التدقيق الداخلي كمدخل حديث لإدارة مخاطر الأمن المعلوماتي وفق نموذج خطوط الدفاع الثلاثة

كاست علي - طالب دكتوراه
كلية العلوم الاقتصادية والتجارية وعلوم التسيير
جامعة الجزائر 3

ملخص :

إن تعزيز أمن البيانات والالتزام بالمعايير وأطر العمل اللازمة لتحسين خصوصية البيانات يعتبر من ضمن الأولويات القصوى للمؤسسات. حيث يتزايد حجم ومعدل تواتر حوادث الأمن الحاسوبي تزايدًا حادًا. وعلى المؤسسات أن تتابع باستمرار شتّى التهديدات الحاسوبية لكي تتجنّب الوقوع ضحية للهجمات الحاسوبية الإجرامية.
وفي ظل هذه الظروف، أصبحت عملية إدارة المخاطر المعلوماتية من المواضيع الأكثر أهمية، حيث اتجهت المؤسسات إلى مضاعفة مجهوداتها في سبيل معرفة وتشخيص المخاطر المعلوماتية ومعرفة أسبابها وكيفية معالجتها. في هذا الإطار، أصبح وجود خط دفاع يتمثل في وظيفة التدقيق الداخلي في المؤسسة ضرورة لا غنى عنها، حيث تساهم هذه الوظيفة في دعم إدارة المخاطر المعلوماتية وتقديم الضمان أن هذه المخاطر تدار بطريقة فعالة.

الكلمات المفتاحية: الأمن المعلوماتي، التدقيق الداخلي، مخاطر معلوماتية، إدارة المخاطر، خطوط الدفاع الثلاثة.

Résumé :
Le renforcement de la sécurité des données et le respect des normes et des cadres visant à améliorer la confidentialité des données constituent une priorité absolue pour les entreprises. le volume et la fréquence des incidents de sécurité informatique augmentent fortement, ce qui obligent les institutions à faire face constamment à diverses menaces informatiques afin d'éviter d'être victimes d'attaques de cybercriminalité.
Dans ces circonstances, le management des risques informatiques est devenu l'un des problématiques les plus importantes, car les institutions ont redoublé d'efforts pour identifier et diagnostiquer les risques informatiques, identifier leurs causes et savoir comment y faire face. Dans ce contexte, l'existence d'une ligne de défense dans qui est la fonction d'audit interne au sein de l'institution est une nécessité indispensable, car cette fonction contribue à la au management des risques informatiques et à donner une assurance que ces risques sont gérés avec efficacité.

Mots clés : Cyber sécurité, audit interne, cyber risques, management de risques, trois lignes de défense.

مقدمة

ان التطورات الحديثة في تقنيات المعلومات أحدثت تغييرات مستمرة ومضطردة في كافة الميادين إذ أصبحت عملية انتقال المعلومات عبر الشبكات و الحواسيب إحدى علامات العصر الرقمي المميزة التي لا يمكن الاستغناء عنها، وذلك لميزتها في تسهيل متطلبات الحياة العصرية من خلال تقليل حجم الأعمال وتطوير أساليب إنتاج وتخزين وتوزيع المعلومات، وهذا بدوره أدى إلى تزايد المشاكل والمخاطر المعلوماتية التي تهدد أمن معلومات المؤسسة وتؤثر عليها، مما يستوجب على هذه الأخيرة ضرورة التيقظ لتوفير الأمن اللازم لمعلوماتها خصوصا وأنها تعيش في ظل اقتصاد المعلومات الذي شعاره من يملك المعلومة يملك السيطرة، وهذا ما يدفع المؤسسات إلى إيجاد الطرق المناسبة لإدارة هذه المخاطر المعلوماتية لاسيما وأنها تتميز بصعوبة القياس و بالفجائية. ويعتبر وجود وظيفة التدقيق الداخلي في المنظمة دعما حقيقيا وفعالا لإدارة المخاطر المعلوماتية، حيث تقدم هذه الوظيفة تأكيدا أن هذه المخاطر تدار بالطريقة الجيدة، و من جهة أخرى فإن الاعتماد على وظيفة التدقيق الداخلي في رقابة وادارة المخاطر المعلوماتية يعتبر توجها جديدا حيث توسع نطاق ودور وظيفة التدقيق الداخلي من دورها التقليدي وهو التدقيق المالي والإداري إلى التركيز على إضافة قيمة للمنظمة عن طريق المساهمة في إدارة المخاطر بصفة عامة والمعلوماتية بصفة خاصة.

ولقد جاءت هذه الدراسة لتركز على ضرورة اهتمام المنظمة بموضوع الأمن المعلوماتي والمخاطر المرتبطة به ومدى مساهمة التدقيق الداخلي في الادارة الفعالة لها ضمن نموذج خطوط الدفاع الثلاثة والمتمثلة في الرقابة الداخلية، ادارة المخاطر و التدقيق الداخلي. ومما سبق، تمت صياغة إشكالية هذا البحث كالآتي:

إلى أي مدى يمكن للتدقيق الداخلي أن يساهم في الحد من مخاطر الأمن المعلوماتي في المؤسسات؟

وللإجابة على هذا التساؤل، ارتأينا تقسيم هذه الورقة البحثية إلى أربعة محاور هي:

المحور الأول: ماهية الأمن المعلوماتي والمخاطر المتعلقة به

المحور الثاني: تطور مهنة التدقيق الداخلي في بيئة تكنولوجيا المعلومات

المحور الثالث: دور التدقيق الداخلي في إدارة مخاطر المعلوماتية – نموذج خطوط الدفاع الثلاثة-

المحور الأول: ماهية الأمن المعلوماتي والمخاطر المتعلقة به

لقد ظل مجال أمن المعلومات حتى أواخر السبعينات معروفا باسم أمن الاتصالات والذي حددته توصيات أمن أنظمة المعلومات والاتصالات لوكالة الأمن القومي في الولايات المتحدة الأمريكية بأنه: "المعايير والإجراءات المتخذة لمنع وصول المعلومات لأيدي أشخاص غير مخولين عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات[1]."

[1]- بلجراف سامية، كلاش خلود، الإدارة الإليكترونية وإشكالية الأمن المعلوماتي، مجلة الناقد للدراسات السياسية، العدد 1، جامعة محمد خيضر – بسكرة، اكتوبر 2017، ص272.

أولا - مفهوم الأمن المعلوماتي: ينظر إلى الأمن المعلوماتي من عدة نواحي:

- **الناحية الاكاديمية:** يقصد بالأمن المعلوماتي العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها[1].

- **الناحية التقنية:** يقصد به الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية[2].

- **الناحية القانونية:** يقصد بالأمن المعلوماتي محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات، ومكافحة أنشطة الاعتداء عليها أو إستغلال نظمها في إرتكاب الجريمة وهو لا شك هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظم معالجتها.

وعموما يمكننا تعريف الأمن المعلوماتي بأنه مجموعة من المعايير التي تحول دون وصول المعلومات المخزنة في الشبكات إلى الأشخاص غير المخول لهم الحصول عليها.

ثانيا - مكونات الأمن المعلوماتي: يحدد المتخصصون في أمن المعلومات ثلاث مكونات جوهرية للأمن المعلوماتي عند بناء أي برنامج للأمن المعلوماتي تتمثل فيما يلي[3]:

1- **سرية وخصوصية المعلومات:** حيث يجب اتخاذ التدابير اللازمة لمنع اطلاع غير المصرح لهم على المعلومات الحساسة والسرية والتي يفترض أن تكون محمية.

2- **سلامة المعلومات وتكامل المعالجة:** مما يفرض ضرورة وضع أنظمة حماية كفيلة بحماية المعلومات.

3- **ضمان اتاحة المعلومات و الوصول إليها عند الحاجة إلى ذلك:** حيث أن حرمان من له الحق في الحصول على المعلومة أو جعل عملية الوصول إلى المعلومة صعبا وشاقا يخل بالأمن المعلوماتي خاصة إذا تعرضت للحذف أو شل الأجهزة التي تخزن بها المعلومة.

ثالثا - مخاطر الأمن المعلوماتي: نتيجة للتطور المعلوماتي الحاصل فقد تعددت وتنوعت مظاهر التهديدات و المخاطر المعلوماتية سواء كانت العمدية منها أو غير عمدية، الأمر الذي يؤثر سلبا على استقرار وتبادل المعاملات الإلكترونية[4]، ويمكن تقسيم المخاطر المعلوماتية كما يلي:

---

[1]- ليتيم فتيحة، ليتيم نادية، الأمن المعلوماتي للحكومة الإلكترونية و إرهاب القرصنة، مجلة المفكر، العدد الثاني عشر، جامعة بسكرة، 2017، ص 239.

[2]- خالد ممدوح ابراهيم، أمن المعلومات الالكترونية، الدار الجامعية، الاسكندرية، 2008، ص27.

[3] - القحطاني محمد، الغثبر خالد، أمن المعلومات بلغة ميسرة، الطبعة الأولى، الرياض، 2009، ص23. نقلا عن نايف بن حسين بن مشبب الوادعي، فاعلية تضمين سياسات أمن المعلومات في تأمين مراحل بناء وتطوير الأنظمة المعلوماتية السعودية، رسالة ماجستير في العلوم الاستراتيجية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2016، ص19.

[4] - خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية للنشر، الإسكندرية، 2008 ، ص56.

1- **المخاطر البشرية:** وهي التي يمكن أن تحدث أثناء تصميم التجهيزات أو نظم المعلومات أو من خلال عمليات البرمجة أوالاختبار أو التجميع للبيانات أو أثناء ادخالها للنظام، أو في عمليات تحديد الصلاحيات للمستخدمين، وتسبب هذ الأخطاء نسبة كبيرة من المشاكل المعلوماتية التي تواجهها المؤسسات[1]. وتنقسم المخاطر البشرية إلى ما يلي:

- **المخاطر الداخلية:** من قبل الأفراد أوالعاملون الذين ينتمون لنفس الجهة المستهدفة؛
- **المخاطر الخارجية:** من قبل أشخاص من خارج المؤسسة.
- **خطر سوء الاستخدام:** حيث هناك بعض الأخطاء التي تنتج عن سوء استخدام الأفراد لشبكات المعلومات تلحق ضررا بالغا على أمن وسلامة البيانات داخل الشبكة.
- **القرصنة:** يشير مفهوم القرصنة الالكترونية إلى استخدام وسائل الاتصال وتكنولوجيا المعلومات الحديثة في ممارسات غير مشروعة، تستهدف التحايل على انظمة المعالجة الآلية للبيانات، لكشف البيانات الحساسة أو تغييرها والتأثير على سلامتها أو حتى إتلافها[2].

2- **المخاطر التقنية والفنية:** هي المخاطر الناجمة عن القصور والأخطاء الفنية في مختلف مكونات النظام والتي يغلب عليها الطابع الفني والتقني دون أن يكون هناك أي تدخل بشري أو طبيعي ومن مثلها ما يلي:

- **خطر سوء التصميم:** مثل الأخطاء الفنية في تصميم الأنظمة التي تعمل عليها الشبكات.
- **خطر التشويش:** فقد تتعرض المعلومات إلى نوع من التشويش في الإرسال والإستقبال عن طريق بعض المعدات أو البرامج التي تعمل على ذلك.
- **الفيروسات:** ويتمثل الفيروس في برنامج مصمم بهدف الدخول إلى أجهزة الحاسوب وإحداث الأضرار بها، بعرقلة المستخدم من التوصل إلى حاسوبه أو برامجه أو بياناته أو موارد الشبكة، وتصميم برامج التحطيم أوتغيير البيانات والذاكرة والأقراص الصلبة، كما أنه له القدرة على نسخ نفسه أكثر من مرة و يمتاز بقدرته على التخفي[3].

---

[1] - نجم عبد الله الحميدي وآخرون، نظم المعلومات الادارية، مدخل معاصر، دار وائل للنشر، عمان، 2005، ص263. نقلا عن سامية بوقرة، تطور استخدام تكنولوجيا المعلومات والاتصال والأمن المعلوماتي في المؤسسة، دراسة ميدانية بمؤسسة مطاحن سيبوس، مجلة علوم الانسان والمجتمع، العدد 12، نوفمبر 2014، ص 561.

[2] - ليتيم فتيحة، ليتيم نادية، مرجع سبق ذكره، ص 242.

[3] -جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات: رؤية جديدة للجريمة الحديثة، دار البداية للنشر، عمان، 2007، ص183.

3- المخاطر الطبيعية: تعتبر الكوارث الطبيعية من ضمن ما يمكن أن يكون خطراً على الشبكات وبنيتها التي يمكن أن تقع دون أي تدخل بشري أو عطب فني[1]، مثل الزلازل والبراكين والحرائق وغيرها، ولذا يجب عمل نسخ احتياطية بشكل منتظم لمحتويات الشبكة وحفظها في أماكن بعيدة عن مكان الشبكة الأم حتى يمكن استرجاع المعلومات في حالة حدوث أي نوع من هذه الكوارث للشبكة نفسها[2].

المحور الثاني: تطور مهنة التدقيق الداخلي في بيئة تكنولوجيا المعلومات

لقد تعددت تعاريف التدقيق الداخلي، والتعريف الأكثر قبولا هو ذلك الصادر عن ي المعهد الأمريكي للمدققين الداخليين في جوان1999 والمعدل في2010 من خلال النسخة المعدلة من معايير الممارسة المهنية الدولية الصادرة في2008، والمتمثل فيما يلي: "التدقيق الداخلي هونشاط مستقل وموضوعي يقدم تأكيدات وخدمات استشارية بهدف إضافة قيمة للمؤسسة وتحسين عملياتها، وتساعد هذه الوظيفة في تحقيق أهداف المؤسسة من خلال إتباع أسلوب منهجي لتقييم وتحسين فعالية عمليات الحوكمة والرقابة وإدارة المخاطر"[3]. وأدى هذا المفهوم الحديث للتدقيق الداخلي إلى توسيع واجباته وإبراز دوره الواسع الذي تحول من كونه أداة للرقابة الداخلية ليشمل أيضاً **التعريف بالمخاطر** التي تتعرض لها المؤسسة وتقديم الاستشارات اللازمة للإدارة العليا في هذا الخصوص. وقد أشارت دراسة كل من Arena[4] وAzzone إلى أهمية الدور الذي تلعبه وظيفة التدقيق الداخلي في إدارة المخاطر من خلال تنبيه الإدارة ولجنة المراجعة إلى المخاطر الهامة التي تؤثر على أهداف وموارد المؤسسة وكذا تقديم الأساليب الملائمة للتغلب على هذه المخاطر. وأشارت Hermanson[5] إلى أن تقرير"Deloitte" بعنوان" تعظيم دور المراجعة الداخلية في ظل عصر قانون Sarbanes-Oxley أكد على أهمية تركيز التدقيق الداخلي على إدارة المخاطر. ومنذ وقت ليس ببعيد، كانت المخاطر العالية بالنسبة للمؤسسات تتمثل في التوافق مع اللوائح التنظيمية بالإضافة إلى الظروف الاقتصادية، أما اليوم، فقد أصبحت القضايا الرئيسية تشمل الابتكارات الجديدة والتحول الرقمي ومقاومة التغيير المؤسسي والتهديدات السيبيرانية وثقافة الشركات. وقد أظهر الاستطلاع الذي قام به المعهد الأمريكي للمدققين الداخليين عام2015 على عينة من المدققين على المستوى العالمي أن المخاطر المعلوماتية

---

[1] - نايف بن حسين بن مشبب الوادعي، مرجع سبق ذكره، ص57.

[2] - حسنين رجب عبد الحميد، أمن شبكات المعلومات الإلكترونية: المخاطر والحلول، مجلة Cybrarians Journal، العدد 30 ، أبو ظبي، ديسمبر 2012، متاح على الموقع:
http://journal.cybrarians.info/index.php?option=com_content&view=article&id=629:networks&catid=257:studies&Itemid=0 cànsulté le 29/07/2018.

[3] - يوسف داوود الصبح، دليل التدقيق الداخلي وفق المعايير الدولية، الطبعة الثانية، إتحاد المصارف العربية، لبنان، 2010، ص 46.

[4]- Arena, A. and G. Azzone, Development trends and future prospects of internal audit, Managerial Auditing Journal, Bradford, Vol.12, Iss. 4/5, 2005, p 200.

[5]- Hermanson, D, Internal auditing: getting beyond the section 404 implementation crisis, Internal Auditing, Boston, Vol.21, Iss.3, 2006, p 39.

أصبحت ضمن أهم خمس مخاطر التي يوليها المدققون الداخليون اهتماما خاصا من أجل إدارتها[1]، حيث 42% من العينة أجابت بأن المخاطر المعلوماتية تشكل صلب اهتمام التدقيق الداخلي[2]. كما واستنادا إلى استجابة استطلاع الرأي الذي قامت به شركة Protivitti حول المخاطر لعام 2018[3]، فإن هناك تحولات ملحوظة في ما يشكل أكبر10 مخاطر لعام2018 مقارنة بالعام الماضي. والجدول الموالي يوضح مكانة المخاطر الالكترونية ضمن المخاطر الكلية الأكثر أهمية بالنسبة للمنظمة.

الجدول رقم 1: تطور المخاطر والتهديدات المعلوماتية ضمن سلة المخاطر

الترتيب	2015	2017	2018
1	التوافق مع التغييرات التنظيمية والتشريعية	الظروف الاقتصادية في الأسواق المحلية والدولية	زيادة سرعة الابتكار
2	الظروف الاقتصادية	التغيير التنظيمي	مقاومة التغيير
3	**التهديدات الإلكترونية**	**المخاطر الإلكترونية**	**إدارة التهديدات السيبيرانية**
4	القدرة على جذب أفضل المواهب والحفاظ عليها	سرعة الابتكار الهدّام	التغيير في التشريعات وزيادة متطلبات التوافق مع اللوائح التنظيمية.
5	ثقافة مؤسسية لا تساهم في تحديد المخاطر	الخصوصية وحماية الهوية	الثقافة المؤسسية قد لا تشجع تصعيد قضايا المخاطر في الوقت المناسب

المصدر من إعداد الباحث بتصرف من التقارير:

- الرؤى التنفيذية لبروتيفيتي حول أهم المخاطر في 2015

-http://www.protiviti.com/en-US/Documents/Surveys/NC-State-Protiviti-Survey- Top-Risks-2015.pdf

-https://www.knowledgeleader.com/Knowledge-Leader/Content.ns/Web+Content/SRExecutive-PerspectivesonTopRisksfor2017!OpenDocument

-https://www.protiviti.com/US-en/insights/ protiviti-top-risks-survey2018.

[1] - Larry Harrington, Arthur Piper, Réussir dans un monde en mutation: dix impératifs pour l'audit interne, CBOK2015, IIA, P15.

[2] - IIA, rapport mondial pulse of the profession 2015, Saisir les opportunités dans un monde en perpétuelle évolution, cbok 2015, juillet 2015, p6.

[3] - فيشال ذكار، ملخص تنفيذي بشأن أعلى المخاطر لعام 2018، مجلة المدقق الداخلي الشرق الأوسط، الامارات العربية، مارس 2018، ص 6. ويمكن الاطلاع على تقرير المخاطر من خلال الموقع:
https://www.protiviti.com/US-en/insights/ protiviti-top-risks-survey

ويظهر جليا من نتائج هذه الاستطلاعات أن المخاطر المعلوماتية أصبحت تشكل اهتماما بالنسبة للمؤسسات وأن رؤى هذه الأخيرة وبعدما كان توجهها منصبا على المخاطر المالية وغيرها أصبح حاليا يركز على المخاطر المعلوماتية التي تتطور باستمرار، الشيء الذي يدفع المؤسسات إلى إيجاد الطرق المناسبة لإدارتها لاسيما وأنها تتميز بصعوبة القياس و بالفجائية، وهذا ما جعل المؤسسات من جهة، تحتاج إلى وظيفة التدقيق الداخلي التي تدعم إدارة المخاطر المعلوماتية وتقدم تأكيدا أن هذه الأخيرة تدار بالطريقة الجيدة، و من جهة أخرى توسع نطاق ودور وظيفة التدقيق الداخلي من دورها التقليدي وهو التدقيق المالي إلى التدقيق الإداري إلى التركيز على إضافة قيمة للمنظمة عن طريق المساهمة في إدارة المخاطر[1] بصفة عامة والمعلوماتية بصفة خاصة، الشيء الذي يتطلب من المدققين الداخليين الاطلاع المتواصل على مستجدات العالم الرقمي من خلال التحديث المستمر لمعارفهم المتعلقة بالتقنيات الحالية والمخاطر المرتبطة بها، حتى يتمكنوا من أداء دورهم التأكيدي وتقديم المشورة إلى المعنيين بشأن أفضل الطرق الممكنة للتعامل مع مخاطر تكنولوجيا المعلومات الحالية والناشئة. وقد أشار إطار الممارسات المهنية الدولية لمهنة التدقيق الداخلي إلى ثلاثة معايير تحدد مسؤوليات المدققين الداخليين الخاصة بالتكنولوجيا وهي[2]:

المعيار رقم 1210 الكفاءة (معيار التأكيد رقم 3): يجب أن يتوفر لدى المدققين الداخليين معرفة كافية بالمخاطر الرئيسية المرتبطة بتقنية المعلومات وضوابطها وأساليب التدقيق القائمة على التقنيات المتوفرة لأداء الأعمال الموكلة إليهم. بيد أنه ليس من المتوقع أن يتمتع جميع المدققين الداخليين بخبرة المدقق الداخلي الذي تقتصر مسؤوليته الرئيسية على تدقيق تقنية المعلومات.

المعيار رقم 1220 العناية المهنية الواجبة (معيار التأكيد رقم 2): أثناء ممارسة العناية المهنية الواجبة، يجب على المدققين الداخليين النظر في استخدام أساليب التدقيق القائمة على التقنيات وغيرها من أساليب تحليل البيانات الأخرى.

المعيار رقم 2110 الحوكمة (معيار التأكيد رقم 2): يجب ألا يغفل نشاط التدقيق الداخلي تقييم ما إذا كانت حوكمة تقنية المعلومات في المؤسسة تدعم استراتيجيات المؤسسة وأهدافها أم لا.

المحور الثالث: دور التدقيق الداخلي في إدارة المخاطر المعلوماتية وفق نموذج خطوط الدفاع الثلاثة

باتت جميع أنواع المؤسسات أكثر عرضة للتهديدات الحاسوبية بسبب تزايد الاعتماد على العالم الحاسوبي مثل أجهزة الكمبيوتر والشبكات والبرامج والتطبيقات ومواقع التواصل الاجتماعي. وللتصدي لهذا الخطر الناشئ، يواجه الرؤساء التنفيذيين للتدقيق تحديًا متمثلاً في ضمان وضع الإدارة ضوابط وقائية وكشفية على السواء وتنفيذها. كما أن الرؤساء

[1] - يوسف داوود الصبح، دليل التدقيق الداخلي وفق المعايير الدولية، الطبعة الأولى، دار الكتب العلمية للنشر، القاهرة، 2007، ص318.

[2] - معهد المدققين الداخليين (IIA)، المعايير الدولية للممارسة المهنية للتدقيق الداخلي، نسخة 2017. متاح على الموقع: https://na.theiia.org/translations/PublicDocuments/IPPF-Standards-2017-Arabic.pdf. Consulté le 30/07/2018.

التنفيذيين للتدقيق ملزمون بوضع نهجٍ للتدقيق الداخلي يساعد في تقييم الخطر الذي يفرضه الأمن الحاسوبي وقياس قدرة الإدارة على الاستجابة، مع تركيز خاص على وقت الاستجابة السريعة.

وقد قام معهد المدققين الداخليين بإصدار دليل **"تقييم خطر الأمن الحاسوبي: أدوار خطوط الدفاع الثلاثة"** لمساعدة المدققين الداخليين في تنمية كفاءتهم في تقديم تأكيد عن المخاطر التي يفرضها الأمن الحاسوبي. كما يناقش الدليل دور التدقيق الداخلي في الأمن الحاسوبي ويقيّم المخاطر الناشئة والتهديدات

المشتركة الأخرى التي تواجهها جميع خطوط الدفاع الثلاثة ويطرح منهجًا واضحًا لتقييم مخاطر وضوابط الأمن الحاسوبي[1]. وفيما يلي عرض لخطوط الدفاع الثلاثة لإدارة المخاطر المعلوماتية:

1- خط الدفاع الأول: الضوابط التي تضعها الإدارة (ضوابط الرقابة الداخلية)

يشمل خط الدفاع الأول إدارة أمن المعلومات ووحدات الأعمال الأخرى وموظفي الخط الأمامي الذين يمكنهم من خلال أداء مهامهم ومسؤولياتهم إدارة المخاطر المعلوماتية كجزء من الأنشطة اليومية الخاصة بهم وذلك من خلال تنفيذ الضوابط الرقابية مختلفة وهو ما يعرف **بالرقابة الداخلية.** وعرفت لجنة COSO[2] الرقابة الداخلية بأنها: "جميع السياسات والإجراءات التي تتبناها الإدارة من أجل التأكد من أداء الأعمال بكفاءة عالية بما في ذلك تنفيذ السياسات الإدارية وحماية الأصول، ومنع الغش والخطأ أواكتشافه، ودقة اكتمال السجلات والدفاتر المحاسبية وإعداد معلومات مالية يمكن الاعتماد عليها في الوقت المناسب"[3]. ولقد أصدرت لجنة COSO تقرير حول الرقابة الداخلية عام 1992، والذي قدم إطارا متكاملا للرقابة الداخلية، وفي 14 ماي 2013[4] قامت اللجنة بنشر إطار جديد أسمته COSO 2013 يهدف إلى تكييف نظام الرقابة الداخلية لرهانات اليوم والغد، حيث يأخذ الإطار الجديد بعين الاعتبار كل التطورات الحاصلة خلال العشرين سنة الماضية[5] منذ صدور النسخة الأصلية للمرجع عام1992، أين كانت الشركات تعمل في بيئة مختلفة بشكل ملحوظ، فقد كان عدد مستخدمي الإنترنت أقل من الحالي، حتى أن مايكروسوفت لم تكن قد أطلقت بعد المتصفح إنترنت إكسبلورر، ومن ثم كانت الشركات تلجأ في الغالب إلى الهاتف والفاكس للتواصل، إلا أن تكنولوجيا المعلومات في العقدين الماضيين شهدت تحولاً كبيراً يتحكم فيه الفضاء الإلكتروني في المقام الأول. ويتضمن الاطار الجديد كيفية إدارة المؤسسات للابتكار في تكنولوجيا المعلومات مع الأخذ بعين الاعتبار[6] المخاطر الجديدة الناشئة والتي تمثل رهانات جديدة للرقابة الداخلية مثل خطر

[1] - https://na.theiia.org/standards-guidance/recommended-guidance/practiceguides/Pages/GTAG-Assessing-Cybersecurity-Risk-Roles-of-the-Three-Lines-of-Defense.aspx.
[2] - COSO: Committee of Sponsoring Organization of the Tread way Commission.
[3] - Coopers et Lybrand , la nouvelle pratique du contrôle interne, 2eme tirage, éd d'Organisation, 1994, P24.
[4] - Neuilly –sur –seine , le 26 /04/2013 :communiqué de presse 2013-coso 2013 .
[5]- KPMG, publication internal control integrated framework 2013 do COSO, rapport KPMG, 2013, p1.
[6] - IFACI ET PWC- Jean pierre HOTTIN et autres, COSO 2013 une opportunité pour optimiser votre contrôle interne dans un environnement en mutation, propos du colloque du 21.05.2013, paris, juillet 2013, p7.

جرائم الانترنت والحوسبة السحابية وكذا الدور المهم الذي لا تزال تلعبه التكنولوجيا خاصة في ميادين الأداء، الأمن المعلوماتي ...الخ؛ كما يركز الإطار الجديد على العلاقة بين الخطوط الثلاثة للدفاع في المؤسسة[1]؛

ويمكن تقسيم **ضوابط الرقابة الداخلية** إلى ضوابط وقائية، كشفية وأخيرا تصحيحية[2]:

1- **الضوابط الوقائية:** تشمل الانواع الرئيسية من الضوابط الوقائية المستخدمة لأنظمة المعلومات:

- ✓ **تصريح الدخول:** يتم في هذا الضابط تحديد الاشخاص المصرح لهم بالدخول للنظام من خلال إمّا اعطاءُه كلمة المرور أو بصمة أوبطاقة الوصول.
- ✓ **الصلاحيات:** يتم فيها اعطاء صلاحيات للدخول للأنظمة الفرعية بعد التأكد من امتلاك تصريح الدخول للنظام الرئيسي، وذلك حسب الوصف الوظيفي للموظف، و من الضروري وجود مصفوفة الصلاحيات للأنظمة لدى قسم تكنولوجيا المعلومات.
- ✓ **التدريب:** يجب تدريب الموظفين على كيفية حماية اجهزتهم والحفاظ عليها.
- ✓ **ضوابط الوصول المادّي:** وهنا يجب حماية غرفة الخادم الرئيسي (Server) من الدخول غير المصرح له عن طريق بطاقة الدخول او البصمة، كما يجب الحماية من دخول الزوار للمبنى من خلال وضع مرافق للزائر خلال تجواله في مبنى المؤسسة، وحماية الاجهزة من سوء الاستخدام.
- ✓ **ضوابط الوصول عن بعد:** يوجد عده تقنيات مستخدمة لحماية البيانات والأنظمة من التلاعب ومنها أجهزة التوجيه والجدران النارية وأنظمة منع التسلل و تحويل العناوين الرقمية ووضع إجراءات خاصة لأمان الشبكات اللاسلكية.
- ✓ **التشفير:** يكون التشفير هو الحاجز النهائي في عملية وضع الضوابط الوقائية ويتم من خلاله تحويل البيانات من النصوص المقروءة إلى بيانات غير مقروءة مع إمكانية إرجاع البيانات إلى حالتها الطبيعية عند الحاجة.
- ✓ **التحديث التلقائي:** ما يساعد على إيجاد التحسينات المستمرة لسد نقاط الضعف في البرامج والأنظمة؛
- ✓ **التخزين الاحتياطي** لنسخ من محتويات الحواسيب أو شبكات المعلومات في مكان آمن وبعيد؛

2- **ضوابط الكشف:** لا يوجد هنالك أنظمة وقائية تحمي أنظمة المعلومات بشكل كامل نظرا لتطور اساليب مخترقي البيانات و وجود ثغرات في اي نظام للمعلومات، ومن هنا يجب ان يكون هنالك ضوابط تقوم بالكشف

[1]- ولمزيد من التفاصيل يمكن الرجوع الى:

-Henri-Pierre MADERS et autres, les métiers d'auditeur interne et de contrôleur permanent, groupe EYROLLES, Paris, 2015, p13. Et IFACI,trois lignes de maitrise pour une meilleure performance, fiabiliser la stratégie par une gestion organisée des risques, paris, 2013. Et AMRAE (l'association de management des risques et des assurances de l'entreprise): Organisation de la Maîtrise des risques : 3 lignes de performance du CAC 40 à l'ETI, 21eme rencontre de l'AMRAE du 06 au 08 fevrier 2013, lyon.

[2] - احمد سلامة الملاجي، هل نظم الرقابة على أنظمة المعلومات لدى مؤسستك موثوقة ؟، مجلة المدقق الداخلي الشرق الأوسط، عدد ديسمبر 2017، ص10.

عن اي اختراقات لأنظمة المعلومات، فمن خلال ضوابط الكشف يتم الحكم على فعالية أنظمة الضوابط الوقائية. وتتمثل ضوابط الكشف فيما يلي:

- ✓ **تحليل ملف الحركات:** وهو ملف يقوم بتسجيل جميع الحركات التي يقوم بها المستخدم من حذف وتعديل واضافة على سجلات قواعد البيانات.
- ✓ **نظام كشف التسلل:** يقوم بإنشاء سجل للعناوين والمواقع التي مسموح لها المرور إلى الجدار الناري.
- ✓ **التقارير الإدارية:** القيام بعمل تقارير إدارية تشمل مؤشرات الاداء الرئيسية من حيث التوقف عن العمل بسبب الحوادث الامنية وعدد الأنظمة التي تم تركيبها وصيانتها وتطويرها والوقت اللازم للاستجابة للحوادث الامنية التي تم اكتشافها.
- ✓ **اختبار أمن نظام المعلومات:** هنالك العديد من التقنيات التي تستخدم لفحص النظام من الثغرات ونقاط الضعف، حيث يمكن لشخص القيام بمحاولة اختراق نظام المعلومات (شخص مصرح له او شركة استشارات أمنية)للوقوف على الثغرات ونقاط الضعف ومعالجتها.

3- **الضوابط التصحيحية:** وتتضمن التأكد من ان جميع الثغرات والمشاكل التي تم اكتشافها، تم وسوف يتم تصحيحها ومن هذه الضوابط:

- ✓ **فريق الاستجابة للطوارىء الحاسوبية:** يتألف من المتخصصين التقنيين وإدارة العمليات، للتعامل مع الحوادث الرئيسية والتي يجب ان تمارس بإنتظام: إدراك وجود مشكلة، إحتواء المشكلة، حل المشكلة والمتابعة.
- ✓ **ضابط الأمن الرئيسي:** هو فرد معين مسؤول عن نطاق المؤسسة الامني، وينبغي أن يقدم هذا الشخص تقريرا إلى رئيس العمليات أو الرئيس التنفيذي وأن يكون مستقلاً عن وظائف إدارة نظام المعلومات.

2- خط الدفاع الثاني: إدارة المخاطر

يتألف خط الدفاع الثاني من مدراء المخاطر الذين ينظرون إلى المخاطر على مستوى المؤسسة، تراقب هذه الوظيفة كيفية تعامل الإدارة **(الخط الأول)** مع المخاطر المعلوماتية من خلال تحديد مدى مراقبة المخاطر بشكل فعال وإدارتها بشكل مناسب[1]. ومن الواضح أن المؤسسة لا يمكنها إنشاء خط الدفاع الثاني – والذي يتمثل في وظيفة إدارة المخاطر دون وجود أعضاء إدارة مؤهلة أو موظفين في المؤسسة يتحملون المسؤولية المباشرة لإدارة مخاطر الأعمال، ويجب أن تكون إدارة المخاطر المؤسسية مدعومة من خط الدفاع الأول الذي يتحمل المسؤوليات التالية[2]:

[1] - يمكن الاطلاع على:
https://securityintelligence.com/take-a-load-off-delegate-cyber-risk-management-using-/the-three-lines-of-defense-model.

[2] - إيهاب سيف، هل شركتكم مستعدة لإنشاء وظيفة معنية بإدارة المخاطر المؤسسية؟، مجلة المدقق الداخلي –الشرق الأوسط، الامارات العربية، سبتمبر 2016، ص 22.

- مساعدة فرق إدارة المخاطر المؤسسية في تحديد حجم المخاطر التي يمكن للمؤسسة تحمله وحجم المخاطر التي ترغب المؤسسة في تحمله وحدود المخاطر؛
- دعم وظيفة إدارة المخاطر المؤسسية فيما يتعلق بتحليل وتحديد المخاطر الاستراتيجية؛

وقد قامت لجنة (COSO) في عام 2004 بنشر المفاهيم الرئيسية للإطار المتكامل في إدارة مخاطر المشروع ERMوالتي تشير إلى أن عملية إدارة مخاطر[1] هي عملية تنفذ بواسطة مجلس إدارة المنظمة والإدارة وكل الأفراد، لتطبيق الإستراتيجية الموضوعة عبر المنظمة وكل أنشطتها ومصممة لتحديد الأحداث المحتملة التي ربما تؤثر على المنظمة وإدارة الخطر لكي يكون ضمن المخاطر المقبولة، لتوفير تأكيد معقول بالنسبة لإنجاز الأهداف الإستراتيجية؛ التشغيلية؛ أهداف التقارير وأهداف الامتثال".

ونظرا لزيادة تعقيدات التي أصبحت تميز المحيط الاقتصادي وكذا التطورات التكنولوجية التي يجب على المؤسسات مواجهتها[2] والتي أدت إلى تطور و تعقيد المخاطر، أعلنت لجنة المنظمات الراعية COSO عن إصدار تحديث إطار العمل المتكامل الخاص بإدارة المخاطر المؤسسية في 6 سبتمبر2017[3]، ويقوم إطار العمل المنقح بتوضيح أهمية إدارة المخاطر عند إعداد استراتيجية المؤسسة، وكذا تعزيز العلاقة بين الأداء وإدارة مخاطر من أجل تحسين عملية تحديد الأهداف وفهم أثر المخاطر على أداء المؤسسة، كما يأخذ هذا التحديث بعين الاعتبار كل التطورات التكنولوجية[4] والمخاطر المرتبطة بها.

3- خط الدفاع الثالث: التدقيق الداخلي

خط الدفاع الثالث هو التدقيق الداخلي وقد يشمل مدخلات من المدققين الخارجيين و/أو الجهات التنظيمية أيضا. ويمكن للخط الثالث تحديد ما تؤكده الخطوط السابقة فيما يتعلق بكفاية الضوابط الموجودة. حيث يمكن للتدقيق الداخلي أن يلعب دورًا محورياً إذ ينبغي على المؤسسات عند وضعها لخطط الأمن الإلكتروني أن تطلب من التدقيق الداخلي اتخاذ الإجراءات الأكثر ملائمة لها مثل اختبار فعالية الضوابط الرقابية (الضوابط الوقائية وضوابط الكشف) والبروتوكولات ومدى كفاءتها. وبناءً على نتائج الاختبار، تتم طمأنة مجلس الإدارة والإدارة بشأن هذه الآليات. ويجب أن يركز التدقيق الداخلي على المجالات الأربعة التالية المتعلقة بالأمن الإلكتروني[5]:

---

[1]- The COSO, **Enterprise Risk Management-Integrated Framework: Executive Summary**, USA, September 2004, p p1-7.

[2] IFACI, les apports du référentiel COSO ERM 2017, 5eme conférence annuelle de l'IFACI, beffroi de Montrouge, 16.17 novembre 2017, p4.

[3] -Nouveau cadre de gestion du risque d'entreprise du COSO : Enterprise Risk Management – Integrating with Strategy and Performance (2017). Disponible sur le site: https://www.iasplus.com/fr-ca/standards/assurance/autres-normes-canadiennes/coso2019s-updated-erm-framework-enterprise-risk-management-integrating-with-strategy-and-performance-2017. Consulté le 07/08/2018.

[4] - COSO, Le management des risques de l'entreprise : Une démarche intégrée à la stratégie et à la performance Synthèse, juin 2017, P III.

[5] -فيشال ذكار، الدور الحيوي الذي يلعبه التدقيق الداخلي في مجال الأمن الإلكتروني، مجلة المدقق الداخلي –الشرق الأوسط، الامارات العربية، يونيو 2017، ص6.

1- تقديم ضمانات بشأن مستوى الاستعداد والقدرة على الاستجابة؛
2- إبلاغ مجلس الإدارة والإدارة التنفيذية بمستوى المخاطر التي تتعرض لها المؤسسة والجهود المبذولة لمعالجة هذه المخاطر؛
3- العمل بالتنسيق مع قسم تكنولوجيا المعلومات وغيره من الأطراف ذات الصلة لبناء الأنظمة والضوابط الدفاعية والردود الفعّالة؛
4- ضمان التواصل والتنسيق.

وفيما يلي عرض لبعض المخاطر الرئيسية التي تتعرض إليها المؤسسات والتي يجب أخذها بعين الاعتبار فيما يتعلق بالتكنولوجيا الناشئة وهي:

1- الأمن الحاسوبيCyber Security : لتقديم ضمانات بشأن مخاطر الأمن الحاسوبي، يمكن للمدقق الداخلي إجراء مسح للثغرات الأمنية في الشبكة وفحص مدى قابليتها للاختراق، ومراجعة تصميم البنية التحتية للشبكة، واستعراض آخر حوادث الاختراق الأمني، وتنفيذ بعض الفحوصات لضمان مرونة وفعالية خطة إدارة الأزمات في المؤسسة.

2- مواقع التواصل الاجتماعي Social Media: إن غالبية الشركات تتواجد على الإنترنت عبر مواقع التواصل الاجتماعي الشيء الذي قد يؤدي إلى نشر معلومات مغلوطة وسلبية من قِبل عملاء أو موظفين أو أفراد مستائين وحاقدين على الشركة. كما قد يقوم الموظفون الذين يشاركون أنشطة يومية مع أصدقائهم بالإفصاح سهوًا وبدون قصد عن معلومات قد تضر بسمعة الشركة أو الإفصاح عن معلومات تعتبر سرية. وفي هذا الجانب، يمكن للمدقق الداخلي تزويد الإدارة بتقييمٍ مستقل فيما يتعلق بفعالية الضوابط المطبقة على مواقع التواصل الاجتماعي الخاصة بالشركة، كما يمكنه تدقيق سياسات مواقع التواصل الاجتماعي وإجراءاتها، واستعراض مدى كفاية التدريب لأجل التوعية باستخدام مواقع التواصل الاجتماعي والمعلومات التي يمكن نشرها، إجراء مسحٍ لمواقع التواصل الاجتماعي لتحديد ما يمكن نشره من معلومات تخص المؤسسة.

3- الحوسبة النقّالة Mobile Computing: تشمل أجهزة الحوسبة النقّالة الهواتف الذكية وأجهزة الكمبيوتر المحمولة ومحركات أقراص (USB) والكاميرات الرقمية وغيرها من الأجهزة المثيلة. وقد تحتوي هذه الأجهزة على معلومات سرية أو حقوق ملكية فكرية وأسرار مهنية خاصة المؤسسة. وهنا ينبغي للمدقق الداخلي دراسة المخاطر المرتبطة باستخدام الأجهزة النقّالة وربطها بمستوى حساسية المعلومات التي تُخزّنها وتصل إليها هذه الأجهزة، والعمليات التي تعالجها، من منظور الأعمال والقوانين واللوائح التنظيمية. كما يمكن للمدقق الداخلي تدقيق مخزون الأجهزة النقّالة، واستعراض كيفية إدارة الأجهزة المسروقة والمفقودة، والتأكد من تطبيق الضوابط المقررة للأجهزة

المفقودة، ومراجعة آليه تصنيف المعلومات التي يمكن تخزينها على الأجهزة النقّالة، والتأكد من عدم تخزين معلومات المؤسسة الحساسة على الأجهزة النقّالة أو تشفيرها بطريقة آمنة.

4- الحوسبة السحابية Cloud Computing: إن العالم في طور التحوّل من الأسلوب التقليدي في تخزين ومعالجة البيانات ضمن موقع مخصص لتكنولوجيا المعلومات إلى استخدام المصادر التقنية المشتركة التي يوفرها مزودي الخدمات عبر شبكة الإنترنت، وهو ما يُعرف باسم"الحوسبة السحابية" والتي تعني مجموعة من الخدمات والتطبيقات والبرمجيات والأجهزة والعتاد والمصادر التي تتوفر عن طريق الانترنت وتدار من قبل طرف ثالث يدعى مقدم الخدمة في مركز بيانات ويحصل العميل والذي يسمى مشارك على كل ذلك أو على بعضه حسب احتياجه وفق نظام الدفع بحسب الاستخدام[1] وبمقابل مالي[2].

ويمكن أن يلعب المدقق الداخلي دورا هامًا في تبني وتطبيق تقنيات الحوسبة السحابية خاصة في المراحل المبكرة للتطبيق، حيث يمكن له أن يكون ضمن فريق العمل التقني المسؤول عن تحديد وتقييم المخاطر المرتبطة بمثل هذه البيئة التكنولوجية، والتي تتطلب منه فهم التقنيات والعمليات التي تستند إليها الحوسبة السحابية، فضلاً عن العمليات والمعايير المعقّدة المستخدمة في تقييم أداء مُزوّد الخدمة. كذلك ينبغي للمدقق الداخلي أن يفهم متطلبات شركته التعاقدية والتشغيلية والتنظيمية التي قد تتأثّر[3]. ويمكن لقسم التدقيق الداخلي أن يقدم الخدمات التالية:

- تحديد ما إذا كان مُزوّد الخدمة مستوفٍ لمتطلبات الشركة الخاصة بأمن البيانات وتحليل/تقييم إجراءاته الأمنية استنادًا إلى المعايير مثل معايير ISO [4].
- مراجعة اتفاقية مستوى الخدمة لضمان حق المؤسسة في التدقيق على مزود الخدمة واستخدام الخدمة السحابية و إجراء بعض عمليات التدقيق المحدودة. والاستفسار عن موقع حفظ البيانات والمخاطر المحتملة من حفظ البيانات في دولةٍ أخرى خصوصاً فيما يتعلق بمسألة الخصوصية وإمكانية الوصول إلى البيانات، بالإضافة إلى استعراض مقاييس الجودة بخصوص انقطاع الخدمة وتوقيت التحسينات والتعديلات الطارئة على اتفاقية مستوى الخدمة.

---

[1] - العليمي ثروت، العليمي المرسي، سبل الافادة من تطبيقات الحوسبة السحابية في تقديم خدمات المعلومات بدولة الامارات العربية المتحدة، 2014، نقلا عن فردي لخضر، اتجاهات المكتبيين نحو استعمال الحوسبة السحابية بالمكتبات الجامعية الجزائرية في ضوء نموذج قبول التكنولوجيا، المجلة العراقية للمعلومات، المجلد الثامن عشر، العددان 1-2، 2017، ص 109.

[2]- Ibrahim Safieddine, Optimisation d'infrastructures de cloud computing sur des green datacenters, Thèse de doctorat, spécialité informatique, université de Gronoble, 2018, p10.

[3] - عارف زمان، المخاطر الناشئة لتقنية المعلومات :تحديات جديدة في انتظار المدققين الداخليين، مجلة المدقق الداخلي الشرق الأوسط، الامارات العربية، ديسمبر 2016، ص 31.

[4] - عارف زمان، الحوسبة السحابية، مجلة المدقق الداخلي – الشرق الأوسط، الامارات العربية، مارس 2018، ص 11.

- تحديد ما إذا كان بمقدور مُزوّد الخدمة الوفاء بمتطلبات النمو المتوقع للمؤسسة، وإذا لم يكن بمقدوره ذلك، تحديد ما إذا كان لدى المؤسسة خطة طوارئ بديلة في حال لم تستطع نظم مُزوّد الخدمة التوسع لتلبية احتياج المؤسسة.

خاتـمة

من خلال هذه الورقة البحثية يمكن تلخيص أهم النتائج التي تم التوصل إليها في النقاط التالية:

- يعتبر التدقيق الداخلي أداة لمد الإدارة العليا بالمعلومات الضرورية التي تساعدها في اتخاذ القرارات من ناحية، وإمدادها بالمعلومات عن مدى كفاءة وفعالية نظام الرقابة الداخلية المطبق من ناحية أخرى.

- اتسع نطاق التدقيق الداخلي من الدور التقليدي وهو المراجعة المالية إلى الدور الحديث وهو المراجعة الإدارية ثم إلى المساهمة في خلق القيمة عن طريق دعم إدارة المخاطر عامة والمعلوماتية منها بصفة خاصة وهو ما يمثل تحديا كبيرا للمؤسسات ولأقسام التدقيق الداخلي بصفة خاصة.

- أظهرت الاستطلاعات التي قام بها المعهد الأمريكي للمدققين الداخليين ومؤسسات أخرى

راجعين الداخليين بعد الأزمة العالمية أن أقسام المراجعة الداخلية كثفت مجهوداتها في تقييم فعالية إدارة المخاطر.

- تهدف إدارة المخاطر إلى تخفيف احتمالات حدوث المخاطر، وتخفيض الخسارة المحتملة عند وقوع هذه المخاطر وتعتبر المراجعة الداخلية عنصرا فعالا في إدارة المخاطر خاصة بعد الأزمة المالية وذلك من خلال مساعدة المدراء في تحديد المخاطر، تقييمها وكيفية الاستجابة والتعامل معها.

- بعدما كان اهتمام المؤسسات منصبا على المخاطر المالية وغيرها أصبح حاليا ويركز على المخاطر المعلوماتية التي تتطور باستمرار، الشيء الذي يدفع المؤسسات إلى إيجاد الطرق المناسبة لإدارتها لاسيما وأنها تتميز بصعوبة القياس و بالفجائية، وهذا ما جعل المؤسسات من جهة، تحتاج إلى وظيفة التدقيق الداخلي التي تدعم إدارة المخاطر المعلوماتية وتقدم تأكيدا أن هذه الأخيرة تدار بالطريقة الجيدة.

- أصبحت المخاطر المعلوماتية تشكل صلب اهتمام التدقيق الداخلي، فهي ضمن أهم خمس مخاطر التي يوليها المدققون الداخليون اهتماما خاصا من أجل إدارتها.

- مع حدوث تغيرات مستمرة في البيئة المؤسسية وتحوُّل إجراءات العمل بالمؤسسات من الأساليب التقليدية إلى التكنولوجيا الرقمية والذكية المتطورة، تزايدت حاجة المدققين الداخليين إلى فهم أثر هذه الابتكارات والتطورات التكنولوجية الحديثة ومدى قدرتها على تحسين أعمالهم.

قائمة المراجع:

المراجع باللغة العربية:

- **الكتب:**

1- القحطاني مُحَمَّد، الغثبر خالد، أمن المعلومات بلغة ميسرة، الطبعة الأولى، الرياض، 2009.
2- الطائي مُحَمَّد، الكيلاني ينال، إدارة أمن المعلومات، الطبعة الأولى، دار الثقافة للنشر، عمان، 2015.
3- جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات: رؤية جديدة للجريمة الحديثة، دار البداية للنشر، عمان، 2007.
4- خالد ممدوح ابراهيم، أمن المعلومات الالكترونية، الدار الجامعية، الاسكندرية، 2008، ص27.
5- نجم عبد الله الحميدي وآخرون، نظم المعلومات الادارية، مدخل معاصر، دار وائل للنشر، عمان، 2005.
6- يوسف داوود الصبح، دليل التدقيق الداخلي وفق المعايير الدولية، الطبعة الأولى، دار الكتب العلمية للنشر، القاهرة، 2007، ص318.

الاطروحات والرسائل:

7- نايف بن حسين بن مشبب الوادعي، فاعلية تضمين سياسات أمن المعلومات في تأمين مراحل بناء وتطوير الأنظمة المعلوماتية السعودية، رسالة ماجستير في العلوم الاستراتيجية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2016.

المقالات:

8- إيهاب سيف، هل شركتكم مستعدة لإنشاء وظيفة معنية بإدارة المخاطر المؤسسية؟، مجلة المدقق الداخلي – الشرق الأوسط، الامارات العربية، سبتمبر 2016.
9- بلجراف سامية، كلاش خلود، الإدارة الإليكترونية وإشكالية الأمن المعلوماتي، مجلة الناقد للدراسات السياسية، العدد 1، جامعة مُحَمَّد خيضر – بسكرة، اكتوبر2017.
10 - حسين خلف موسى، استراتيجية أمن المعلومات في ظل حروب الجيل السادس، المركز الديمقراطي العربي، سبتمبر 2015.
11 - حسنين رجب عبد الحميد، أمن شبكات المعلومات الإلكترونية: المخاطر والحلول، مجلة Cybrarians Journal، العدد 30، أبو ظبي، ديسمبر 2012.
12 - سامية بوقرة، تطور استخدام تكنولوجيا المعلومات والاتصال والأمن المعلوماتي في المؤسسة، دراسة ميدانية بمؤسسة مطاحن سيبوس، مجلة علوم الانسان والمجتمع، العدد 12، نوفمبر 2014.
13- عارف زمان، المخاطر الناشئة لتقنية المعلومات :تحديات جديدة في انتظار المدققين الداخليين، مجلة المدقق الداخلي الشرق الأوسط، الامارات العربية، ديسمبر 2016.

14- عارف زمان، الحوسبة السحابية، مجلة المدقق الداخلي – الشرق الأوسط، الامارات العربية، مارس 2018.
15- فردي لخضر، اتجاهات المكتبيين نحو استعمال الحوسبة السحابية بالمكتبات الجامعية الجزائرية في ضوء نموذج قبول التكنولوجيا، المجلة العراقية للمعلومات، المجلد الثامن عشر، العددان 1-2، 2017.
16- فيشال ذكار، الدور الحيوي الذي يلعبه التدقيق الداخلي في مجال الأمن الإلكتروني، مجلة المدقق الداخلي – الشرق الأوسط، الامارات العربية، يونيو 2017.
17- فيشال ذكار، ملخص تنفيذي بشأن أعلى المخاطر لعام 2018، مجلة المدقق الداخلي الشرق الأوسط، الامارات العربية، مارس 2018.
18- ليتيم فتيحة، ليتيم نادية، الأمن المعلوماتي للحكومة الإلكترونية و إرهاب القرصنة، مجلة المفكر، العدد الثاني عشر، جامعة بسكرة، 2017.

المراجع باللغة الأجنبية:

Les ouvrages:

19- Henri-Pierre MADERS et autres, les métiers d'auditeur interne et de contrôleur permanent, groupe EYROLLES, Paris, 2015.

Les thèses:

20- Ibrahim Safieddine, Optimisation d'infrastructures de cloud computing sur des green datacenters, Thèse de doctorat, spécialité informatique, université de Gronoble, 2018.

Les articles et les conférences:

21- AMRAE (l'association de management des risques et des assurances de l'entreprise): Organisation de la Maîtrise des risques : 3 lignes de performance du CAC 40 à l'ETI, 21eme rencontre de l'AMRAE du 06 au 08 fevrier 2013, lyon.
22- Arena, A. and G. Azzone, Development trends and future prospects of internal audit, Managerial Auditing Journal, Bradford, Vol.12, Iss. 4/5, 2005.
23- COSO, Le management des risques de l'entreprise : Une démarche intégrée à la stratégie et à la performance, Synthèse, juin 2017.
24 - Hermanson, D, Internal auditing: getting beyond the section 404 implementation crisis, Internal Auditing, Boston, Vol.21, Iss.3, 2006.
25- IFACI, les apports du référentiel COSO ERM 2017, 5eme conférence annuelle de l'IFACI, beffroi de Montrouge, 16.17 novembre 2017.
26-IFACI,trois lignes de maitrise pour une meilleure performance, fiabiliser la stratégie par une gestion organisée des risques, paris, 2013.

Les rapports:

27- The COSO, Enterprise Risk Management-Integrated Framework: Executive Summary, USA, September 2004.
28- IIA, rapport mondial pulse of the profession 2015, Saisir les opportunités dans un monde en perpétuelle évolution, cbok 2015, juillet 2015.

29- IIA, Larry Harrington, Arthur Piper, Réussir dans un monde en mutation: dix impératifs pour l'audit interne, CBOK 2015.

Les sites internet:

30- https://www.iasplus.com/fr-ca/standards/assurance/autres-normes-canadiennes/coso2019s-updated-erm-framework-enterprise-risk-management-integrating-with-strategy-and-performance-2017.

31- https://securityintelligence.com/take-a-load-off-delegate-cyber-risk-management-using-/the-three-lines-of-defense-model.+-0+9 .

32- https://na.theiia.org/translations/PublicDocuments/IPPF-Standards-2017-Arabic.pdf.

33- https://www.protiviti.com/US-en/insights/ protiviti-top-risks-survey

34http://journal.cybrarians.info/index.php?option=com_content&view=article&id=629:networks&catid=257:studies&Itemid=0.