جامعة غرداية
كلية الاقتصاد
الملتقى الوطني حضوري وعن بعد:
عنوان الورقة البحثية:

فعالية التدقيق الداخلي في تعزيز ودمج برامج الامن السيبيراني في المؤسسات –دراسة تحليلية-

The effectiveness of internal auditing in enhancing and integrating cybersecurity programs in organizations—an analytical study.

الدكتورة : خيرة رقيب، جامعة غرداية، (الجزائر)، الايميل: eguieb.kheira@univ-ghardaia.edu.dz

الدكتور: شاوش حجة الله، جامعة غرداية، (الجزائر)، الايميل: chaouche.hodja@gmail.com

الملخص:
تهدف الدراسة إلى إبراز الدور الاستراتيجي الذي يمكن أن يلعبه التدقيق الداخلي في حماية الأصول المعلوماتية، وتحقيق التكامل بين الأمن السيبراني والتدقيق الداخلي والتركيز على التحديات التي تعيق فعالية هذا الأخير مثل نقص الكفاءات الفنية، وضعف التنسيق بين الجهات المعنية والتغيير المستمر في طبيعة التهديدات السيبرانية.
وقد توصلت الدراسة إلى ان تفعيل دور التدقيق الداخلي في المجال السيبراني يتطلب تطوير مهارات المدققين وتعزيز التعاون بين الإدارات وتبني اطر عمل مرجعية ؛
كما اقترحت الدراسة انشاء وحدات تدقيق سيبراني متخصصة والاستفادة من التقنيات الحديثة كتحليلات البيانات والذكاء الاصطناعي، مما يساهم هذا التكامل بين التدقيق الداخلي والامن السيبراني في بناء بيئة رقمية أكثر امانا، ويدعكم المؤسسات في مواجهة التحديات التقنية المتزايدة بكفاءة ومرونة.
الكلمات المفتاحية: تدقيق داخلي، امن سيبراني، تدقيق سيبراني، برامج امن سيبراني، مخاطر سيبرانية

Abstract:
The study aims to highlight the strategic role that internal audit can play in protecting information assets, achieving integration between cybersecurity and internal audit, and focusing on the challenges that hinder the latter's effectiveness, such as a lack of technical competencies, weak coordination between relevant entities, and the ever-changing nature of cyber threats.
The study concluded that enhancing the role of internal audit in the cyberspace requires developing auditors' skills, enhancing interdepartmental cooperation, and adopting reference frameworks.
The study also proposed establishing specialized cyber audit units and leveraging modern technologies such as data analytics and artificial intelligence. This integration between internal audit and cybersecurity contributes to building a more secure digital environment and supports organizations in facing increasing technical challenges with efficiency and flexibility.
Keywords: Internal Audit, Cybersecurity, Cyber Audit, Cybersecurity Programs, Cyber Risks

مقدمة:

في ظل التحول الرقمي المتسارع واعتماد المؤسسات بشكل متزايد على التكنولوجيا، اصبحت التهديدات السيبرانية تمثل أحد أبرز المخاطر التشغيلية التي تواجه الكيانات العامة والخاصة على حد سواء، ومع تزايد حدة الهجمات الالكترونية وتعقيد اساليبها، برزت الحاجة إلى وجود آليات رقابية فعالة تسهم غي حماية أصول المعلومات وضمان استمرارية الأعمال.

ويعتبر التدقيق الداخلي من أهم الأنشطة الداخلية التي ترتكز عليها المؤسسات، لما لها من أثر بالغ في ضبط نظام الرقابة الداخلية ومراجعة مختلف الأنشطة والعمليات المالية المتعلقة بمختلف المعاملات التي تتعرض لها، والتحقق من سلامة السجلات والبيانات، والمحافظة على أصول الشركة، وكذلك المساهمة في تفعيل دوره الأساسي في التقييم وذلك استنادا إلى معايير التدقيق الداخلي المتعارف عليها، وهو أحد الأدوات الرقابية التي تساهم في تعزيز الأمن السيبراني داخل المؤسسات، حيث يلعب دورا محوريا في تقييم كفاءة الضوابط الأمنية، وقياس مدى التزام المؤسسة بالسياسات والإجراءات، بالإضافة إلى الكسف عن الثغرات ونقاط الضعف التي قد تستغل من قبل المهاجمين، ولا يقتصر دور التدقيق الداخلي على اكتشاف المخاطر، بل يمتد ايضا إلى تقديم التوصيات الاستراتيجية لتحسين البنية التحتية الامنية وتعزيز ثقافة الوعي الامني لدى الموظفين.

وفي هذا السياق تتناول الدراسة التدقيق الداخلي كأداة فعالة في تعزيز ودمج برامج الأمن السيبراني ضمن منظومة الحوكمة الشاملة للمؤسسة، بما يحقق حماية مستدامة للمعلومات والأنظمة الرقمية.

إشكالية الدراسة:

رغم التطور الكبير في أدوات وتقنيات الأن السيبراني، إلا أن العديد من المؤسسات لا تزال تواجه تحديات كبيرة في حماية أصولها الرقمية من الهجمات والاختراقات المتزايدة تعقيدا، وهذا نتيجة ضعف التكامل بين وظائف الامن السيبراني والتدقيق الداخلي أو قصور في تقييم ومتابعة فعالية الضوابط الأمنية وتحديد السيبرانية في الوقت المناسب.

ومن هذا المنطلق تبرز الإشكالية الرئيسية:

إلى أي مدى يسهم التدقيق الداخلي في تعزيز ودمج برامج الأمن السيبراني؟

أهمية واهداف الدراسة:

تكمن أهمية هذه الدراسة في تسليط الضوء على العلاقة التكاملية بين التدقيق الداخلي والأمن السيبراني، وبيان كيف يمكن تعزيز هذا الدور لضمان بيئة رقمية آمنة ومستقرة، كما تهدف الدراسة إلى إبراز التحديات التي قد تعيق فعالية التدقيق الداخلي في هذا المجال، وتقديم توصيات عملية تسهم في تطوير قدراته ورفه كفاءته في التعامل مع المخاطر السيبرانية.

إن فهم هذا الدور وتفعيله بشكل منهجي يعد خطوة جوهرية نحو تحقيق حوكمة فعالة للمخاطر، وبناء ثقافة مؤسسية واعية بالأمن السيبراني، خاصة في ظل التوجه المتزايد نحو الرقمنة والتحول الرقمي.

- **المحور الأول :التدقيق الداخلي –رؤيا شاملة:-**

إن الزيادة في حالات الفشل وإفلاس المؤسسات في الولايات المتحدة في الأربعينيات من القرن السابق[1]، أدى إلى بدأ الاتجاه نحو ضرورة الاعتراف بالتدقيق الداخلي كمهنة تكون لها مقوماتها التي تمكنها من تحقيق الغرض منها، حيث تم إنشاء معهد المدققين الداخليين في الولايات المتحدة في عام 1941[2].

وذلك بغرض تطوير التدقيق الداخلي كمهنة يعترف بها، و أدى إنشاء فروع عديدة لهذا المعهد في عدد كبير من الدول، إلى انتشار فكرة "المهنية "للتدقيق الداخلي وضرورة تطويرها كمهنة تتوافر لها مقوماتها من وجود معايير مهنية لممارستها، و الترخيص بمزاولتها، و قواعد السلوك المهني يجب الالتزام بها، مع ضرورة التعليم والتطوير المستمر لممارسي المهنة، حيث جاء في أول تعريف سنة "1994 IIAللتدقيق الداخلي والصادر عن معهد المدققين الداخليين الأمريكي "

-1تعريف التدقيق الداخلي:

ينص أول تعريف للتدقيق الداخلي الصادر سنة 1941عن المعهد المدققين الداخليين الأمريكي على أن "التدقيق الداخلي هو نشاط تقييمي مستقل يوجد في منظمة الأعمال لمراقبة العمليات المحاسبية والمالية، والعمليات الأخرى، من أجل تقديم خدمات وقائية وعلاجية للإدارة، داخل التنظيم للقيام بالمسئوليات المنوطة بها بدرجة عالية من الكفاءة وذلك عن طريق توفير التحليل والتقييم والتوصيات والمشورة والمعلومات التي تتعلق بالأنشطة التي تتم مراجعتها.[3]"

ولقد وضعت لجنة العمل التابعة لمعهد المدققين الداخليين سنة 2003أن التدقيق الداخلي على أنه "نشاط مستقل، تأكيد موضوعي واستشاري مصمم لزيادة قيمة المنظمة وتحسين عملياتها، ومساعدتها على إنجاز أهدافها بواسطة تكوين مدخل منظم ومنضبط لتقييم وتحسين فعالية إدارة المخاطر والرقابة وعمليات التحكم[4]" نلاحظ أن هنا تطور في مفهوم التدقيق الداخلي على نفس المعهد حيث اشتمل المفهوم الجديد على نوعين من الخدمات التي تقدمها –بالإضافة إلى المفهوم التقليدي –وظيفة التدقيق الداخلي وهما تقييم المخاطر وتقديم الخدمات الاستشارية على غرار التعريف القديم الذي ركز على المفهوم الرقابة الداخلية من خلال الفحص والتقييم .وبالتالي يوجد تطور في أهداف التدقيق الداخلي.

1-1مجالات التدقيق الداخلي :إن المتأمل في المداخل التي على المدقق الداخلي الوقوف عندها، والتي تكون مادة عمله، يجد أن هناك نوعين من المداخل لموضوع مادة هذه الوظيفة وهما:

<u>المدخل الأول</u> :تدقيق مدى الالتزام يهدف)المدقق (عملية التدقيق من هذا المدخل إلى التحقق إذا كان العاملون في المستويات الإدارية المختلفة، قد التزموا بنص الأوامر والتعليمات الصادرة عن الإدارة العليا واتبعوا الإجراءات المناسبة في تنفيذ واجباتهم، وتتم هذه التدقيق من خلال ثلاث مستويات هي:

-مستوى التحقق: بموجب هذا المستوى يبحث المدقق عن أدلة وبراهين تثبت صحة أية عملية يدققها، و يحرص المدقق هنا على جمع معلومات من أعمال المؤسسة من جهة خارجية محايدة مثل :شهادة الرصيد الصادرة عن البنوك -رسائل وأجوبة المدينين والدائنين -إعادة تقييم الممتلكات من قبل متخصصين.

-مستوى التدقيق المستندي: يعتمد المدقق في هذا المستوى على المستندات التي تثبت صحة القيود والمطابقة القانونية للشروط والواجبات الإتباع في المعاملات والعمليات، وبموجب هذا المستوى لا يفحص المراجع أكثر من السجلات والدفاتر والوثائق.

-مستوى تدقيق النظم: يركز المدقق وفقا لهذا المستوى على النظام نفسه، فيأخذ كل نظام على حدى، ويفحصه ويقيمه ويحاول ربطه مع النظم الأخرى، وذلك للتحقق من أن النظم الموضوعة تعمل بشكل صحيح، وأنها تحقق الغرض الذي وضعت من أجله وأنها لا تتعارض في الأهداف.

<u>المدخل الثاني</u> :مراجعة العمليات "يسعى المدقق في تدقيق للعمليات إلى الحصول على أدلة وقناعات تثبت ارتفاع كفاية العمليات، وفعالية السياسات والإجراءات ووسائل الرقابة المتبعة لتدعيم كفاءة تلك العمليات.

وبشكل أساسي فإن هذه المراجعة تشتمل على فحص وتقييم الاستخدام الأمثل للموارد المتاحة.

يتبع المدقق الداخلي في تدقيق العمليات مستويين لتحقيق غايات التدقيق وهما:

-المستوى التنظيمي: يركز المدقق الداخلي في هذا المستوى اهتماماته على الوحدة التنظيمية، حيث يخضع جميع عملياتها وأنشطتها لتدقيق وتحليل وتقييم، ويشمل فحصه تدقيق أهداف وخطط وأساليب وإجراءات هذه الوحدة، ولكنه لا يخرج بفحصه عن الحدود التنظيمية لهذه الوحدة.

-المستوى الوظيفي :يتبع المدقق الداخلي في هذا المستوى العملية أو النشاط محل التدقيق من بداية العملية أو النشاط إلى نهايته، وحتى وإن اخترقت إجراءات هذه العملية الحدود التنظيمية للوحدات المختلفة، فالعمليات كثيرا ما تشترك في إنجازها أكثر من وحدة تنظيمية، وعلى المدقق أن يقوم بفحص جميع الإجراءات التي تمت في المراحل التي قطعتها في مختلف الوحدات التنظيمية، ومن أمثلة العمليات التي تدقق عمليات الشراء، البيع وإصدار الأوراق المالية.

2-1معايير التدقيق الداخلي :لقد أصدرت معايير للتدقيق الداخلي سنة 1978من قبل معهد المدققين الداخليين بالولايات المتحدة الأمريكية، والتي عدلت سنة 1993حيث تم تقسيم معايير التدقيق الداخلي إلى خمسة أقسام تم تبويبها في مجموعات وتتضمن 25معيار فرعيا تغطي الجوانب المختلفة للتدقيق الداخلي

في أي تنظيم و تتمثل تلك الأقسام في :[5]الاستقلالية -العناية المهنية -نطاق العمل -أداء أعمال التدقيق - إدارة قسم التدقيق الداخلي.

- كما أصدر معهد المدققين الداخليين في الولايات المتحدة الأمريكية تعديلا في شكل هذه المعايير سنة 2001وسنة 2004حيث قسم معايير التدقيق إلى مجموعتين رئيسيتين :[6]

معايير السمات أو الخصائص أو الصفات) :Attribute standardsسلسلة الألف (وهي التي تتناول معايير السمات وخصائص المنظمات والأفراد الذين يؤدون أنشطة التدقيق الداخلي -معايير الأداء) :Performanceسلسلة الالفين (وهي التي تصف طبيعة أنشطة التدقيق الداخلي، والمعايير التي من خلالها يتم قياس أداء تلك الأنشطة.

ولقد كان آخر تعديل قام به معهد المدققين الداخليين لهذه المعايير في 26أكتوبر 2010أين تكلم على معايير التنفيذ التي تتولى تطبيق معايير السمات والأداء على أنواع محددة من الأنشطة، حيث أنه قد توجد فئة واحدة من معايير السمات ومن معايير الأداء، لكنه يوجد لها فئات متعددة من معايير التنفيذ، فميز بين نوعين من الأنشطة، الأنشطة الاستشارية والتي يشار إليها بحرف **C** بعد رقم المعيار مثل **-c11130 (c1)**، أنشطة التأكيد والتي يشار إليها بحرف A بعد رقم المعيار مثل [7]**.A11130- (A2)**

المحور الثاني: الأمن السيبراني

أصبحت تكنولوجيا المعلومات جزءًا أساسيًا من مختلف جوانب الحياة، حيث تسهم في تحسين العمليات التشغيلية، وتعزيز التواصل، وتوفير حلول رقمية مبتكرة. ومع هذا التوسع الرقمي، برزت تحديات جديدة تتعلق بحماية البيانات والأنظمة من التهديدات المتزايدة، مثل الاختراقات والهجمات الإلكترونية. لذا، أصبح الأمن السيبراني ضرورة ملحّة لضمان سلامة المعلومات، والحفاظ على سرية البيانات، وحماية البنية التحتية الرقمية من المخاطر المحتملة.

1. ماهية الأمن السيبراني

حسب المعهد الوطني للمعايير والتكنولوجيا:(NIST): عرفه بأنه: "مجموعة من التقنيات والعمليات والممارسات المصممة لحماية الشبكات والأجهزة والبرامج والبيانات من الهجمات أو التلف أو الوصول غير المصرح به ".[1]

حسب الاتحاد الدولي للاتصالات: (ITU): "مجموعة من الأدوات و السياسات و مفاهيم الأمن و تحفظات الأمن و المبادئ التوجيهية و نهج إدارة المخاطر و الإجراءات و التدريب و أفضل الممارسات و آليات الضمان و التكنولوجيات التي يمكن استخدامها في حماية البيئة السيبرانية وأصول المؤسسات و المستعملين".[2]

2. مجالات الأمن السيبراني:

شمل الأمن السيبراني مجموعة واسعة من المجالات[3].

- **أمن الشبكات:**(Network Security) : وفيه تتم حماية أجهزة الحاسوب من الهجمات التي قد يتعرض لها داخل الشبكة وخارجها، ومن أبرز التقنيات المستخدمة لتطبيق أمن الشبكات جدار الحماية الذي يعمل بين الجهاز الشخصي والأجهزة الأخرى في الشبكة، بالإضافة إلى أمن البريد الإلكتروني.

---

[1] **National Institue of Standards and Technology (NIST)** , NIST special publication 800-53 version 5 , security and privacy controls for information systems and organizations , u.s , department of commerce ,p 5, 2020, retrieved from : https://cscr.nist.gov/publications/detail/sp/800-53/rev-5/final.

[2] **الاتحاد الدولي للاتصالات** ، شبكات البيانات و الاتصالات بين الأنظمة المفتوحة وسائل الأمن لمحة عامة عن الأمن السيبراني، ص8، 2008، https://www.itu.int/rec/T-REC-X.1205-200804-I

[3] بريج سلمى، بودبوزة وهيبة، تأثير التدقيق الداخلي على الأمن السيبراني،مذكرة ماستر،تخصص محاسبة و تدقيق،جامعة العربي بن مهيدي ام البواقي،الجزائر، 2024، ص22-23.

- **أمن التطبيقات**:(Application Security): وفيه تتم حماية المعلومات المتعلقة بتطبيق على جهاز الحاسوب كإجراءات وضع كلمات المرور، وعمليات المصادقة، وأسئلة الأمن التي تضمن هوية مستخدم التطبيق
- **الأمن السحابي**:(Cloud Security): تشير البرامج السحابية إلى أنظمة تخزين البيانات وإدارتها عبر الإنترنت، حيث يفضل العديد من المستخدمين حفظ بياناتهم على المنصات السحابية بدلاً من التخزين المحلي. وقد أدى ذلك إلى الحاجة المتزايدة لحماية هذه البيانات، لذا توفر البرامج السحابية إجراءات أمان متقدمة لضمان حماية المعلومات وخصوصية المستخدمين.
- **الأمن التشغيلي(Operational Security):** [4] يشمل العمليات والقرارات التي تتعامل مع أصول البيانات وتكفل حمايتها من خلال مراقبة وإدارة الوصول إلى البيانات والتأكد من تطبيق السياسات الأمنية بفعالية. ويشمل ذلك التحكم في الأذونات، وإجراءات المصادقة، ومراقبة الأنشطة المشبوهة لضمان استمرارية الأعمال وحماية الأصول الرقمية من المخاطر السيبرانية.

3.أهداف الأمن السيبراني:

إن هدف الأمن السيبراني هو القدرة على مقاومة التهديدات المتعمدة وغير المتعمدة والاستجابة والتعافي، وبالتالي التحرر من الخطر أو الأضرار الناجمة عن تعطيل آو إتلاف وهذا تكنولوجيا المعلومات والاتصالات أو بسبب إساءة استخدام تكنولوجيا المعلومات والاتصالات ويهدف الى[5]

الشكل رقم (1) يوضح: اهداف الامن السيبيراني

المصدر: من اعداد الباحثين بناء على المرجع المدكور في التهميش.

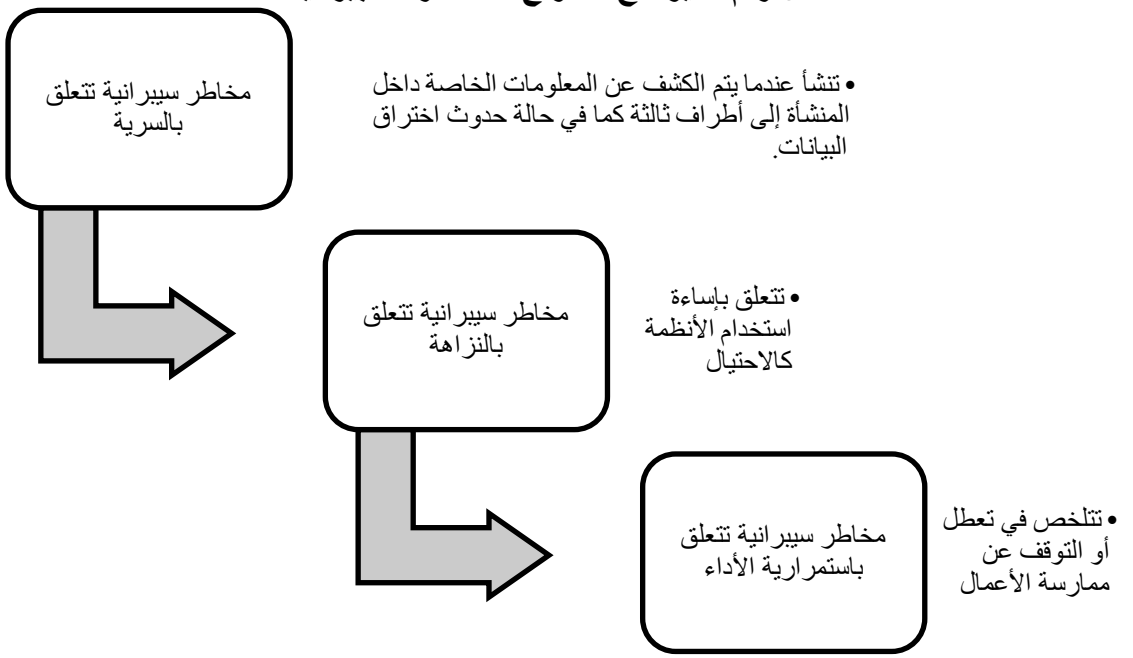
---

[4] - فايزة احمد الحسيني مجاهد، **الوعي بالأمن السيبراني ضرورة في عصر المعلوماتية**، مجلة بحث و تربية المعهد الوطني للبحث في التربية،المجلد:13،العدد02،ديسمبر2023،ص60.

[5] - حميدي حياة، طايلب نسيمة، **مدخل مفاهيمي حول الامن السيبراني**، مجلة مدار للدراسات الاتصالية الرقمية، مجلد02، العدد02،نوفمبر2022، ص9.

4. أنواع المخاطر السيبرانية:[6]

الشكل رقم 2 يوضح : أنواع المخاطر السبيرانية



المصدر: من اعداد الباحثين بناء على المرجع المذكور في التهميش

المحور الثالث : متطلبات التدقيق الداخلي لتعزيز الأمن السيبراني

يُعد التدقيق الداخلي جزءًا أساسيًا من منظومة الأمن السيبراني في أي مؤسسة، حيث يساهم في تقييم مدى فعالية الضوابط الأمنية، والكشف عن الثغرات والمخاطر وضمان الامتثال للمعايير والسياسات الأمنية، فالتدقيق الداخلي لا يقتصر فقط على الفحص المالي والإداري، بل يمتد ليشمل أنظمة تكنولوجيا المعلومات والامن السيبراني لضمان حماية الاصول الرقمية من التهديدات الالكترونية.

1-تقييم المخاطر: يتضمن تقييم المخاطر في مجال الأمن السيبراني الخطوات التالية[7]:

- الكشف عن نقاط الضعف في الأنظمة والشبكات والتطبيقات التي قد يستغلها المهاجمون، حيث يتم فحص الأنظمة من طرف فريق تقييم المخاطر لتحديد الثغرات الأمنية التي تعرض الأنظمة للخطر.
- تحليل التهديدات الداخلية والخارجية التي قد تواجهها المؤسسة، حيث يتم تقييم التهديدات الحالية والمحتملة من داخل المؤسسة وخارجها، مما يساعد على تحديد المصادر المحتملة للهجمات والانتهاكات.
- تقييم احتمالية حدوث المخاطر وشدتها، حيث يتم تحليل الثغرات المكتشفة وتحديد احتمالية استغلالها من قبل المهاجمين والتأثير المحتمل لهذه الاستغلالات على عمليات المؤسسة.

2-ضمان الامتثال للمعايير والقوانين:

---

[6] - جيهان عادل أميرهم، **اثر جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني وانعكاساته على ترشيد قرارات المستثمرين(دراسة ميدانية)**، مجلة البحوث المالية و التجارية ، المجلد(23)-العدد03، يوليو 2022،ص339.

[7] سهى يونس على البرزنجي، زياد هاشم يحي السقا، **متطلبات التدقيق الداخلي لتعزيز الأمن السيبراني في الوحدات الاقتصادية في ضوء إرشادات معهد المدققين الداخليين**، مجلة تكريت للعلوم الإدارية و الاقتصادية،المجلد:19،العدد:63، 2023،ص103.

عبر رقابة الالتزام يجب على التدقيق الداخلي مراجعة مدى امتثال المؤسسة للسياسات الأمنية الداخلية والمعايير الدولية مثل نظام إدارة أمن المعلومات ISO 27001 والقانون العام لحماية البيانات في الاتحاد الأوروبي GDPR و NIST Cybersecurity Framework (إطار الأمن السيبراني للمعهد الوطني للمعايير والتكنولوجيا). وتساهم هذه المراجعة المستمرة لضمان التزام المؤسسة بهذه المعايير مما يعزز الامان السيبراني وتحديد المجالات التي قد تفتقر الى الحماية المناسبة.

3-حماية الأصول الرقمية والمعلومات الحساسة:

-يساعد التدقيق الداخلي في ضمان سلامة وسرية وتوفر البيانات الرقمية، والمعروفة بمبدأ CIA Triad.

- يحمي الأصول الرقمية مثل قواعد البيانات، أنظمة البريد الإلكتروني، المعلومات المالية، وسجلات العملاء من السرقة أو التلف ويساهم في الحد من الهجمات التي تستهدف سرقة الهوية، التجسس الإلكتروني، وتسريب البيانات.

4-تحسين كفاءة الضوابط الأمنية:

- يعمل التدقيق الداخلي على تقييم فعالية الإجراءات الأمنية الحالية، مثل جدران الحماية، أنظمة كشف التسلل، وأدوات التشفير و يساعد على تحسين عمليات إدارة الهوية والوصول(IAM) ، والتأكد من أن الموظفين لديهم فقط الصلاحيات اللازمة لأداء مهامهم.

- يوصي بتحديث السياسات الأمنية وتطوير ضوابط أفضل لحماية البيانات الحساسة.

5-**تحسين استجابة المؤسسة للهجمات السيبرانية:**

- يختبر التدقيق الداخلي مدى استعداد المؤسسة للاستجابة للحوادث الأمنية.

- يقوم بمراجعة خطة الاستجابة للحوادث الأمنية، ويتأكد من أن الفرق المسؤولة لديها الأدوات والمعرفة اللازمة للتعامل مع التهديدات بفعالية و يقلل من تأثير الهجمات من خلال تطوير خطط استجابة سريعة وفعالة للتعامل مع الاختراقات الإلكترونية.

6- **تحسين وضعية الأمن السيبراني**: إن تحسين الأمن السيبراني يجب أن يحدث في أسرع وقت للبقاء على قيد الحياة و مواكبة التطور في التهديدات الالكترونية باعتماد سياسات أمنية واسعة النطاق و متطورة يتم إتباعها من قبل كل موظف لتحسين إجراءات امن المعلومات في الوحدة الاقتصادية و التي يجب أن تخضع باستمرار للتقييم المستمر لمدى فعالية تنفيذها و مدى تماشيها مع أهداف العمل.

7-إدارة مخاطر الأمن السيبراني يمكن أن تدار من خلال ثلاث خطوط دفاعية، حيث يتمثل **الخط الدفاعي الأول** في مديرو وحدات الأعمال جنبا إلى جنب مع وظيفة تكنولوجيا المعلومات ، كما يتمثل **الخط الدفاعي الثاني** في إدارة مخاطر امن المعلومات حيث توفر الخبرة لتنفيذ و متابعة فعالية الضوابط الأمن السيبراني، و يتمثل **الخط الدفاعي الثالث** في وظيفة المراجعة الداخلية حيث تزود مجلس الإدارة و لجنة المراجعة التابعة لها بتوكيد مستقل عن فعالية إستراتيجية و سياسات إجراءات و ضوابط إدارة مخاطر الأمن السيبراني.[8]

الجدول رقم 1: الخطوط الدفاعية الثلاثة لإدارة مخاطر الأمن السيبراني.

مجلس الإدارة أدوار مجلس الإدارة (النزاهة و القيادة و الشفافية)		
الخط الأول: مديرو وحدات الأعمال ووظائف تقنية المعلومات	**الخط الثاني:** وظائف إدارة مخاطر تقنيات المعلومات (وظيفة الأمن السيبراني ووظيفة InfoSec)	**الخط الثالث:** وظيفة التدقيق الداخلي

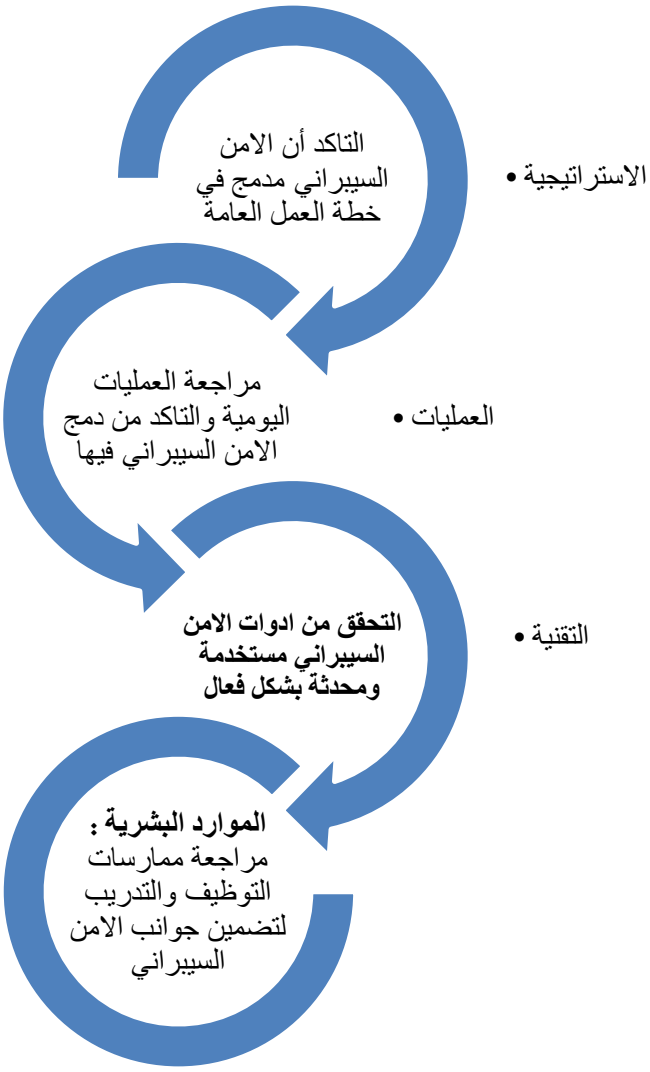
[8] محمد حارس محمد طه ابو الخير،اثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الاستقرار المالي في البنوك الالكترونية،المجلة العلمية للدراسات و البحوث المالية و الادارية،المجلد:15،العدد:2023،01،ص13.

إنشاء الهياكل والضوابط المناسبة لإدارة العمليات والمخاطر وتامين التقنيات و البيانات	توفر الخبرة لتنفيذ و متابعة فعالية ضوابط الأمن السيبراني و ضمان وجود عمليات و ضوابط الخط	التوكيد المستقل والموضوعي بمدى فاعلية و كفاءة عمليات الخطين الأول و الثاني و المشورة بشان تعزيز الأمن السيبراني

المصدر: من اعداد الباحثين .

يكمن دور التدقيق الداخلي في دمج برامج الأمن السيبراني في النقاط التالية ملخصة كالاتي :

الشكل رقم (3) يوضح: **دور التدقيق الداخلي في دمج برامج الأمن السيبراني**



المصدر: من اعداد الباحثين بناء على معلومات سابقة.

خاتمة:

يعد التدقيق الداخلي محور أساسي في تعزيز ودعم برامج الأمن السيبراني داخل المؤسسات، ليس فقط من خلال فحص الضوابط والإجراءات الأمنية، بل أيضا عبر تقديم توصيات استراتيجية تسهم في الوقاية من التهديدات المستقبلية وتعزيز برامج الأمن السيبراني، وابرزت الدراسة أهمية التكامل بين وظيفة التدقيق الداخلي ووحدات الأمن السيبراني كجزء من منظومة الحوكمة وإدارة المخاطر.

كما تبين أن فعالية هذا الدور تكمن في مجموعة من النقاط الاساسية ألا وهي توفر الكفاءات المتخصصة في التدقيق السيبراني واعتماد منهجيات مرجعية واضحة، اضافة إلى دعم الإدارة العليا ووعي الموظفين بأهمية الأمن السيبراني، لذلك فإن تطوير قدرات المدققيين الداخليين في هذا المجال وتحديث ادوات واساليب التدقيق بشكل مستمر، أصبح ضرورة ملحة لمواجهة التحديات المعاصرة في بيئة رقمية دائمة التغير،

التوصيات:

- تطوير مهارات المدققين الداخليين في مجال الأمن السيبراني؛
- يجب توفير برامج تدريبية وتكوينية لرفع كفاءة المدققين الداخليين ومساعديهم في كيفية التعامل مع التهديدات الرقمية وتقييم الضوابط الفنية؛
- تعزيز التعاون بين وحدات التدقيق الداخلي ووحدات الأمن السيبراني؛
- تحديث منهجيات التدقيق لتشمل المخاطر السيبرانية من خلال تعديل خطط ومجالات التدقيق لتواكب المتغيرات التقنية وضمان تضمين تقييم شامل لأنظمة الأمن السيبراني ضمن جدول الاعمال الرقابية؛
- تبني اطار عمل موحد لإدارة الامن السيبراني مما يسهل على المدققين تقييم مدى الامتثال واكتشاف الانحرافات عن المعايير العالمية.
- زيادة وعي الإدارة العليا بأهمية التدقيق الداخلي في حماية الاصول الرقمية وذلك عبر تقارير دورية وتوصيات استراتيجية تربط الامن السيبراني بحوكمة المؤسسة وأدائها العام.

المراجع المعتمدة:

1. أحمد حلمي جمعة، **التدقيق الداخلي والحكومي**، دار صفا، ط 1عمان،2011 ، ص. 46
2. بغدود راضية، صبايحي نوال، **دور التدقيق الداخلي في تفعيل إدارة المخاطر المصرفية**، الملتقى الدولي حول : إدارة المخاطر المالية وانعكاساتها على اقتصاديات دول العالم، جامعة آكلي محند أولحاج البويرة، الجزائر، سنة؟، ص ص.15-14
3. يونس عليان الشوبكي، **أهمية التدقيق الداخلي في الشركات الأردنية المساهمة العامة في الحد من مخاطر الأحكام الشخصية لمعدي القوائم المالية) دراسة ميدانية لبعض البنوك التجارية(**، مجلية جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد30 ، العدد الأول، جامعة الشرق الأوسط، عمان، الأردن، 2014ص).192 بتصرف(.
4. الهيئة السعودية للمحاسبين القانونين، مشروع معايير المراجعة الداخلية وقواعد السلوك المهني، مكتبة الملك فهد الوطنية، النشرة الإلكترونية، الرياض، يوليو2004 ، www.socpa.org.sa.26/07/2005,15h:43m
5. عبد الوهاب نصر علي، المراجعة الداخلية وإدارة المخاطر، الدار الجامعية، ط1، الإسكندرية، 2011، ص08
6. **National Institue of Standards and Technology (NIST)** , NIST special publication 800-53 version 5 , security and privacy controls for information systems and organizations , u.s , department of commerce ,p 5, 2020, retrieved from : https://cscr.nist.gov/publications/detail/sp/800-53/rev-5/final.
7. **الاتحاد الدولي للاتصالات** ، شبكات البيانات و الاتصالات بين الأنظمة المفتوحة وسائل الأمن لمحة عامة عن الأمن السيبراني، ص8، 2008، https://www.itu.int/rec/T-REC-X.1205-200804-I
8. بريج سلمى، بودبوزة وهيبة، تأثير التدقيق الداخلي على الأمن السيبراني،مذكرة ماستر،تخصص محاسبة و تدقيق،جامعة العربي بن مهيدي ام البواقي،الجزائر، 2024، ص22-23.

9. فايزة احمد الحسيني مجاهد، **الوعي بالأمن السيبراني ضرورة في عصر المعلوماتية**، مجلة بحث و تربية المعهد الوطني للبحث في التربية،المجلد:13،العدد02،ديسمبر2023،ص60.
10. حميدي حياة، طايلب نسيمة، **مدخل مفاهيمي حول الامن السيبراني**، مجلة مدار للدراسات الاتصالية الرقمية، مجلد02، العدد02،نوفمبر2022، ص9.
11. جيهان عادل أميرهم، **اثر جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني وانعكاساته على ترشيد قرارات المستثمرين(دراسة ميدانية)**، مجلة البحوث المالية و التجارية ، المجلد(23)-العدد03، يوليو 2022،ص339.
12. سهى يونس على البرزنجي، زياد هاشم يحي السقا، **متطلبات التدقيق الداخلي لتعزيز الأمن السيبراني في الوحدات الاقتصادية في ضوء إرشادات معهد المدققين الداخليين**، مجلة تكريت للعلوم الإدارية و الاقتصادية، المجلد:19،العدد:63، 2023،ص103.
13. محمد حارس محمد طه ابو الخير،اثر جودة المراجعة الداخلية في الحد من المخاطر السيبرانية بهدف دعم الاستقرار المالي في البنوك الالكترونية،المجلة العلمية للدراسات و البحوث المالية و الادارية،المجلد:15،العدد:2023،01،ص13.