بالأمن السيبراني ولديهم توقعات ذات صلة ومباشرة لزيادة مستويات احتراف المدقق والتدريب (Islam, 2018: 4).

انطلاقاً من مقولة الاتحاد الأوروبي لمعهد المدققين الداخليين في تقرير التركيز عن المخاطر لعام 2022 " لقد تغير العالم يجب أن يتغير التدقيق الداخلي أيضا " ومما ورد مسبقاً يرى الباحثان ان وظيفة التدقيق الداخلي قد ازدادت اهميتها في وقتنا الحالي، وأصبح نشاطاً تقويمياً واستشارياً لكافة الأنشطة والعمليات في المنشأة، بهدف تطوير هذه الأنشطة ورفع كفايتها الإنتاجية، وتعود أهمية هذه الوظيفة للخدمات التي تقدمها للإدارة في مختلف المجالات وفي الوقت الذي زاد فيه التدقيق الداخلي بالفعل من تركيزها على مجالات المخاطر الناشئة بما فيها المخاطر السيبرانية بدأت مجالس الإدارات وأصحاب المال ورجال الأعمال في الشعور بأنهم بحاجة إلى خط ثالث للدفاع السيبراني المتمثل بوظيفة التدقيق الداخلي بتقديم مراجعة مستقلة للتدابير الأمنية والأداء فضلا عن الدور الأساسي الذي يمكن أن يتبناه في تقييم وتحديد الفرص لتعزيز أمن الوحدة الاقتصادية السيبراني ولتأدية هذا الدور يتوجب وجود مجموعة المتطلبات اللازمة لذلك وهذا ما سنتناوله في المبحث القادم.

المبحث الرابع: متطلبات تطبيق إرشادات معهد المدققين الداخليين لتعزيز الأمن السيبراني في الوحدات الاقتصادية

يعد المدقق الداخلي مقدم ضمان مستقل ضرورياً للإدارة السليمة للمخاطر والحوكمة والمساعدة في ضمان فعالية برامج ادارة مخاطر الأمن السيبراني التنظيمي، وتحقيقاً لهذه الغاية تعتبر العديد من الوحدات الاقتصادية IAFكخط حاسم للدفاع الإلكتروني، مما يوفر مراجعة مستقلة للتدابير الأمنية وأدائها وبالتالي يجب على التدقيق الداخلي تحديد نقاط الضعف وتقييم مدى كفاية الضوابط والسياسات والإجراءات المعمول بها والمساعدة في ضمان تلبية إرشادات الأمن السيبراني التنظيمية مثل إفصاحات SEC ومتطلبات Sarbanes Oxley ومتطلبات Hipaa (Islam, 2018: 5) وتحقيق هذا الدور الرئيسي داخل الوحدات الاقتصادية يتطلب من المدققين الداخليين فضلا عن مدونة قواعد الاخلاق الصادرة عن معهد المدققين الداخليين الدولي (IIA) النظر في المعايير الدولية للممارسة المهنية للتدقيق الداخلي (IIA, 2017) واطار الممارسة المهنية الدولية (IPPF)، وفي هذا السياق تم تطوير أطار الممارسة المهنية الدولية وذلك لتنظيم مجموعة كاملة من ارشادات التدقيق الداخلي من IIA Global بطريقة يسهل الوصول إليها متضمنا نوعين من التوجيه وهما. (Kahyaoglu, Caliyurt, 2018: 370):

1. التوجيه الالزامي: يطلب من أعضاء IIA الامتثال للتوجيهات الالزامية وتم تطوير الدليل بعد التشاور مع الأعضاء.
2. التوجيه الموصى به وفيه يوصى أعضاء IIA الامتثال لهذا التوجيه وهو يصف ممارسات التنفيذ الفعال للمبادئ الأساسية.

وبالاستناد إلى ارشادات معهد المدققين الداخليين الخاصة بالأمن السيبراني ونتائج الدراسات السابقة يمكن تحديد أهم المتطلبات الواجب توافرها لتمكين التدقيق الداخلي من القيام بتعزيز الأمن السيبراني بشكل فاعل في الوحدات الاقتصادية التي يعمل فيها بالآتي:

1. **المتطلبات الخاصة بصفات المدقق الداخلي واداءه:** وهو يتضمن وجوب توافر لدى المدقق الداخلي فهم أساسي لوظائف وعمليات تقنية المعلومات في الوحدات الاقتصادية التي يعملون بها، أي أصبح مطلوبا من المدققين الداخليين فهم بيئة الضوابط الرقابية في الوحدة الاقتصادية، وذلك لتقديم تأكيدات للجنة التدقيق ومجلس الادارة فيما إذا كانت الضوابط المطبقة مناسبة لتحقيق الهدف منهما سواء فيما يتعلق بالحوكمة أو تقييم المخاطر السيبرانية أو إدارة الخطر السيبراني بالنظر لما ورد في المعيار (1210 الكفاءة) يجب أن يكون لدى المدققين الداخليين معرفة كافية بمخاطر وضوابط تقنية المعلومات الرئيسية وتقنيات التدقيق المعتمدة على التقنية لأداء العمل المنوط بهم، مع ذلك لا يُتوقع أن يتمتع جميع المدققين الداخليين بخبرة المدقق الداخلي الذي تتمثل مسؤوليته الأساسية في تدقيق تقنية المعلومات.(وهذا الفهم يتم الحصول عليه من خلال الاستعانة بمصادر خارجية او داخلية المتخصصين بالأمن السيبراني والحصول على شهادات الأمن المناسبة مثل الشهادات الأمنية (CISM, CSP) وشهادات تدقيق أمن نظم المعلومات مثل شهادة (QICA, CISA) أو الحصول على دورات تدريبية متخصصة والمؤهلات الاكاديمية والشهادات المهنية بمجال تحديد المخاطر السيبرانية وادارتها لتمكين المدققين الداخليين من القيام بدورهم بشكل فاعل وكفوء في كافة مراحل التعامل مع الهجمات السيبرانية حيث إن هذا الفهم سيمكنهم من تقديم نتائج التدقيق السيبراني مضيفة للقيمة تعمل على تحسين الأمن السيبراني بالوحدات الاقتصادية، وكذلك فأن الأمانة والموضوعية

والشهادة في العمل من الصفات التي يجب ان يتسم بها موظفي التدقيق الداخلي عند تدقيق الأمن السيبراني.

تدقيق الأمن السيبراني بجودة عالية يتطلب تأهيل فريق التدقيق الداخلي بالمنشأة بمعرفة متطورة بتقنية المعلومات (IT) ذات الصلة ومخاطرها بما في ذلك الحواسيب المركزية والشبكات والجدران النارية ونظم ادارة الشبكات وبروتوكولات الأمان ونظم التشغيل والكفاءة في قياس الأداء مقابل المعايير المعمول بها وتطبيق الاجراءات المناسبة للتقييم مقابل تلك المعايير والإبلاغ عن النتائج، وأن يكون لديهم القدرة على التحكم في أساليب التدقيق القائمة على التقنية الحديثة والمتاحة لأداء انشطة التدقيق الداخلي وبالتالي القدرة على تطوير علاقات أعمق مع وظائف أمن نظم المعلومات ومن ثم المساهمة في بناء برنامج إدارة الأمن السيبراني أكثر فعالية وجودة.

كما يجب أن يكون لدى المدققين الداخليين معرفة وافية بأهم مخاطر الفضاء السيبراني والضوابط الرقابية المتعلقة به ويتطلب من المدققين الداخليين مواكبة التهديدات الالكترونية باستمرار وما يمكن أن يقوم به المسؤولين عن الأمن السيبراني لإدارة المخاطر السيبرانية ومدى امتثال الموظفين للإجراءات المعمول بها وماهية التدابير المتخذة من قبل قادة وحدات الأعمال وماهي نقاط الضعف والثغرات الأمنية لتقنية المعلومات المتعلقة بالطرف الثالث ولاسيما فيما يتعلق بالخدمات السحابية ومقدمي خدمات تقنية المعلومات الأخرين ليتمكن من تقديم الاستشارة الفاعلة لمجلس الإدارة التي تعمل على تعزيز الأمن السيبراني بالوحدة الاقتصادية، إلا أنه غالبا ما يواجه المدقق صعوبات في طريقة تقديم الخدمة الاستشارية (CE) التي قد تمس باستقلاليته، مما يتطلب دوما استرشاده بالمعايير المهنية التي تساعده على تجاوز تلك الصعوبات، فالتدقيق الداخلي نشاط مستقل بمعنى أنه غير تابع فيما يتعلق بالسلطة والمسؤولية الى الجهات الخاضعة للتدقيق، وبذلك يجب أن يتبع أعلى المستويات الادارية في الوحدة الاقتصادية. أي يجب على مجلس الادارة أو لجنة التدقيق ضمان استقلالية وظيفة التدقيق الداخلي من خلال ارتباطها المباشر مع المجلس أو اللجنة، ومن خلال التقارير المرفوعة إلى المجلس أو اللجنة.

2. **الدعم الكافي والمركز التنظيمي المناسب للمدقق الداخلي:** لكي يتمكن التدقيق الداخلي من اداء مهامه ومسؤولياته المتعلقة بالأمن السيبراني للوحدات الاقتصادية التي يعمل بها يتوجب أن يتلقى المدققون الداخليون الدعم الكافي من مجلس الادارة بإتاحة الوقت وتوفير الموارد المالية اللازمة ودعم مشاركتهم في طرح وتطوير الرؤى حول المخاطر السيبرانية، فضلا عن منحهم الصلاحيات التي تمكنهم من أداء أعمالهم بمرونة كافية حيث نادراً ما تعطّي الوحدات الاقتصادية تفويضاً كاملا للمدقق الداخلي للاطلاع على كافة المعلومات والبيانات بسبب وجود مناطق أو مجالات ذات خصوصية يتعذر وصول المدقق إليها بدون الحصول على تفويض خاص وفي حالات أخرى، يحتوي نص التعاقدات القانونية للوحدة مع العملاء والموردين على بند خاص يعطي الحق للمدقق الداخلي في تدقيق حساباتهم حال قيامهم بالتعامل مع هذه الاطراف الثالثة من خلال أجهزة الهاتف المحمولة على سبيل المثال، وهذا ما أشار إليه المعيار الدولي 2220 أ (يجب أن يشمل نطاق المهمة النظر في النظم والسجلات والموظفين والممتلكات المادية ذات الصلة، بما في ذلك تلك الواقعة تحت سيطرة أطراف ثالثة)، أي يجب ان يكون التدقيق الداخلي في المركز الوظيفي المناسب ويمتلك الموارد الكافية حيث لا يمكن المحافظة على النزاهة والموضوعية والاستقلالية دون أن يكون التدقيق الداخلي في المركز الوظيفي المناسب ويتوفر لديه الموارد الكافية لتأدية مهامه.

إعطاء المدقق الداخلي المكانة التي تمكنه من المشاركة في ادارة المخاطر بالوحدة الاقتصادية بما فيها المخاطر السيبرانية تجعله يتبنى نهج التفكير الابتكاري الاستراتيجي والتركيز على أهداف العمل بدلًا من أهداف التدقيق فقط وهذا سيؤدي إلى تقديم وجهات نظر ونتائج موضوعية إلى لجنة التدقيق وأعضاء مجلس الادارة من خلال إجراء تقييم شامل للمخاطر السيبرانية، حيث يقدم المركز التنظيمي المناسب مساعدة في توفير السبل لقسم التدقيق الداخلي في الحصول على مقدار كافي من المعلومات بالشكل الملائم التي يمكن الاستناد عليها في تنفيذ مهامه المختلفة.

3. **تحديث منهج التدقيق واعتماد اعتبارات خاصة بعملية التخطيط:** من الآليات والعمليات التي تدعم الأمن السيبراني لمنع التهديدات السيبرانية تعديل أطار التدقيق التقليدي للسماح بمجموعة من خدمات التأكيد في العصر الحديث مما يعني اعادة النظر في نموذج التدقيق التقليدي لتطوير خدمات ضمان جديدة لاسيما فيما يتعلق بالأمن السيبراني والضمان المستمر (Kahyaoglu, Caliyurt, 2018: 364).

أن القيام بعملية تدقيق الأمن السيبراني يتطلب إعادة النظر في ثلاثة عناصر أساسية على الأقل من نموذج التدقيق التقليدي، التقرير الزمني المحدد، الطبيعة الصفرية (الواحدة للرأي)، مفهوم التمثيل العادل (الأهمية النسبية)، هذه العناصر جوهرية لعصر مختلف وتقنية مختلفة، واحتياجات مختلفة للمستثمرين وأصحاب المصلحة الآخرين من الوحدات الاقتصادية وقد يتطلب الأمر اجراء بعض التعديلات المتمثلة بتوقيت وتكرار عملية التدقيق وزيادة التعلم بالتقنيات والأساليب التحليلية المستخدمة في عملية التدقيق واعتماد الفحص الشامل بدلاً من العينات، حيث يتجاهل النهج التقليدي لتعريف المعايير دمج الطبيعة المتغيرة باستمرار لتهديدات الأمن السيبراني على سبيل المثال لا يتضمن تحليلاً للتأثيرات المحتملة التي قد يحدثها الفشل في نظام الأمن السيبراني علاوة على ذلك، ظهرت مجموعة من التقنيات والعمليات التحليلية التي تعمل على تحسين جودة التصديق أو التدقيق ومع ذلك، فإن مثل هذه التقنيات والعمليات التحليلية لا تتوافق بشكل جيد مع معايير التدقيق التقليدية وقد يتم تغيير عملية التدقيق بأكملها. فمن الضروري إخضاع معايير التدقيق الداخلي إلى عملية تقويم وتطوير مستمرة لتسهيل وضبط عمل المدققين الداخليين في ظل هذه المعايير وكجزء من الاستجابة للحوادث السيبرانية العالمية ومستجداتها وكعلاج لها في تطوير دور التدقيق الداخلي والوظائف التي يؤديها، فالتعامل مع مخاطر الأمن السيبراني لا يتسق معه تطبيق المنهج التقليدي للتدقيق كما إنه يتطلب توافر عدة مقومات غير موجودة بالمنهج التقليدي للتدقيق لذا فأن الدور المتأمل للتدقيق الداخلي يتطلب اتباع منهجيات حديثة تتوافق مع بيئة الأعمال المتغيرة وسرعة وتعقيد الهجمات السيبرانية كالمنهجية الرشيقة Roach Agile التي تهدف إلى تطوير أداء التدقيق الداخلي والانتقال بها من المنهج التقليدي إلى منهج يعتمد على المرونة وسرعة أداء المهام والتواصل والتفاعل مع مختلف اصحاب المصلحة.

فضلا عما سبق إن وظيفة التدقيق الداخلي تحتاج إلى وضع خطة لتقييم المخاطر السيبرانية وتقييم الاجراءات التي تتخذها الادارة للتخفيف من هذه المخاطر وما إذا كانت بحاجة إلى تحسين وهذا يتطلب أن يكون تخطيطاً سنوياً وأن يتم تحديثها كلما استجدت احداث جديدة ومخاطر سيبرانية جديدة بالوحدة الاقتصادية حيث إن تخطيط عملية التدقيق تعد نقطة البداية للقيام بعملية التدقيق ليتمكن من تقديم توكيد مرتكز على المخاطر. فهذا المبدأ يعد الدور الأساسي للتدقيق الداخلي والذي لا بد له أن يقضي أغلب وقته لتحقيقه لذا لا بد من تطوير خطة تدقيق مبنية على المخاطر مع الأخذ بالاعتبار إطار المخاطر الذي تبنته الوحدة الاقتصادية، حيث يتمثل الغرض من التخطيط السنوي للتدقيق

السيبراني في ضمان توافق انشطة التدقيق مع احتياجات الوحدة الاقتصادية وإضافة القيمة لتحقيق الأهداف السيبرانية المحددة مسبقاً، كما يساعد التخطيط السنوي في الاستغلال الأمثل للموارد المحددة لعملية التدقيق.

وبهذا الخصوص أوصت إرشادات الأمن السيبراني الصادرة من معهد المدققين الداخليين في مايو 2020 بوضع خطة التدقيق على أساس تقييم المخاطر، بما في ذلك وضع تخطيط شامل تستجيب للمخاطر مع التركيز على المخاطر التي تؤثر على تحقيق الوحدة الاقتصادية لأهدافها بشكل كبير (IIA, 2020b).

4. **العمل التعاوني مع فرق تقنية المعلومات والأمن السيبراني:** الأمن السيبراني ليست مسؤولية شخص واحد فقط أو فريق واحد هي مسؤولية الوحدة الاقتصادية بأكملها، منذ ذلك الحين التعاون بين المدققين الداخليين والفرق الأخرى (على سبيل المثال، تقنية المعلومات التشغيلية، وأمن المعلومات) يؤدي إلى اعادة هندسة تطبيق البيئة الرقابية وإدارة مخاطر الأمن السيبراني بشكل أفضل، والمدققين الداخليين بحاجة إلى فهم المخاطر السيبرانية وفهم العمل الذي يقوم به CIO وCISO لتوفير التوكيد المناسب للشركة بأن مخاطر الأمن السيبراني يتم تحديدها بشكل صحيح وتحديد أولوياتها والتخفيف من حدتها وهذا يتطلب تكوين علاقة قوية وموثوقة مع هذه المهن لتطوير خطة التدقيق الداخلي بشكل مشترك وتوجيه الموارد إلى المجالات الأكثر قلقاً ومخاطرة للمؤسسة، فقيام الوظيفتين بتوضيح وجهة نظر متسقة ومتماسكة للمخاطر هو وسيلة فعالة لموازنة المخاطر الالكترونية.

تعد المشاركة المبكرة مع وظائف تقنية المعلومات والأمن السيبراني أمرًا ضروريًا لمساعدة وظيفة التدقيق الداخلي على فهم وجهات نظرهم وأولوياتهم الرئيسية، ستساعد المناقشات المبكرة الفرق على فهم أي عمل حاسم مطلوب، وما إذا كانت هناك أي مخاطر سيبرانية جديدة أو مرتفعة يجب دمجها في خطة التدقيق الداخلي السنوية كما تعمل على تقليل ازدواجية الأعمال والجهود وهذا ما أشار إليه المعيار (2050) التنسيق والاعتماد (يجب على الرئيس التنفيذي للتدقيق الداخلي مشاركة المعلومات وتنسيق الأنشطة والنظر في الاعتماد على عمل مقدمي خدمات الضمان والاستشارات الداخليين والخارجيين الآخرين لضمان التغطية المناسبة وتقليل ازدواجية الجهود) كما أشارت إرشادات معهد المدققين الداخليين إلى أن العمل بشكل وثيق مع تقنية المعلومات ونظم المعلومات، يمكن نشاط التدقيق الداخلي أن يضمن حصول الإدارة العليا ومجلس الإدارة على رؤية واضحة وشاملة لاستعداد الوحدة الاقتصادية للحوادث السيبرانية، ومن شأن هذه الرؤية أن تتضمن تقييمًا لمدى كفاية وفعالية ضوابط الاستجابة والاسترداد، وتحديد المخاطر المتبقية التي قد تتطلب مزيدًا من التخفيف (IIA, 2022c). وبهذا الصدد عند تدقيق العمليات التي يفترض أدائها من قبل خطي الدفاع الأول والثاني يتطلب من المدققين الداخليين اعتماد أطار عمل يستند إلى أحد معايير الأمن السيبراني ليتمكن من القيام بعملية التدقيق بشكل منهجي حيث إنها ستحدد نطاق عملية التدقيق التي يقوم بها المدقق الداخلي وقد أشارت إرشادات الأمن السيبراني إلى أن نشاط التدقيق الداخلي يضيف قيمة للمؤسسة عندما تقدم مثل هذه الخدمات وفقًا للمعايير ومع إشارات إلى أطر الرقابة المقبولة على نطاق واسع، لا سيما تلك المستخدمة من قبل وظائف تقنية المعلومات وأمن المعلومات بالمنظمة وسيسمح تدقيق واحد أو أكثر من أطر التحكم في IT-IS، (مثل أطر ISACA وNIST) لنشاط التدقيق الداخلي استكمال معرفته الجماعية بأفضل ممارسات الرقابة (IIA, 2020c)، وبهذا الخصوص تتعدد المعايير إلا أن المدقق الداخلي يجب أن يستخدم اطر عمل ومعايير متماثلة مع ما هو معتمد من

قبل أقسام الأمن السيبراني وتقنية المعلومات لضمان التطابق والتماثل في المصطلحات المستخدمة في التقارير الموجهة إلى مجلس الادارة.

الاستنتاجات والمقترحات

أولاً. الاستنتاجات:

1. مفهوم الأمن السيبراني اوسع واشمل من مفهوم أمن المعلومات بعدّه المجال الذي يعنى بأمن كل ما هو موجود في السايبر ومن ضمنه أمن المعلومات فهو يحمي الفضاء الالكتروني نفسه وكل من يستخدمه من أفراد ومنظمات ودول وحماية تقنية الاتصالات والمعلومات الإلكترونية.
2. الهدف الأسمى للأمن السيبراني هو القدرة على مقاومة التهديدات والجرائم السيبرانية والتخفيف من آثارها واعادة الوضع إلى ما كان عليه بأسرع وقت بضمان الاستجابة المناسبة للحوادث السيبرانية والتعافي منها للمحافظة على سمعة الوحدات الاقتصادية وتوفير بيئة أمنة موثوق بها في التعاملات التي تجري فيها.
3. أهمية الأمن السيبراني تكمن في الاستفادة من برامج الدفاع السيبراني سواء كان على المستوى الفردي بالحفاظ على الهوية والبيانات المهمة من السرقة أو الفقدان أو على مستوى المجتمع بتأمين حماية البنية التحتية الحيوية كمحطات الطاقة والمستشفيات وشركات الخدمات المالية وغيرها من التهديدات السيبرانية وضمان عملها بطريقة آمنة وطبيعية.
4. إن التدقيق الداخلي قد ازدادت أهميته في الوقت الحاضر وأصبح نشاطاً تقويمياً واستشارياً لكافة الأنشطة والعمليات في المنشأة، وتعود أهمية هذه الوظيفة للخدمات التي تقدمها للإدارة في مختلف مجالات المخاطر الناشئة بما فيها المخاطر السيبرانية ادراكاً لحاجة الكثير من الوحدات الاقتصادية إلى خط ثالث للدفاع السيبراني المتمثل بوظيفة التدقيق الداخلي بتقديم مراجعة مستقلة للتدابير الأمنية.
5. لكي يتمكن التدقيق الداخلي من أداء مهامه ومسؤولياته المتعلقة بالأمن السيبراني في الوحدات الاقتصادية التي يعمل بها فأن هناك مجموعة من المتطلبات التي أشارت إليها إرشادات معهد المدققين الداخليين وهي ضرورة امتلاكه لمعرفة متطورة بتقنية المعلومات ومخاطرها وأن يتلقى المدققون الداخليون الدعم الكافي من مجلس الإدارة وتحديث منهج التدقيق الداخلي بالشكل الذي يتلاءم مع بيئة العمل السيبراني وضرورة بناء علاقات قوية مع وظائف IT , CS.

ثانياً. المقترحات:

1. إيلاء موضوع الأمن السيبراني اهتمام أكثر كون المخاطر التي يمكن أن تتعرض لها البنية التحتية الرقمية مخاطر لها تأثير كبير على عمل الأفراد والوحدات الاقتصادية.
2. ادراج الأمن السيبراني ضمن استراتيجية ادارة المخاطر للمؤسسة واعتماد ضوابط وعمليات واضحة وقوية مبنية على اساسيات هامة للأمن السيبراني على مستوى الوحدة الاقتصادية ككل.
3. توعية كافة العاملين في الوحدات الاقتصادية بأهمية الأمن السيبراني وتدريبهم على متطلبات تحقيقه.
4. تفعيل دور التدقيق الداخلي في تعزيز أمن الوحدات الاقتصادية السيبراني وتوفير كافة المتطلبات التي يحتاجها المدقق الداخلي بهذا الصدد من أهمها إقامة دورات تدريبية تعرف المدقق بأطر ومعايير السلامة السيبرانية وأهم المخاطر السيبرانية ومنحه الصلاحيات اللازمة لتدقيق الأمن السيبراني.
5. تشجيع الدراسات في هذا الاتجاه بسبب زيادة الحاجة إلى التدقيق الداخلي من أجل تقليل ومنع المخاطر السيبرانية.

6. توجيه اهتمام المنظمات المهنية الدولية إلى تكييف معايير التدقيق الداخلي بالشكل الذي ينسجم مع الدور الذي يتبناه المدقق الداخلي في تعزيز أمن الوحدات الاقتصادية السيبراني.

المصادر

اولاً. المصادر العربية:

1. أسعد طارش عبد الرضا، علي إبراهيم مشجل المعموري، 2020، الامن السيبراني ودوره في انتشار ظاهرة الارهاب في العراق بعد العام 2003، مجلة دراسات دولية، 80.
2. الهيئة السعودية للأمن السيبراني، 2018، الضوابط الاساسية للأمن السيبراني.
3. الموسوعة السياسية، 2019 على الموقع https://political-encyclopedia.org/dictionary/
4. تقرير الاتحاد الدولي للاتصالات،2011 (اتجاهات الإصلاح في الاتصالات للعام 2010-2011)
5. حنين جميل أبو حسين، 2021، الإطار القانوني لخدمات الامن السيبراني، رسالة ماجستير غير منشورة، جامعة الشــرق الأوسط.
6. ساعد بوقــرص، (2022)، الأمن السيبراني: مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات خاصة. مجلة أبحاث الحماية الاجتماعية، 3(1).
7. فارس محمد العمارات، إبراهيم الحمامضة، 2022، الأمن السيبراني (المفهوم وتحديات العصر)، الطبعة الاولى، دار الخليج للنشر والتوزيع، الاردن.
8. فاطمة يوسف المنتشري، رندة الحريري (2020)، درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات، المجلة العربية للتربية النوعية 4(14).
9. مني عبدالله السمحان، 2020، متطلبات تحقيق الامن السيبراني لأنظمة المعلومات الادارية في جامعة الملك سعود، جامعة الملك سعود، المملكة العربية السعودية.
10. ناظم حسن رشيد،2022، الامن السيبراني منظور التدقيق الداخلي، الطبعة الاولى، دار ابن الاثير للطباعة والنشر في جامعة الموصل، العراق.

ثانياً. المصادر الأجنبية:

1. American Institute of Certified Public Accountants (AICPA), (2017), Security and Privacy.
2. Arishee, J., (2019), Information Security in the Arab World: Risks and Challenges. The International Journal of Informatics, Media and Communication Technology, 1(1).
3. Couto, J. C. P., (2018), Auditoria de Cibersegurança-Um Caso de Estudo Doctoral dissertation, Instituto Politecnico do Porto Portugal.
4. Deloitte, (2017), Cybersecurity and the Role of Internal Audit: An Urgent Call to Action, Deloitte.
5. Goutam, R. K., (2015), Importance of cyber security, International Journal of Computer Applications, 111(7).
6. Islam, S., Farah, N., and Stafford, T., (2018), Factors Associated with Security /Cybersecurity Audit by Internal Audit Function: An International Study. Managerial Auditing Journal, 33 (4)
7. International Professional Practices Framework IPPF, 2017, Available at: www.na.theiia.org .

8. Institute of Internal Auditors, (2020a), Cybersecurity Risk Assessment - The Three Lines Model
9. Institute of Internal Auditors (2020b), The International Professional.Practice Framework (IPPF), "Developing A Risk–Based Internal Audet Plan," IIA,
10. Institute of Internal Auditors, (2020c), The International Professional Practice Framework (IPPF), "IT Essentials for Internal Auditors,"IIA, june, available at:
11. http://www.theiia.org/standards . guidance/recommended-guidance/pages.
12. Institute of Internal Auditors IIA, (2022a): Providing senior management, boards of directors, and audit committees Issue 110 with concise information on governance-related topics.
13. Institute of Internal Auditors IIA, (2022b): Critical Partners — Internal Audit and the CISO.
14. Institute of Internal Auditors IIA, (2022C) Auditing cyber lncident Response and Recovery.
15. Information Systems Audit and Control Association ISACA (2016) , Cybersecurity Fundamentals Glossary.
16. International Professional Practices Framework IPPF, (2017), Available at: www.na.theiia.org.
17. Jamison,J., Morris,L.,& Wilkinson, C. (2018). The future of cyber security in internal audit. Disponibil online la www.crowe.com/-/media/Crowe/LLP/foliopdf/The-Future-of-Cybersecurity-in-IA-Risk-18000-k002A-update.
18. Kahyaoglu, S. B., & Caliyurt, K. (2018) Cyber security assurance process from the internal audit perspective, Managerial Auditing Journal.
19. Lois, P., Drogalas, G., Karagiorgos, A., & Tsikalakis, K., (2020), Internal audits in the digital era: opportunities risks and challenges. EuroMed Journal of Business .
20. Selimoglu, S., Altunel, M., 2019, Internal audit as abridge and catalyst in the protection of cybersecurity risks, denetisim,9,19.
21. Simić, N., (2022), The Internal Auditor's Role in Cybersecurity Governance: A qualitative study about the internal auditor's influence on the people factor of cybersecurity.
22. Shamsuddin, A., Adam, M. A., Adnan, S. A., & Yasin, Y. M.2018, the effectiveness of internal audit functions in managing cyber security in Malaysia's banking in stitutions.
23. Slapničar S., T. Vuko, M. Čular, M. Drašček,2022, Effectiveness of Cybersecurity Audit, International Journal of Accounting Information Systems.
24. Schatz, D., Bashroush, R., & Wall, J., (2017), Towards a more representative definition of cyber security. Journal of Digital Forensics, Security and Law, 12(2).