دعم المراجعة الداخلية المبنية على المخاطر بآليات حوكمة تكنولوجيا المعلومات وفقاً لإطار (NIST 800 - 37) للرقابة الداخلية وانعكاسه على تقارير الأجهزة العليا للرقابة

Supporting Risk Based Internal Auditing By Information Technology Mechanisms According To Internal Control Framework (NIST 800-37) And Its Reflection On Superime Oversight Organization Reports

أ.م.د/ مرفت على محمود العادلى

أستاذ المحاسبة المساعد

كلية التجارة - جامعة الأزهر- القاهرة

مستخلص البحث :

هدف البحث إلى تناول مجالات المراجعة الداخلية والتعرف على المرحلة التى تتعلق بحوكمة تكنولوجيا المعلومات ، وذلك على أثر تحول الحكومة بوحداتها الإدارية إلى الحكومة الإلكترونية ، فظهرت العديد من المخاطر من أهمها مخاطر أمن المعلومات مما أثر على نظام الرقابة الداخلية ، فكان من الضروري تطويره بآلية من آليات حوكمة تكنولوجيا المعلومات ، فتم اختيار آلية NIST الصادرة عن المعهد القومي الأمريكي لأمن وخصوصية المعلومات ، بهدف تحقيق جودة لتقرير المراجعة الداخلية المتعلق بتقييم نظام الرقابة الداخلية الذى يرفع للإدارة العليا من خلال لجنة المراجعة بشأن تقييم المخاطر ، بما ينعكس على تقرير الجهاز المركزي للمحاسبات بصفته أحد أهم أجهزة الرقابة العليا فى مصر .

لتحقيق الهدف تم وضع الفروض حول المشكلة ومواجهتها ، تم الاعتماد على المعلومات من خلال جمع وتحليل قائمة استبيان وجهت إلى فئة المراجعين الداخليين ومراجعي الجهاز المركزي للمحاسبات .

تم الوصول إلى العديد من النتائج، أهمها : وجود علاقة معنوية بين كل من حوكمة تكنولوجيا المعلومات و الحوسبة السحابية، بين آلية NIST للرقابة الداخلية والحد

من مخاطر الحوسبة السحابية فى الوحدات المحلية فى مصر ، بين حوكمة تكنولوجيا الحوسبة السحابية وجودة تقرير المراجعة الداخلية ، وبين جودة تقرير المراجعة الداخلية وتحسين تقارير الجهاز المركزي للمحاسبات .

الكلمات المفتاحية :المراجعة الداخلية ، حوكمة تكنولوجيا المعلومات ، آلية NIST Sp800-37 ، مخاطر أمن وخصوصية المعلومات .

Abstract :

The aim of the research is to address the areas of internal auditing and to identify the stage related to the governance of information technology . was due to the transformation of the government with its administrative units into E-government , so many risks emerged , the most important of which were information security risks , which affected the internal control system , so it was necessary to develop it with a mechanism of information technology governance , so the "Nist" mechanism issued by the USA National institute for information security and privacy . to achieve the quality of the internal audit report hat relates to the evaluation of the internal control system that is submitted to senior management through the audit committee on risk assessment which is reflected in the reports of the central auditing organization as one of the most important oversight agencies in Egypt .

to achieve the goal , hypotheses were set about the problem and confronted , information was relied upon by collecting and analyzing a questionnaire list directed to the category of internal auditors.

many results were reached, the most important of which are : the existence of a significant relationship between information technology governance and cloud computing ,between the NIST mechanism for internal control and reducing the risks of cloud computing in local units in EGYPT, between the governance of computing technology and the quality of the internal audit report, between the quality of the internal audit report and the improvement of the reports of the central auditing organization.

Keywords :

Internal audit , information technology governance , NIST Sp800-37, Information security and privacy risk .

مقدمة :

تبنت مصر مجموعة من الإصلاحات الحكومية رغبة فى تحسين التقارير المالية، بالتحول من الأساليب اليدوية والورقية إلى التكنولوجيا من خلال حزمة من البرمجيات التى تخدم أنماط العمل المؤسسي وفقاً لاحتياجاته ومعاملاته المالية والإدارية والاعتماد على نظم تخطيط موارد المنشأة وهو ما يسمى بالحكومة الالكترونية إلا أن هذا التغيير صاحبه العديد من المخاطر منها المخاطر المرتبطة بتكنولوجيا المعلومات . مما دعى إلى تطوير المراجعة الداخلية لتكون قادرة على مراقبة وتحديد وتقييم المخاطر من خلال إدخال تغييرات جوهرية فى بيئة المراجعة الداخلية وإدخال مهام جديدة تتعلق بالجانب التكنولوجي من تقديم تأكيدات موضوعية عن هذه المخاطر .

فلم يعد دور المراجعة الداخلية التحقق من سلامة العلميات الحكومية من الناحية القانونية والمالية (مراجعة الالتزام) فقط، بل أصبح الحصول على أفضل الخدمات بأسرع وقت وأقل جهد وتكلفة مطلباً أساسياً لخدمة العملاء . مما تطلب حوكمة تكنولوجيا المعلومات للحماية من : الهجمات والقرصنة الالكترونية، وعدم القدرة على الدخول إلى البيانات المخزنة، تلف الأجهزة والبيانات نتيجة الكوارث، انقطاع التيار الكهربائي المفاجئ، الأمر الذى يحتم على المراجع الداخلي الحكومي تقديم الضمانات الكافية للتحقق من جودة المعلومات المحاسبية الواردة فى التقارير من خلال إتباع منهج جديد يتوافق مع بيئة الأعمال المعاصرة تناسب طبيعة وأهداف المنشآت الحكومية والأجهزة العليا للرقابة عليها .

ويتم تقسيم البحث إلى الأقسام الآتية :

- المبحث الأول : الإطار العام للبحث .
- المبحث الثاني : المراجعة الداخلية المبنية على المخاطر وحوكمة تكنولوجيا المعلومات
- المبحث الثالث : الإجراءات الرقابية لتأمين الحوسبة السحابية باستخدام آلية (NIST Sp 800 – 37) للرقابة الداخلية فى المؤسسات الحكومية وأثرها على جودة تقارير المراجعة الداخلية .

- المبحث الرابع : أثر تطوير الرقابة الداخلية بآليات حوكمة تكنولوجيا المعلومات على تقارير أجهزة الرقابة العليا فى مصر .
- المبحث الخامس : الدراسة التطبيقية .

المبحث الأول : الإطار العام للبحث

الدراسات السابقة :

يتم تقسيم الدراسات السابقة إلى الآتي :

أولاً : دراسات تتعلق بالمراجعة الداخلية المبنية على المخاطر وحوكمة تكنولوجيا المعلومات

ثانياً : دراسات تتعلق بحوكمة تكنولوجيا المعلومات وآليات الرقابة الداخلية .

ثالثاً : دراسات تتعلق بمدى تأثير دعم المراجعة الداخلية بحوكمة تكنولوجيا المعلومات على تقارير الأجهزة العليا للرقابة .

أولاً : دراسات تتعلق بالمراجعة الداخلية المبنية على المخاطر وحوكمة تكنولوجيا المعلومات :

تناولت دراسة (Kalpesh & Saurabh, 2019) أثر التحول الرقمي على وظيفة المراجعة الداخلية من خلال التركيز على العناصر التى يؤثر فيها التحول الرقمي من العنصر البشري، البيانات، البرامج والتطبيقات (البرمجيات)، وتوصلت إلى أن المؤسسات العامة والخاصة تحتاج لمسايرة التغييرات المحيطة من أجل الاستمرار والبقاء وتحسين جودة الخدمات المقدمة لإرضاء العملاء مع وجود دور فعال لأنشطة المراجعة الداخلية، وكذلك وجود الإدارة الرقمية يساعد المراجعة الداخلية على التطور والوصول لأعلى مستويات الكفاءة والفعالية فى الأداء من خلال تحسين إدارة المخاطر وتحقيق مستوى من الدقة مع خفض أخطاء العنصر البشري .

درس FISHER ، تأثير استخدام تكنولوجيا المعلومات بالمؤسسات الحكومية وكفاءة المراجعة الداخلية، وخلص إلى أن تنوع وزيادة حجم البيانات المتاحة، وهو ما يفرض على المراجع فحص مدى تكامل هذه البيانات ودرجة الدقة والموثوقية والعوامل

المؤثرة فى تأمينها من منطلق دوره فى تقديم تأكيدات موضوعية عنها فى ظل تطبيق إستراتيجية تكنولوجيا المعلومات، وكشفت النتائج عن القدرات الضعيفة للمراجعين الداخليين ومستوى تأهيلهم لفحص أساليب تكنولوجيا المعلومات، وعدم قدرتهم على تقديم تقارير غير تقليدية عن عملية المراجعة تلبى احتياجات أصحاب المصالح . (Fischer, et al., 2020)

تبنت دراسة (Betti and Sarems, 2020) فهم كيفية تطور وظيفة المراجعة الداخلية فى ظل رقمنة الأعمال، وتمت فى بلجيكا، وأظهرت النتائج أن التحول الرقمي يؤثر على وظيفة المراجعة الداخلية فى ثلاث جوانب هى : نطاقها أى من المتوقع أن يزيد تخطيط المراجعة الداخلية وأن تحتل مخاطر تكنولوجيا المعلومات أهمية عالية خاصة تهديدات أمن المعلومات، وأن الطلب على الأنشطة الاستشارية للمراجعين الداخليين يكون مطلوب أكثر، وأن أساليب عمل المراجع الداخلي تتغير وتتطور لتلائم متطلبات المرحلة الجديدة .

عرض معهد المراجعين الداخليين (IIA, 2021) أن الاستثمار التكنولوجي فى المراجعة الداخلية يمكن أن يحقق عائداً مضاعفاً عند القيام به بشكل استراتيجي، وعلى المراجعين الداخليين إثبات أهمية العائد على الاستثمارات فى التكنولوجيا، حيث تعد المهارات والقدرات الخاصة بوظيفة المراجعة الداخلية أحد المحاور الرئيسية فى مجال التحول الرقمي وهى : سرعة الاستجابة (المرونة)، التحليلات السريعة، الترميز والذكاء الرقمي، ..... وغيرها .

تناولت دراسة (Vuko, et al. 2021) تحديد العوامل التى تؤثر على فعالية وظيفة المراجعة الداخلية، وقسمتها إلى **عوامل تنظيمية** : وتتضمن عوامل تتعلق بالقوانين واللوائح المتعلقة بالأمن السيبرانى التى تحتاج المنظمات الامتثال لها، وعوامل تتعلق بالجانب المهني المتمثلة فى المعايير المهنية التى تشكل الخلفية الأكاديمية والتدريب للمراجعين الداخليين وعوامل تتعلق بمحاكاة ممارسات الأمن السيبرانى للمنظمات المهنية المعترف بها وبنجاحها، **وعوامل تتعلق بالوكالة** : وهى تعكس قدرة المراجعة الداخلية فى مواجهة توقعات أصحاب المصلحة والمراجعين الخارجيين . وتشمل دعم مجلس الإدارة لمراجعة الأمن السيبرانى، كفاءات مجلس الإدارة، والتفاعل بين وظيفة

المراجعة الداخلية مع مجلس الإدارة والإدارات التنفيذية مع وضع خطة توكيد يتم فيها تحديد المسئوليات مما يحسن من فعالية عملية مراجعة الأمن السيبرانى وصولاً لمساهمة المراجعة الداخلية فى عمليات الحوكمة وإدارة المخاطر والرقابة .

تبنت دراسة (Betti, et al., 2021) كيفية تعديل أنشطة المراجعة الداخلية لتتوافق مع الحكومة الالكترونية، واختبرت أثر الأنشطة الاستشارية للمراجعة الداخلية واستخدام تحليلات البيانات ودور المراجع الداخلي، وتوصلت الى وجود علاقة إيجابية بين مستوى التحول الرقمي بالمؤسسة واستخدام المراجعين الداخليين لتحليلات البيانات فى أداء مهامها، كذلك هناك تأثير غير مباشر لمستوى التحول الرقمي على تخطيط المراجعة الداخلية .

ثانياً : دراسات تتعلق بحوكمة تكنولوجيا المعلومات وآليات الرقابة الداخلية وأثرهما على مخاطر نظم المعلومات الإلكترونية :

هدفت دراسة البلقاسى إلى تناول إطار COBIT5 كأحد اطر حوكمة تكنولوجيا المعلومات ودوره فى تخفيض فجوة المخاطر فى نظم المعلومات الإلكترونية، وكانت الدراسة ميدانية، وخلصت إلى أن تطبيق مفاهيم حوكمة تكنولوجيا المعلومات تحسن الجودة والكفاءة والفعالية بنظم المعلومات الإلكترونية، بما يترتب عليه من تقليل الفجوة بين التوقع والواقع، وأوصت الدراسة بتبنى المفاهيم الحديثة مزامنة مع تطور تكنولوجيا المعلومات .(البلقاسى ، ٢٠١٨)

تناولت دراسة (Metalia & Sugarmon, 2020) تحديد العوامل المؤثرة فى كفاءة أداء جهاز الرقابة الداخلية للحكومة الاندونيسية . وهذه العوامل هى الدعم الإداري، الكفاءة والموضوعية للموظفين فى هذا الجهاز والنزاهة على أداء الرقابة الداخلية للحكومة، وتوصلت إلى أن هذه العوامل لها تأثير كبير على أداء جهاز الرقابة الداخلية للحكومة الاندونيسية، وأن دور الحكومة فى توجيه المؤسسات الحكومية والإشراف عليها يلزمها بالحفاظ على أدائها وتحسينه . وأوصت بضرورة مشاركة الحكومات فى دعم ووضع سياسات من شأنها تحسين إدارة موظفي الرقابة الداخلية .

بحثت دراسة (Masanja & Mosimba, 2020) فى فعالية نظام الرقابة الداخلية على كفاءة الإدارة المالية فى مؤسسات تدريبية مختارة، وقد طبقت منهج البحث الكمي وكان تصميم البحث وصفياً، وأُجريت فى جامعة أروشا – تنزانيا . وتشير النتائج إلى أن كفاءة الإدارة المالية ترجع لتطبيق أنظمة الرقابة الداخلية المناسبة فى المؤسسات . وأوصت بالمزيد من الجهود والموارد لأنظمة الرقابة الداخلية حيث أنها ضرورية لكفاءة الإدارة المالية .

وتبنت دراسة أخرى لبعض الباحثين تقيم وتحليل واقع آليات حوكمة تقنيات المعلومات وإدارة المخاطر لها، وتحليل العلاقة والتأثير بين آليات حوكمة تقنيات المعلومات وإدارة المخاطر لنظم المعلومات المحاسبية المحوسب . وتمت فى إقليم كردستان (العراق)، وتوصلت إلى نتائج من أهمها : أن آليات حوكمة تكنولوجيا المعلومات له دور فى تفعيل إدارة مخاطر تقنية المعلومات المحاسبية المحوسب، وهناك تأثير بين آليات حوكمة تكنولوجيا المعلومات وإدارة المخاطر، وأوصت بضرورة تبنى المنظمات أطر الرقابة الداخلية المتعلقة فى حماية أنظمة المعلومات المحاسبية المحوسب لحماية امن المعلومات من المخاطر المتعلقة بها . (على، ناكره، ٢٠٢٠)

ثالثاً : الدراسات المتعلقة بتأثير المراجعة الداخلية لحوكمة تكنولوجيا المعلومات على تقارير الأجهزة العليا للرقابة :

تناولت دراسة (Johnsen, et al., 2019) تأثير التغيرات الاقتصادية للأجهزة الرقابية العليا من حيث التفويضات والاستقلال عن مدى فعالية العمليات الحكومية من حيث جودة الحوكمة فى أربع دول هى فنلندا، النرويج، الدنمارك، السويد عام ٢٠١٠، وتم التوصل إلى التأثير الجوهري للأجهزة العليا للرقابة المالية على جودة العمليات الحكومية وفعالية وكفاءة القطاع العام والقابلية للمساءلة .

توصلت دراسة المكصوصى الى العديد من النتائج ، من أهمها : وجود تأثير معنوي موجب للتكامل بين معايير الانتوساى ورقابة حوكمة تكنولوجيا المعلومات على جودة تقارير الأجهزة العليا للرقابة، وكذلك تسعى منظمة الانتوساى من خلال

الأجهزة العليا للرقابة المالية إلى تعزيز رقابة حوكمة تكنولوجيا المعلومات لتحقيق مصداقية وجودة تقاريرها الرقابية . وأوصى الباحث بتوصيات من أهمها : تبني ديوان الرقابة المالية الاتحادي أحدث التقنيات والبرامج فى مجال تكنولوجيا المعلومات لمواكبة التطور السريع فى العالم، والابتعاد عن الأدوات التقليدية فى أساليب الرقابة المالية وكذلك المحاولة بتطبيق التكامل بين معايير الانتوساى ورقابة حوكمة تكنولوجيا المعلومات لجعل قيمة للجهاز الأعلى للرقابة المالية عن طريق رفع مستوى جودة التقارير الرقابية ومواكبة التطور والتقدم فى مجال تكنولوجيا المعلومات . (المكصوصى، ٢٠٢٣)

الفجوة البحثية :

لم تتناول الدراسات السابقة دور المراجعة الداخلية كنشاط فى مساعدة الإدارة العليا فى إدارة المخاطر من خلال دعمها بنظام رقابة داخلية متطور مثل آلية حوكمة تكنولوجيا المعلومات وفقاً لمعايير المعهد الوطني الأميركي NIST 800 - 37 National Institute Standard Technology لحماية امن وخصوصية المعلومات الناتجة من النظم الرقمية للحكومة الإلكترونية وانعكاس ذلك على جودة تقارير الجهاز المركزي للمحاسبات كأحد أهم أجهزة الرقابة العليا فى مصرفى اطار اعتماد مراقب الحسابات على أعمال المراجعة الداخلية . وهذا يكون موضوع هذا البحث .

مشكلة البحث :

اتجه نظر العالم الخارجي إلى أهمية تطوير المراجعة الداخلية، على أثر الانهيارات المالية العالمية للشركات الكبرى فى الفترات السابقة، إلى اعتبارها جزء لا يتجزأ من الإدارة العليا، فظهر منهج المراجعة على أساس المخاطر ليطور أدائها . وينقل تركيزها إلى تقديم ضمانات عن تأمين المخاطر وإدارتها فى حدود المستوى المقبول من قبل مجلس الإدارة، وأيضاً من أن الاستجابات التى اتخذتها الإدارة تعمل بفعالية على تخفيض المخاطر إلى المستوى المقبول، وجاءت المعايير الدولية لممارسة المراجعة الداخلية لتؤكد على ضرورة إعداد خطة المراجعة الداخلية أساس المخاطر (المطيرى، ٢٠١٦)، والتركيز على المجالات والأنشطة الأكثر تعرضاً للمخاطر،

وذلك حتى تواكب التطورات التى لحقت بها فى البيئات العالمية وحتى تتفق مع إصدارات معهد المراجعين الداخليين فى كل من أمريكا وانجلترا . فقد تطلب معيار المراجعة رقم ١٢١٠ أن يكون المراجع الداخلي على دراية تامة بالوسائل التكنولوجية وكيفية استخدامها ومخاطرها حتى يتمكن من أداء عمله بكفاءة وفعالية، كما يتطلب أن يكون لديه مهارات استخدام الوسائل التكنولوجية لتخطيط وأداء مهامها (IIA, 2020)، والمعيار (٢١٠٠) بعنوان : "طبيعة العمل"، على ضرورة قيام وظيفة المراجعة الداخلية بتقييم عمليات الحوكمة واقتراح التوصيات المناسبة لتحسين الحوكمة فى المنشأة، بالإضافة لى ضرورة قيامها بتقييم عمليات إدارة المخاطر، وتقييم مدى كفاية وفعالية الضوابط الرقابية فى التعامل مع المخاطر المتعلقة بالأهداف الإستراتيجية للمنشاة، وموثوقية المعلومات المالية والتشغيلية، كفاءة وفعالية العمليات والبرامج، حماية الأصول، والالتزام بالقوانين والسياسات والعقود . (IIA, 2016)

وأن تكون ادارة المراجعة الداخلية على دراية بأى تطورات أو تغيرات فى الخدمات المقدمة والمعاملات بالمنشأة مما يتطلب معه تأهيل المراجعين لمواجهة أى تحديات، وضرورة إعادة النظر فى إجراءات المراجعة الداخلية فى ظل التحول الرقمي لتشمل أعباء ومسئوليات جديدة تتعلق بجانب الحماية ضد الجرائم الإلكترونية من خلال توفير وفهم الآليات لحوكمة هذه التكنولوجيا الجديدة لتعزيز كفاءة وفعالية نظم الرقابة الداخلية التى لديها القدرة على جعل المنشاة تزدهر أو تتخلف . فعلى سبيل المثال، شركات مثل Black Berry و Kodak تكبد أصحابها خسائر مالية هائلة بسبب فشل الضوابط الداخلية، فى حين تفوقت شركات أخرى مثل Amazon ,Ober بسبب أنظمة الضوابط الداخلية القوية . (Bubilek, 2017)

توصلت دراسة (Bubilek, 2017) إلى أن دور كل من المراجعة الداخلية والرقابة الداخلية هو السماح للمنشأة بتحقيق أهدافها من خلال عمليات تنظيمية أكثر فعالية وإدارة المخاطر وصنع القرار .

نتيجة للمخاطر والتحديات التى صاحبت تطبيق تكنولوجيا المعلومات فى إنتاج معلومات محاسبية ذات جودة عالية وتحقيقاً للشفافية التى أصبحت مطلباً أساسياً

للعملاء بجانب الحصول على الخدمات فى أسرع وقت وبأقل جهد . ظهرت أهمية حوكمة هذه التكنولوجيا لزيادة درجة الثقة فى تلك المعلومات . (Hamdon, 2017)

نظراً للتهديدات التى تحيط أمن المعلومات المحاسبية الالكترونية فى ظل التحول الرقمي وتبني الحكومة هذا التحول (الحكومة الإلكترونية)، فإنها تستثمر جزء كبير من ميزانياتها فى الحد من هذه التهديدات وتأمين أنظمة المعلومات المادية لديها، وإنشاء سياسات أمنية لخلق بيئة من الوعي الأمنى، وفى ضوء محدودية ميزانياتها، فكان من الضروري فحص هذه التهديدات بشكل تفصيلي . (Hwang, et al., 2019)

ذلك لأن القصور فى ممارسات أمن المعلومات والافتقار إلى طرق حمايتها يقود إلى الاحتيال، التلاعب، إساءة استخدام البيانات، وجود صفقات مزيفة، تزوير المعاملات المالية للتهرب من المسائلة القانونية ، ....

(Abu-Musa, 2008; Otero, 2015; Zaydi & Nasser eddine, 2019)

فقد أصدرت المنظمة الدولية للشرطة الجنائية التقرير على أنه من المتوقع أن تصل الأضرار الناجمة عن جرائم الإنترنت إلى ما يقدر بنحو ١٠٥ تريليون دولار بحلول عام ٢٠٢٥ وفقاً لتقدير Edsurge (خدمات التعاون فى مكافحة الجريمة السيبرانية. https://www.interpol.int/ar14/616) ، و أصدر المنتدى الاقتصادي العالمي Word Economic Forum (WEF) بعض التوصيات فى مجال الحكومة الإلكترونية مثل / استخدام تحليل البيانات وتعزيز استقلالية أقسام المراجعة ونظم الرقابة وكذلك قدرتها على تحقيق النزاهة وتحسين إجراءاتها وضمان الالتزام بإجراءات الضبط والمراقبة . (WEF, 2020)

أما عن الوضع فى مصر فقد تبنت الإستراتيجية الوطنية لمكافحة الفساد ،التحول الرقمي واعتماد تكنولوجيا المعلومات والاتصالات كأداتين هامتين لمكافحة الفساد، وتشمل بعض الأهداف ضمن إستراتيجية 2022 - 2019 إنشاء آلية الدفع الإلكتروني للخدمات الحكومية وأتمتة تقديم الخدمات، وتعزيز تدفق البيانات الرقمية

بين الهيئات الحكومية، وتبني برنامجاً لبناء قدرات الموظفين يهدف إلى نشر وتعزيز ثقافة مكافحة الفساد من خلال التركيز على أهمية ودور تكنولوجيا المعلومات والاتصالات فى الوظائف والمهام لمنع الممارسات الفاسدة وزيادة الكفاءة (ACA, 2019) .

إلا أنه مع تزايد ممارسات الاحتيال والفساد المالي زادت المطالبات بتطبيق معايير أجهزة الرقابة العليا وتحقيق مستوى عالي من رقابة حوكمة تكنولوجيا المعلومات، وزيادة التعليم لمواجهة التطور السريع لأنظمة المعلومات، وذلك لتحسين وتفعيل التقارير الصادرة من هذه الجهات عن الوحدات الحكومية .

بالاضافة الى أثر أحكام قانون الخدمة المدنية فى مادته الأولي باستحداث تقسيمات تنظيمية فى وحدات الجهاز الإداري للدولة ومنها المراجعة الداخلية، وفى المادة الثانية يصدر رئيس الجهاز المركزي للتنظيم والادارة القرارات واتخاذ الإجراءات لتعديل الهيكل التنظيمي للوحدات الإدارية بما يتفق وأحكام هذا القرار لعام ٢٠١٩، وأشار فى مادته الأولي " على كل وزارة أو مصلحة أو جهاز حكومي أو حدة محلية أن تتخذ الإجراءات اللازمة لتطوير أو استحداث تقسيم تنظيمي للمراجعة الداخلية فى هيكلها التنظيمي يتبع السلطة المختصة ويتعاون فنياً مع هيئة الرقابة الإدارية" . ويهدف هذا التقسيم التنظيمي للمراجعة الداخلية بجانب أنشطتها التقليدية تقديم الملاحظات والتوصيات إلى السلطة المختصة لتطوير وتحسين مختلف شئون الوحدة، دعم مبادئ الحوكمة، وتطبيق معايير المراجعة الداخلية . وتتوافق هذه الأهداف مع المراجعة الداخلية فى التجارب الدولية فيما عدا إهمال الإشارة إلى دورها فى إدارة المخاطر وتقييم الرقابة الداخلية . (وهدان، ٢٠٢٢)

فى ضوء ما سبق ترى الباحثة انه يمكن تلخيص هذه المشكلة الى أنه فى ظل الحكومة الالكترونية وباعتبار المراجعة الداخلية أحد أعمدة نظم الرقابة الداخلية وعين الإدارة العليا للمؤسسة وأذن المراجعة الخارجية فى دورها فى إدارة المخاطر وتحديدها

وتقييمها . فهل تحتاج إلى دعم نظم الرقابة الداخلية بآليات حوكمة تكنولوجيا المعلومات باستخدام إصدار المعهد الوطني الأمريكي . (NIST, 2018) لتحقيق الأمن والخصوصية والثقة فى المعلومات المحاسبية المنتجة بواسطة تكنولوجيا المعلومات ؟ وهل ينعكس دورها الجديد على جودة تقارير الأجهزة العليا للرقابة فى مصر وخاصة رقابة الجهاز المركزي للمحاسبات ؟

أهمية البحث :

تنقسم أهمية البحث الى الآتى:

الأهمية العلمية :يستمد البحث أهميته العملية من أهمية المكانة التى تحظي بها حوكمة تكنولوجيا المعلومات وقدرتها على تحقيق الأمن والسرية والخصوصية للمعلومات الحكومية التى تتصف بأنها عمومية، وذلك لتحقيق قدر كبير من الشفافية وحماية حقوق أصحاب المصالح . وكذلك من اهتمام المنظمات العلمية بإصدار المعايير والإرشادات التى تساهم فى تطوير المراجعة الداخلية بشأن تقييم المخاطر (بما فيها المخاطر التكنولوجية) للأدوات المستحدثة فيها (الحوسبة السحابية وغيرها ....) وتقييم نظم الرقابة الداخلية وحوكمة تكنولوجيا المعلومات المتعلقة بهذه الرقابة الداخلية من اجل مكافحة الاحتيال والتلاعب والفساد الذى هو ركيزة عمل الأجهزة العليا للرقابة على هذه المؤسسات العامة .

الأهمية العملية :تنبع الأهمية العملية من توفير آلية مثل آلية NIST ودراستها لمدي توافقها مع حوكمة تكنولوجيا المعلومات الخاصة بالحوسبة السحابية فى المؤسسات الحكومية لدعم الأمن والخصوصية للمعلومات الناتجة فى التقارير التى ترفعها إدارة المراجعة الداخلية للادارة العليا من خلال لجنة المراجعة، وانعكاس تأثير تلك التقارير وجودتها على جودة تقارير الأجهزة العليا للرقابة فى مصر .

منهج البحث :

يتبع منهجية البحث التقسيم الآتي :

المنهج النظري : تم الإطلاع على المصادر الأولية من خلال الدوريات العلمية والرسائل والأبحاث السابقة المرتبطة بموضوع البحث، وما نشر على الانترنت، ....

المنهج العلمي : تم تصميم قائمة استبيان تضم محاور تغطى أهداف البحث ويمكن بها اختبار فروض البحث، وتم توجيهها إلى المراجعين الداخليين فى الوحدات المحلية الحكومية فى مصر، ومراجعي الجهاز المركزي للمحاسبات لمعرفة مدى تأثير دور المراجعة الداخلية فى تحسين جودة تقاريرهم عن هذه الوحدات .

أهداف البحث :

يهدف هذا البحث إلى تحقيق الآتي :

١) إبراز العلاقة بين المراجعة الداخلية بمجالاتها ومراحلها وحوكمة تكنولوجيا المعلومات .

٢) دراسة آلية NIST الصادرة عن المعهد القومي الأمريكي للمعايير والتكنولوجيا، لإمكانية استخدامها كآلية رقابة داخلية لحوكمة أمن وخصوصية المعلومات من اجل جودة التقارير .

٣) اختبار آلية حوكمة تكنولوجيا المعلومات للرقابة الداخلية من وجهة نظر هاتين الفئتين : المراجعين الداخليين، أعضاء الجهاز المركزي للمحاسبات المصري لتحقيق أمن وخصوصية المعلومات فى المؤسسات الحكومية المصرية .

٤) توضيح دور تقارير المراجعة الداخلية بعد دعمها بحوكمة تكنولوجيا المعلومات بآلية NIST للرقابة الداخلية فى تقييم نظم الرقابة الداخلية (الحوكمة، المخاطر) فى تحسين جودة تقارير الأجهزة العليا للرقابة (الجهاز المركزي للمحاسبات المصري)

نطاق البحث :

- يقتصر التطبيق على الوحدات المحلية التابعة للجهاز الإداري للدولة المصرية، باعتبارها أحد المؤسسات العامة .
- يقتصر تناول الحوسبة السحابية كأحد نظم تكنولوجيا المعلومات المستحدثة باعتبارها كمخزن ومعالجة وتحليل وتقييم للمعلومات وإمكانية استرجاعها من خلال المؤسسات (العملاء) بأقل تكلفة، ولمزاياها المتعددة، بجانب أنها وسيلة من وسائل التحول للحكومة الإلكترونية .

فروض البحث :

فى ضوء مشكلة البحث وأهميته وأهدافه وحدوده، يتم اشتقاق الفروض الآتية :

١) توجد علاقة معنوية ذات دلالة إحصائية بين المراجعة الداخلية وحوكمة تكنولوجيا المعلومات .

٢) توجد علاقة معنوية ذات دلالة إحصائية بين آلية NIST للرقابة الداخلية ومخاطر الحوسبة السحابية فى الوحدات المحلية .

٣) توجد علاقة معنوية ذات دلالة إحصائية بين حوكمة تكنولوجيا الحوسبة السحابية وفقاً لإطار NIST وجودة المراجعة الداخلية فى الوحدات المحلية .

٤) توجد علاقة معنوية ذات دلالة إحصائية بين جودة المراجعة الداخلية وتحسين تقارير الجهاز المركزي للمحاسبات .

هيكل البحث أو المحتويات :

المبحث الأول : الإطار العام للبحث .

المبحث الثاني : المراجعة الداخلية المبنية على المخاطر و حوكمة تكنولوجيا المعلومات .

المبحث الثالث : الإجراءات الرقابية لتأمين الحوسبة السحابية باستخدام آلية NIST للرقابة الداخلية فى المؤسسات الحكومية وأثرها على جودة تقارير المراجعة الداخلية.

المبحث الرابع : أثر تطوير الرقابة الداخلية بآليات حوكمة تكنولوجيا المعلومات على تقارير أجهزة الرقابة العليا فى مصر .

المبحث الخامس : الدراسة التطبيقية .

النتائج والتوصيات والرؤية المستقبلية .

المراجع العربية والأجنبية .

المبحث الثاني : المراجعة الداخلية المبنية على المخاطر وحوكمة تكنولوجيا المعلومات

تمهيد :

تعد أنشطة إدارة المخاطر بالمنشأة مسئولية تضامنية بين إدارة المراجعة الداخلية ومجلس الإدارة ، فمهمة مجلس الإدارة أداء جميع الأنشطة التى من شأنها تحقيق إدارة شاملة المخاطر من تحديد وتقييم المخاطر ، بينما وظيفة المراجعة الداخلية هي تقديم أنشطة استشارية لمساعدة الإدارة فى تفعيل إدارة المخاطر ، وأخرى تأكيدية تتمثل فى توفير تأكيد معقول حول موثوقية وملائمة المعلومات ونظم الرقابة الداخلية بشأن المخاطر من خلال تقرير يقدم إلى لجنة المراجعة ومنها إلى مجلس الإدارة . ولهذا فهي تساعد مجلس الإدارة فى رسم السياسة العامة لإدارة المخاطر ، وذلك بتقديم خدمات استشارية واقتراحات ، التحقق من مدى التقيد بالأنظمة والإجراءات الواردة فى السياسة العامة لإدارة المخاطر ، تقييم مدى كفاية وفعالية أنظمة التعرف على المخاطر وأنظمة القياس المتبعة على مستوى كل الأنشطة والعمليات بالمؤسسة ، وتقييم التقارير المعدة من طرف مدير المخاطر حول تطبيق الإطار العام لإدارة المخاطر وسرعة الإبلاغ بمعالجتها وتقييم مدى كفاية وفعالية أنظمة الضبط الداخلي وآليات الرقابة الموضوعة للتحكم فى المخاطر وصحة قياسها .

وعلى أثر اتجاه المؤسسات الحكومية إلى التحول إلى الحكومة الإلكترونية (الاستعانة بأدوات نظم المعلومات والتكنولوجيا) نتيجة للتحول الرقمي فكان لهذا التغيير تأثير على عملية وممارسة المراجعة الداخلية فبالإضافة إلى أنها وظيفة مستقلة تقوم بشكل مستمر بتقييم السياسات والأنظمة المالية والمحاسبة وتراقب مدى الامتثال للضوابط والتعليمات المتعلقة بعمل المؤسسة الحكومية . أصبح لها دور فى كشف التلاعب والأخطاء وتقييم أنظمة التحكم مع تقديم تأكيدات للإدارة بأن أنظمة الرقابة تتوافق مع الخطط الموضوعة ، وحتى تؤدي هذا الدور ظهر الأمن السيبراني الذى يهدد سمعة المؤسسات واستقرارها المالي والتشغيلي .

- مجالات المراجعة الداخلية .
- علاقة المراجعة الداخلية بحوكمة تكنولوجيا المعلومات .

مع تحول الأعمال إلى الرقمنة فتبع ذلك تطوير فى المراجعة الداخلية ليس فقط على نوع المراجعة الداخلية التى يتم إجراؤها وطريقة تقديم التأكيد ، بل على المهارات المطلوبة ومنهجيتها فظهر تقرير عن معهد المراجعين الداخلين (IIA,2019) عن ضرورة مراعاة ثلاث محاور لتطوير خطة المراجعة الداخلية داخل المؤسسة الرقمية (الحكومية أو غير الحكومية) وهم : التعاون والاتصال والتواصل :

- التعاون بين المراجعة الداخلية وشركاء خارجين على أثر استبدال أنظمة الملفات بأنظمة المشاركة المستندة إلى السحابة (الحوسبة السحابية) مما يتطلب رقابة قوية من خلال حوكمة البيانات وكذلك إمكانية الاعتماد على منصات الطرف الثالث (المزود بالخدمة) ، غياب أصحاب المصلحة وانعدام المساءلة ، نشر معلومات خاطئة غير خاضعة للرقابة وقد لا يكون مصدر المعلومات معروفاً ، وبالتالي فهم المخاطر لإدارة المراجعة الداخلية وضياع القرار يصبح أمراً صعباً
- الاتصال فتشمل مجالات المراجعة ما يلي : الوصول إلى البيانات غير المؤسسة تكون أسرع وتمتاز بالزيادة مما يؤثر فى الوضع الأمني السيبراني

وخصوصية البيانات سواء للجهات الخارجية (أصحاب المصالح) أو الداخلية مما يهدد سمعة المؤسسة ونتائج أعمالها ، الخطأ البشري ، حوسبة المستخدم النهائي .

- التواصل : يجب أن تعكس خطة المراجعة الداخلية أهمية التواصل ، فيراعي فيها الفورية ، ودعم الموظفين بمجالات الاتصالات الداخلية والخارجية ، العملاء من أجل إدارة العلامات التجارية ومعالجة الشكاوي وتطوير المنتجات .

فى تقرير معهد المراجعين الداخليين للتحديات التى تواجهها المراجعة الداخلية قبل عام من جائحة Covid -19 وبعد عام لخص التحديات فى الآتي (IIA,2020) : تحديد وتقييم المخاطر الجديدة، التعاون عن بعد مع أصحاب المصلحة فى المراجعة، التواصل والمتابعة مع أصحاب الأعمال، إضاعة الوقت والموارد فى المهام اليدوية والإدارية . وكاستجابة لهذه التحديات فإن الأمر يستدعى انتقال المراجعة الداخلية إلى استخدام التكنولوجيا القائمة على السحابة (الحوسبة الحسابية : تحليلات البيانات الضخمة،....) بما توفره من مزايا فى إمكانيات الوصول إلى المستندات فى أي وقت ومن أي مكان وبأقل تكلفة. إلا أنه طبقاً لدراسة (pwc,2019) فإن المخاطر التى تواجه المؤسسة عند التغير (التحول الرقمي) تتمثل فى الآتي :- الاضطراب الرقمي بسبب تقنيات منصات الأجهزة المحمولة ، تحليلات البيانات الضخمة ، السحابة ، إنترنت الأشياء تعمل على تعطيل نماذج الأعمال عبر القطاعات، والبيانات الضخمة .- زيادة حجم البيانات وزيادة حجم المعاملات يستدعى حوكمة وإدارة أفضل لها، ومخاطر الأمن والخصوصية .- أعمال القرصنة للملكية والفكرية ، وسرقة بيانات العملاء ، والتجسس الإلكتروني مما يستدعى الحوكمة بآليات مناسبة .

أشار تقرير معهد المراجعين الداخليين (IIA,2021) على المراجعين الداخليين إثبات أهمية العائد على الاستثمارات التكنولوجية لأنها موجودة لجعلهم أكثر كفاءة وفعالية

من خلال سرعة الاستجابة فى تقييم المخاطر ، تحسين إنتاجية فريق المراجعة والتواصل ، التعاون بين المؤسسة وتزويدها بتغطية أوسع ، رؤية أفضل لحالة واتجاهات المخاطر والتوكيدات ، زيادة الملكية والمساءلة عن الرقابة ، تحسين إمكانية الوصول لتمكين القوى العاملة الموزعة ، توفر الوقت والتكلفة .

معايير المراجعة الداخلية فى ظل التحول الرقمي :

صدر عن معهد المراجعين الداخليين من رئيسه التنفيذي بعض الفقرات من معايير المراجعة الداخلية ذات الصلة بالتحول الرقمي (Chambers,2017) :

معيار 2010 "التخطيط" : تطوير الخطة القائمة على المخاطر وتعديلها حسب الضرورة كاستجابة للتغيرات فى أعمال المؤسسة والمخاطر والعمليات والبرامج والأنظمة والضوابط . معيار 2130 "الرقابة" : دور المراجعة الداخلية فى الحفاظ على ضوابط رقابية من خلال تقييم كفاءة وفعالية المؤسسة والدفع نحو التحسين المستمر . معيار 1210 "المهارات" : على المراجعين الداخليين امتلاك كل من المهارة (القدرة على استخدام المعرفة) ، الفهم ، اتساع مجالات المعرفة بالعلوم المتعلقة بالتكنولوجيا الجديدة وتخصصهم .

مجالات المراجعة الداخلية للنظم التكنولوجية وآليات التحول الرقمي :

حدد أحد الباحثين (شحاته ، ٢٠٢٠) مراحل المراجعة الداخلية للنظم التكنولوجية فى الآتي :

المرحلة	مجالاتها
١) الأساسية :	فحص ضوابط تقنية المعلومات ، تقييم مخاطر تقنية المعلومات ، التحقق من سلامة أمن المؤسسة ، رقابة تخطيط موارد المؤسسة فصل الواجبات ، مراجعة العمليات التشغيلية وعمليات تحويل نظام المراجعات المسبقة ، إدارة استمرارية الأعمال وخطط مواجهة الأزمات والكوارث .
٢) المتقدمة :	حوكمة تكنولوجيا المعلومات ، حوكمة تخطيط موارد المؤسسة ، تقييم المخاطر ، فحص الامتثال ، أمن تطوير التطبيقات ، إدارة الثغرات الأمنية ، أمن التطبيقات ، إدارة أصول البرمجيات ، شفافية قواعد البيانات وتكاملها ، والاستعانة بمصادر خارجية لتكنولوجيا المعلومات ، وإدارة مخاطر الجهات الخارجية ، تحليل بيانات المراجعة الداخلية ، تقييم التقارير الذكية .
٣) الحوسبة السحابية :	التحقيق من سلامة التواصل الاجتماعي ، تقييم إدارة مخاطر تكنولوجيا المعلومات ، فحص ضوابط الأمن عبر الهاتف المحمول ، وتقييم مخاطر خصوصية البيانات ونظم الحماية ، وتقييم مخاطر الإنترنت ، وتحليل المشاريع التنبؤية ، مراجعة وتقييم المنصات الرقمية ، مراجعة تكنولوجيا المعلومات والنظم الرقمية المستدامة .

المراجعة الداخلية وعلاقتها بحوكمة تكنولوجيا المعلومات :

حوكمة تكنولوجيا المعلومات التى عرفها أحد الباحثين (سليمان،٢٠١٩) بأنها مجموعة من الأطر التنظيمية والعمليات التى تؤكد أن تكنولوجيا المعلومات تعمل على تدعيم الأهداف الإستراتيجية للمؤسسة ، وتتأكد من تحقق الاستثمارات التكنولوجية فيها بشكل جديد للاستفادة من القيمة التى تضيفها ، وفى نفس الوقت الرقابة والوقاية من المخاطر . وتعتبر حوكمة تكنولوجيا المعلومات عين الرقابة على أنشطة وأعمال تكنولوجيا المعلومات ، والتأكد من سيرها بالاتجاه الصحيح من خلال تحقيق التناسق بينها والتوافق المطلوب ، وذلك من خلال توفير آليات تحد من هذه المخاطر باستخدام أحكام الرقابة السليمة . وتعد الرقابة الداخلية من أهم وسائل كشف الانحرافات ، حيث أنها تتمثل فى مجموعة من الإجراءات والوسائل المتبعة فى تنفيذ العملية الرقابية داخل المؤسسات بمختلف خصائصها .

أما الانتوساى فأضافت لأهداف الرقابة الداخلية ما يلي : حماية الموارد من الخسارة والتلف وسوء الاستخدام ، توفير معلومات تتصف بالدقة لتحقيق أهداف التقرير المحاسبي ، وخاصة تحقيق المساءلة، الالتزام بالنظم والقوانين والسياسات والتعليمات السارية .(الانتوساى،٢٠١٤)

قدمت منظمة التعاون الاقتصادي والتنمية (OECD) إطار الرقابة الداخلية ، وحددت دور المراجعين الداخليين فى قياس مدى فعالية ترتيبات الرقابة الداخلية كجزء من مهامهم ، ويتمثل دورهم فى تقييم ما إذا كانت المكونات المختلفة لنظام الرقابة الداخلية (بيئة الرقابة فى المخاطر ، أنشطة الرقابة ، المتابعة والرصد) موجودة ومطبقة ووضع ضوابط كافية وفعالة ، وتقديم توصيات بشأن تطوير أوجه القصور والتداخل والثغرات فيها . قدمت لجنة تريدواي Treadway نموذج لخطوط الدفاع الثلاثة فى إدارة المخاطر والتحكم فيها بصورة فعالة كما يلي :

- الخط الأول : تقوم الإدارة التشغيلية بتدابير الإدارة والرقابة الداخلية المصممة من خلال النظم والعمليات (أصحاب الأعمال والعمليات التى تحدد أنشطتهم المخاطر التى قد تسهل أو تعيق تحقيق أهداف المؤسسة وتقييمها ورصدها) .

- الخط الثاني : يرصد الحوكمة والمخاطر والامتثال ، كما أنه يعد بمثابة وظيفة الإدارة والرقابة ، ويكون منفصل عن الخط الأول ولكن يتمثل دوره الأساسي فى إضافة الخبرة أثناء دعم أنشطة خط الدفاع الأول .
- الخط الثالث : يتمثل فى المراجعة الداخلية ، حيث أنه يعني بتقديم ضمانات مباشرة للمسئولية والإدارة العليا حول جهود الحوكمة وإدارة المخاطر والرقابة GRC (Governance - Risk - Control) فيما يخص الخط الأول والثاني ، ولهذا كان من الضروري ضمان موضوعية واستقلالية الخط الثالث لأداء مهامها بكفاءة وفعالية (لجنة المنظمات الراعية للجنة تريدواي ،OECD ، ٢٠١٩)

ترى الباحثة أنه مع تزايد أهمية وظيفة الرقابة الداخلية داخل المؤسسات الحكومية لدعمها لإدارة المال العام وتحقيق الشفافية والمساءلة ، وقدرتها على توفير توصيات مفيدة تساعد الإدارة فى الوفاء بمسئولياتها من خلال تخطيط أعمال المراجعة فإن فعاليتها تعتمد بشكل أساسي على دورها فى تقييم وتحسين عمليات إدارة المخاطر ونظم الرقابة والحوكمة .

تمر حوكمة تكنولوجيا المعلومات بالخطوات الآتية : (جودي،٢٠١٢) .

المواءمة بين الإستراتيجية العامة للمؤسسة وخطط التشغيل اللازمة لتحقيق الأهداف (التخطيط الاستراتيجي لتكنولوجيا المعلومات) . وضع خطة تشغيل ، وضع خطة مالية وتمويلية لتقنية المعلومة . وضع إطار عام لحوكمتها والرقابة عليها معتمداً على ما تصدره جهات الرقابة والإشراف والتشريعات المنظمة للعمل بالمؤسسات واختيار البدائل المطروحة . مشاركة مسئول إدارة تكنولوجيا المعلومات فى إستراتيجية الوحدة . ممارسة الالتزام ، ومساءلة ومحاسبة المسئولين عن الانحراف .

تم تقديم معايير الإيزو (ISO) لتوفير مبادئ توجيهية ومهارات لإدارة مخاطر أمن المعلومات بالإضافة إلى اختيار وتنفيذ وإدارة الضوابط الأمنية التى من خلالها يتم الحد من المخاطر التى تتعرض لها التقارير المالية الإلكترونية .

من ثم تحقيق خصائص جودة المعلومات المحاسبية التى من خلال توافرها يتم الحكم على جودة التقارير المالية ، كما تقوم معايير الإيزو بتعزيز الجهود والضوابط الأمنية

للحفاظ على نظام أمن المعلومات من خلال تحقيق مثلث أمن المعلومات المتمثل فى : السرية والموثوقية ، والتكاملية وسلامة المحتوى ، وتوفير المعلومات فى الوقت المناسب (Haren,2018/2019) .

فعلى سبيل المثال يتضمن أمن تكنولوجيا المعلومات مجموعة من السياسات والإجراءات الواجب الالتزام بها لتقليل احتمال حدوث انحراف أو خسائر ، وتقليل آثارهما فى حال حدوثهما ، وتتمثل تلك الضوابط على أمن وسلامة المعلومات وفقاً لمعيار ISO ١٧٩٩ فيما يلي : (المري،٢٠٢٣) : تحقيق أمن الأفراد ، وتخفيض الأخطار المرتبطة بخطأ بشري ، ويتطلب تعريفهم بالأخطار المختلفة . اعتماد برامج تمنع إقفال الدفاتر والسجلات والخروج منها فى حال وجود خطأ . التخطيط لاستمرار أنشطة المؤسسة بمنع أو تخفيف حدة الأعطال والأضرار التى قد تصيب أنشطة وعمليات المؤسسة عند وقوع أحداث تضر بأمن أنظمة المعلومات . وجود رقابة على الدخول إلى معلومات النظام ، حيث يتم تحديد الأنشطة والمسئوليات التى يقوم بها كل المستخدمين للنظام ثم يتم تحديد المعلومات والخدمات التى يسمح لكل مستخدم بالوصول إليها . تأمين مصادر الطاقة للحماية من أي انقطاع التيار الكهربائي . وجود صيانة وتطوير مستمرين للنظام ومكوناته والتوصل إلى متطلبات الأمن الواجب توافرها فى هذه الأنظمة . استعمال برامج الكشف عن الفيروسات وتحديثها ، وعدم فتح أي ملفات والتأكد من خلوها من أي فيروسات تضر بالبيئة . الالتزام بالقيود القانونية والتنظيمية والتعاقدية ، ومراعاة التشريعات والقوانين الدول المختلفة عند تبادل البيانات والمعلومات فيما بينها .

تناول (العبيدي،٢٠١٩) مبررات تطبيق حوكمة تكنولوجيا المعلومات التى تدفع المؤسسات للتعامل مع أمن المعلومات بصورة جدية فى الآتي : الاعتماد التام والمتزايد على نظم المعلومات والاتصال (لضمان السلامة والنزاهة أي أن تكون المعلومات محمية ومصونة وبعيدة عن أيدي العابثين) . قيمة المعلومات الإستراتيجية (دعم المستلزمات الفنية والبشرية والقيادية وإدراك أهمية استدامتها وحمايتها من المخاطر المختلفة) . تزايد قيمة الاستثمارات فى التقنيات . الخسائر الناتجة عن توقف المنظومة المعلوماتية .

حدد الباحثان (Grem Bergen & haes,2019) أبعاد حوكمة تكنولوجيا المعلومات فى الآتي، البعد الأول : مواءمة تكنولوجيا المعلومات مع أنشطة الأعمال . البعد الثاني : عمليات حوكمة تكنولوجيا المعلومات . البعد الثالث : مقاييس أو مخرجات تكنولوجيا المعلومات .

تخلص الباحثة مما سبق بأن حوكمة تكنولوجيا المعلومات محركاً من محركات نجاح أي مؤسسة بما تضيفه من قيمة لأعمالها على المستوى التشغيلي وأيضاً على المستوى الاستراتيجي لأنها تضمن الاستدامة للمؤسسة فى المدى الطويل (السمعة الحسنة) وأن أمن المعلومات وإدارتها إحدى مهام حوكمة تكنولوجيا المعلومات فأن ما يسري على حوكمة تكنولوجيا المعلومات أولى بالتطبيق على حوكمة أمن هذه المعلومات .

هذا ما دعى بالباحثة إلى البحث عن آلية لتحقيق أمن المعلومات من أجل تحقيق حوكمة رشيدة وقوية لتكنولوجيا المعلومات .هذه الآلية المقترحة هي NIST الصادرة المعهد الوطني الأمريكي للمعايير والتكنولوجيا (NTST) Cyberian Security Frame (CSF) سيتم تناولها فى جزء لاحق لهذا البحث .

لأن حوكمة تكنولوجيا المعلومات تهتم ببناء تكنولوجيا المعلومات للمؤسسات والرقابة عليها كلياً وتفصيلياً ، فهي إطار عام يحدد سلطة إيجاد القرار ، وتحديد المسئولية بهدف البحث على السلوك المرغوب فيه عند استخدام أدوات تكنولوجيا المعلومات .

أفاد معهد حوكمة تكنولوجيا المعلومات (ITGI) بأن حوكمة تكنولوجيا المعلومات يغطي خمس مجالات وهي المواءمة مع استراتيجيات الأعمال ، قياس الأداء ، إدارة الموارد ، إدارة المخاطر ، إضافة قيمة للمؤسسة .

تناولت دراسات كل من (عطية،٢٠٢١ ، شحاته،٢٠٢٠، Kahyaglu&Calturt,2018) دور المراجع الداخلي فى تحسين أنظمة إدارة المخاطر والرقابة الداخلية ، وألقت الضوء على وضع ضوابط رقابية لضمان الأمن السيبراني لحماية المؤسسات من الجرائم الإلكترونية .

المبحث الثالث : الإجراءات الرقابية لتأمين الحوسبة السحابية باستخدام آلية NIST فى المؤسسات الحكومية وأثرها على جودة تقارير المراجعة الداخلية

تتنوع أدوات تكنولوجيا المعلومات التى يعتمد عليها التحول الرقمي للمؤسسات ، والتى من أهمها ، الحوسبة السحابية – البيانات الضخمة – سلاسل الكتل – الروبتات – أدوات الذكاء الاصطناعي . وتتمتع هذه الأدوات بالعديد من المزايا والقبول من قبل مستخدميها أهمها : إمكانية تخزين قدر أكبر من المعلومات ، سهولة الوصول للمعلومات فى أي وقت ومن أي مكان ، أقل تكلفة، إلا أنه على الرغم من مزاياها العديدة فهى تتعرض لتحديات أو مخاطر تتمثل فى الآتي : مخاطر فقد المعلومات فى حالة حدوث تلف للأجهزة ، أو تعمد من أحد المستخدمين، مخاطر الخصوصية ، سرقة بيانات العملاء (Nambisan etal.,2019) والتى تمثل خطر يهدد نظم تشغيل المؤسسات وتحتاج لتأمين البيانات وحمايتها من القرصنة والاختراق ، وغيرهم من الجرائم الإلكترونية مما يتطلب حوكمتها .

ترى الباحثة اختيار الحوسبة السحابية والتركيز فى إدارة مخاطرها وحوكمتها من أجل الحفاظ على أمن وخصوصية والدقة والموثوقية فى المعلومات بما ينعكس فى تقارير المراجعة ، باعتبارها تمثل إحدى التقنيات الحديثة لتكنولوجيا التحول الرقمي ، وأنها ثالث مراحل التحول الرقمي المناظرة لأحدث مجالات التطوير فى المراجعة الداخلية ، وعلى اعتبار أن المخاطر الأمنية لها تمثل أهم مصدر قلق، حيث يتم تخزين بيانات المؤسسة المستخدمة فى يبوفر بعيد ، وإن ذلك يثير بعض المخاوف بشأن الخصوصية والسرية ، حيث يمر تحويل البيانات أثناء التشغيل السحابي عبر الإنترنت .

لهذا يتم تناول الموضوعات الآتية :

- الحوسبة السحابية وعلاقاتها بالرقابة الداخلية.
- آلية NIST للرقابة الداخلية ودورها فى حوكمة تكنولوجيا الحوسبة السحابية، المراجعة الداخلية وتوكيدها لمخاطر الأمن السيبراني فى المؤسسات الحكومية .

الحوسبة السحابية وعلاقتها بالرقابة الداخلية :

تناولت دراسة (علي وآخرون ، ٢٠٢٣) أن للحوسبة أثر هام على هيكل الرقابة الداخلية لأنها تمكن من مزامنة الملفات ومشاركتها على المستودعات السحابية ، والاحتفاظ بنسخة احتياطية منها فهي بذلك يمكن أن تخفض التكاليف الرأسمالية وكذلك تمكن من الوصول إلى التكنولوجيا المستخدمة من قبل المؤسسات الأخرى ، وتحسين التنظيم الداخلي وإدارة التقلبات بشكل استراتيجي ، وتطبيق مبدأ المساءلة ، وتوفر تقييم ومتابعة الأنشطة الرقابية بانتظام إلا أنها مع هذه المزايا تواجه عدد من التحديات والمخاطر تتمثل فى بطء شبكة الإنترنت أو تعطيلها ، ضعف الاتصال بين قواعد بيانات المؤسسة وتطبيقات الحوسبة ، نقص فى البنية التحتية للمؤسسات ، مخاطر متعلقة بالتهديدات الأمنية (الأمان والخصوصية للبيانات ، الاختراقات ، الهجمات الفيروسية ، فقد أو ضياع وعدم إمكانية استرجاع البيانات ، انتهاك حقوق الملكية الفكرية ، فقدان السيطرة على الملفات لأنها تحت سيطرة مزود الخدمة الذى قد يتسم بعدم النزاهة ، عدم توافر الاتفاقيات القانونية الملزمة للأطراف المتعاملة ، عدم توفير معايير محاسبية تحمي خصوصية وأمن المعلومات ، مخاطر نقص الخبرة والمهارة فى المتعاملين بالخدمة عند رفع البيانات والمعلومات المحاسبية وتحليلها) .

قد رصد تقرير منظمة أمنية للسحابة (Cloud security Alliance (CSA),2011)) التهديدات المرصودة للحوسبة السحابية والتى تتمثل فى : إساءة الاستعمال ، واجهات التطبيقات غير آمنه ، فقد أو تسرب البيانات ، الاستيلاء على البيانات أو الخدمة ، قضايا التكنولوجيا المشتركة ، الفيروسات .

تتميز المخاطر المرتبطة بالأدوات التكنولوجية بالخصائص الآتية : زيادة تأثير المخاطر الكامنة ، أي أنه فى حالة حدوث أي أخطاء أو تلاعب فى أي عملية فإن الخطأ يمتد إلى كل معاملة فى العملية، زيادة سرعة المخاطرة وبالتالي سرعة الخسائر المادية، إذا كان من الممكن الاستعانة بطرف ثالث للحصول على تلك الأدوات فى إنجاز المهام ، فإنه يكون من الصعب الاستعانة بأي طرف ثالث لمعالجة المخاطر خاصة فى حالة عدم توافر الموارد الذاتية للحصول عليه، من المخاطر المرتبطة بالحوسبة السحابية مخاطر نقص الخبرة والمهارة والمعرفة لفريق العمل ومخاطر عدم تدريب المستخدمين على التعامل عند رفع البيانات لتحليلها، لذلك تعد هذه المخاطر تبريراً لحوكمة هذه التكنولوجيا ، وخاصة فى المؤسسات الحكومية عن غيرها من المؤسسات الخاصة بأن بياناتها أكثر سرية لأنها ذات طابع عمومي .

عندما تواكب هذه المؤسسات تطبيق هذه التكنولوجيا عند انتقالها للحكومة الإلكترونية فإنها توافق متطلبات لحوكمة استخدام هذه التكنولوجيا ، وتتمثل هذه المتطلبات فى الآتي : فوفقاً لتصور أحد الباحثين (مسرحد ، ٢٠١٩) تبني سياسة حكومية للحوسبة السحابية مثل : وضع معايير لمنح التراخيص لمزودي الخدمة ترتكز على توفير الأمن وسلامة البيانات ، وضع شروط للعقود بين الحكومة ومزودي الخدمة ، عمل شراكة تجمع بين خبراء تكنولوجيا المعلومات المؤسسات الحكومية لتطوير أمن الحوسبة، اعتماد حوسبة سحابية خاصة (بنية تحتية حكومية للحوسبة من مراكز البيانات والأجهزة والبرمجيات والتطبيقات الخاصة لمعالجة وتبادل ونقل البيانات)، تبني سياسة إعداد وتدريب الموارد البشرية للتعامل مع هذه السحابة .

تهتم نظم المعلومات المحاسبية بجمع وتخزين البيانات المتعلقة بالأنشطة المالية للمؤسسة بكفاءة وفعالية ، وتوفير المعلومات لمتخذي القرار ، والتأكد من وجود الضوابط لتسجيل البيانات ومعالجتها بدقة ، وفى سبيل ذلك تحتاج إلى مقومات تتمثل فى الأشخاص الإجراءات والتعليمات ، البرامج المستخدمة فى معالجة البيانات

، البنية التحتية لتكنولوجيا المعلومات (الماديات التكنولوجية) ، مجموعة الضوابط والإجراءات الأمنية المستخدمة لحماية البيانات .

تأتي مشكلة أمن المعلومات فى السحابة الإلكترونية من مصدرين هما : مزود الخدمة والمستفيد منها. ويقع العبء الأكبر على عاتق مزود الخدمة، فهو ملزم بتوفير أدوات وبنية تحتية ومستودعات خزن البيانات مؤمنة بمقابل مادي، إلا أنه فى الآونة الأخيرة انتشرت الاختراقات الأمنية والهجمات التى تسببت فى عدم الأمان والخصوصية، والثقة فى المعلومات المحاسبية المحوسبة. مما يتطلب إيجاد قواعد تنظيمية لسد الفجوات التأمينية ولتوفير خدمات تقنية مؤمنة تناسب حجم هذه البيانات . وكذلك بالإضافة إلى ضرورة تأكد المؤسسة من مزودي الخدمة وسمعتهم ومقر شركاتهم القانونية (المراجعين الخارجيين لهم) والفروع التابعة لها، وموقع خوادمهم حول العالم، التأكد من توافر الدعم الفني وسهولة الاستخدام، واسترجاع البيانات .

اتفقت دراسة (محمود، رمضان، ٢٠١٧) فى ضرورة الانتقال للحوسبة السحابية لما لها من أهمية بالغة فى ترشيد الإنفاق الحكومي والمحافظة على تحسين وتطوير الأداء الحكومي، إضافة إلى دورها فى مواكبة المتغيرات التكنولوجية، فضلاً عن العمل على إرضاء المواطنين (العملاء) وتلبية احتياجاتهم مما ينمي انتماؤهم للدولة . وكان من أهم توصياتها التأكد من توفير الأمن والحماية للبيانات والمعلومات الحكومية المحولة للسحابة.

تناولت دراسة (مجدوب، زيانى، ٢٠١٨)، حصر أهم المخاطر التى تعترض تطبيق الحوسبة السحابية من خلال الاعتماد على تطبيق مفهوم الأهداف الرقابية ضمن إطار COBIT5 . من خلال سرد مجموعة من التهديدات المرافقة للحوسبة، وتتفق الباحثة مع هذه الدراسة فى ضرورة أن تكون المؤسسات على علم بقضايا كثيرة مثل إجراءات الأمن الداخلي والاتفاقيات الأمنية، الولوج للسحابة وغيره وإلا ستتعرض لهجمات مختلفة تستهدف مستوى البنية التحتية كخدمة IAAS، والبرمجيات كخدمة

SAAS، والمنصة الحاسوبية كخدمة PAAS، وهنا تظهر أهمية حوكمة الحوسبة كدرع وقاية وحماية لكل المتعاملين بهذه التكنولوجيا .

آلية NIST للرقابة الداخلية ودورها فى حوكمة تكنولوجيا الحوسبة السحابية

يتم استخدام هذه الآلية للأسباب الآتية :

- يقع على المؤسسة مسئولية تقييم ورقابة المخاطر التى تنشأ عن استخدام الحوسبة من خلال توفير وسائل فعالة للتحقق مما إذا كانت البنية التحتية والخدمات التى يقدمها مزود الخدمة تلبي احتياجات المؤسسة من حيث تقييم المخاطر وذلك لتطوير استراتيجيات مناسبة لمواجهة هذه المخاطر وذلك لتطوير استراتيجيات مناسبة لمواجهة هذه المخاطر . (Yang, et al., 2016)
- التطورات التى لحقت بالمؤسسات الحكومية نتيجة التحول الرقمي، يتطلب تغيير طرق تصميم البرامج، إدارة الأنظمة وتامين المعلومات، وهذا يحتاج على توفير الخوادم أو تغيير رمز الاختيار، مما يستدعي الإطلاع ودراسة كل ما يقدمه مزودي الخدمة من المنافسين .
- أمن وخصوصية المعلومات فى ظل السحابة يعتمد على كل من مزودي الخدمة والمستفيد (المؤسسة)، فمن الضروري ألا تغفل الآلية دور الطرفين فى الحفاظ على أمن وخصوصية وموثوقية المعلومات .
- مراجعة تكنولوجيا الحوسبة تواجه حالات الفشل والإخفاق من أجل تحسين نوعية وجودة الخدمات السحابية التى تكون عرضة للتهديدات الأمنية سواء الداخلية أو الخارجية (الداخلية : الاختراقات الأمنية "السرقة"، أما الخارجية : بسبب الكوارث الطبيعية كالزلازل والحرائق)، والأخطر أن مزودي الخدمة قد يكونوا عديمي النزاهة ويقوموا بتسريب المعلومات لمنافسين المؤسسة أو غير ذلك. (Tian, et al., 2019)
- منهج NIST CSF لتقييم مخاطر الأمن السيبرانى يمكنها اشتقاق مقاييس قابلة للقياس لكل وظيفة أساسية للإطار والفئات المعنية، وبالتالى تؤكد تمكين المؤسسة من التأكد من استعداد الأمن السيبرانى للمخاطر الفعلية، وأن تقييم

الالتزام بالمستوى المطلوب لـ NIST CSF يساعد فى تحديد الأشخاص المحددين والمعالجة ومجالات التكنولوجيا التى تتطلب التحسين، والتى تؤثر بشكل مباشر فى التخفيف من التهديدات الأمنية . بالإضافة إلى أنه يقدم ميزة عن أطر أخرى فى هذا الهدف وكذلك يمكنه الاستعانة بالأطر ذات الصلة مثل : Cobit ، COSO ، ISO 27000 ، ITIL، .. وأن القائمين عليه ما زالوا يقدموا التطوير الإضافي للأدوات لتبسيط عملية تنفيذها لجعلها قابلة للتكيف لجمهور أوسع وقابلة للقياس الكمي .

عرض الباحثون (Ibrahim, et al., 2018) : دراسة حالة لتقييم موقف الأمن السيبرانى لمؤسسة حكومية محلية فى غرب استراليا، باستخدام نموذج NIST CSF الصادر عن معهد المعايير التكنولوجي الأمريكي للأمن السيبرانى . ومن خلال هذه الحالة تم تناول الآتي : تقييم وضع الأمن السيبرانى للمؤسسة بغض النظر عن أعمالهم أو الحجم، التطبيق على منظمة حكومية محلية، عرض النتائج، التوصيات، وتعتبر المساهمة الرئيسية لهذه النتائج هى اعتماد NIST CSF كأداة تقييم واستهداف مستويات مختلفة من المؤسسة، اعتماداً على مستوى خبرتها والحصول على الاستجابات لتسهيل التقييم، القياس الكمي للتقييم ليعكس مدي شدة المخاطر الفعلية والتى بدورها تمكن المنشأة من معالجة القضايا بشكل فعال للوصول إلى المستوي المطلوب للامتثال، مراجعة تفصيلية لأطر العمل المماثلة .

خطوات تحسين وضع الأمن السيبرانى باستخدام NIST CSF :

١) تحديد الأولويات والنطاق، تحدد المؤسسة أهداف أعمالها، مهماتها، وأولوياتها التنظيمية

٢) تحدد المؤسسة الأنظمة والأصول ذات الصلة والمتطلبات التنظيمية والمخاطر ثم تحدد التهديدات ونقاط الضعف لهذه الأنظمة والأصول .

٣) إنشاء ملف تعريفي حالي (للوضع الحالي) . تقوم فيه المؤسسة من خلال نتائج الخطوتين ١، ٢ بإنشاء هذا الملف لوصف حال المؤسسة .

٤) إجراء تقييم المخاطر من خلال تحليل البيئة التشغيلية من أجل تحديد احتمالية حدوث الأمن السيبرانى والتأثير الذى يمكن أن يحدثه الحدث على المؤسسة .

٥) إنشاء ملف شخصي للمؤسسة مستهدفاً يركز على تقييم ووصف نتائج الأمن السيبرانى المطلوب .

٦) تحديد الثغرات وتحليلها وتحديد أولوياتها، من خلال مقارنة الملف الحالي بالملف المستهدف، وعمل خطة عمل ذات أولوية لمعالجة الثغرات التى تعتمد على محركات المهمة، وتحليل التكلفة/العائد، وفهم المخاطر لتحقيق النتائج إلى الملف الشخصي المستهدف .

٧) تنفيذ خطة العمل، تحدد المؤسسة الإجراءات التى يجب اتخاذها فيما يتعلق بالفجوات، إن وجدت، (المحددة فى الخطوة السابقة) .

تتم هذه الخطوات من خلال وظائف خمس[١] (NIST, 2014)، فهذه الوظائف تمثل الركائز الأساسية لبرنامج الأمن السيبرانى الناجح والشامل فهى تساعد المؤسسات فى التعبير بسهولة عن إدارتها لمخاطر الأمن السيبرانى على الأنظمة والأشخاص والأصول والبيانات والقدرات . وهذه الوظائف هى :

١) **التحديد (ID) Identify** : تحديد الهوية فى تطوير فهم تنظيمي لإدارة مخاطر الأمن السيبرانى على الأنظمة والأشخاص، فهم سياق الأعمال والموارد التى تدعم الوظائف الحيوية ومخاطر الأمن ذات الصلة بما يمكن المؤسسة من التركيز على جهودها وتحديد أولوياتها بما يتفق مع إستراتيجية إدارة المخاطر واحتياجات الأعمال

(١) يلاحظ على هذه الوظائف الخمسة بأنها متزامنة ومستمرة

٢) **الحماية (PR) Protect** : إنشاء حماية أمن البيانات بما يتفق مع إستراتيجية المخاطر فى المؤسسة لحماية سرية المعلومات وسلامتها وتوافرها، بالإضافة إلى حماية الأصول وإدارتها، حماية الموارد التنظيمية من خلال الصيانة .

٣) **الكشف (DE) Detect** : اكتشاف أحداث الأمن السيبرانى وتحديد الأنشطة المناسبة لتحديد حدوث حدث الأمن السيبرانى فى الوقت المناسب، وضمان اكتشاف الشذوذ (الانحرافات، الاختراقات)، وفهم تأثيرها المحتمل .

٤) **الاستجابة (RS) Respond** : اتخاذ إجراءات بشأن حادثة الأمن المكتشفة، والقدرة على احتواء تأثير الحادث المحتمل، ضمان تنفيذ عملية تخطيط الاستجابة أثناء وبعد الحادث مع أصحاب المصلحة (بالاقتضاء، ....) .

٥) **الاسترداد (الاستعادة) (RC) Recover** : تحديد الأنشطة المناسبة للحفاظ على خطط المرونة واستعادة أى قدرات أو خدمات تم إعاقتها بسبب حادث الأمن (الاستعادة فى الوقت المناسب للعمليات)، تنسيق الاتصالات الداخلية والخارجية أثناء وبعد الاستعادة .

وعن أهداف التحكم فى المعلومات والتقنيات ذات الصلة نجد أن COBIT5 هو CSF للأعمال المصممة لإدارة وصيانة أنظمة تكنولوجيا المعلومات للمؤسسات . حيث أنه يتكون من خمس مجالات ، ٣٧ عملية تتماشي مع مجالات المسئولية فى التخطيط والبناء والتشغيل والمراقبة . ويتم تنسيق COBIT5 مع معايير تكنولوجيا المعلومات والممارسات الجيدة الأخرى المعترف بها مثل : NIST ، COSO ، ISO، ITIL ... وغيرها . وجميعها مبنية على الاعتبارات الآتية : الحاجة إلى تلبية توقعات أصحابا لمصلحة، التحكم فى العملية من طرق إلى طرف آخر للمؤسسة، العمل كإطار واحد متكامل، إدراك أن الإدارة والحوكمة شيئان مختلفان . (IASCA, 2012)

على أثر التكامل بين إطر حوكمة نظم المعلومات المحسوبة الصادرة عن المعهد القومي الأمريكي الذى يعتبر الآن جزء من وزارة التجارة الأمريكية والتى استعانت بها الشركات الأمريكية فى الاقتصاد الأمريكي بما يتجاوز ٥٠٪ منها ، وإصدار COBIT 2013 ، فإن تصميم أداة تقييم بناءً على هذه الوظائف الخمس

السابق عرضها (التحدي، الحماية ، الكشف ، الاستجابة ، الاسترداد) تمكن من تحديد المستوى الحالي للمخاطر فى المؤسسات طبقاً للعوامل الداخلية والخارجية الآتية ، ممارسات إدارة المخاطر ، بيئة التهديد ، المتطلبات القانونية والتنظيمية ، أهداف الأعمال ، قيود المهمة ، وعلى المؤسسات تحديد المستوى المقبول للمخاطر لها شرط أن يكون من الممكن تنفيذه ويقلل من مخاطر الأمن السيبراني ، ويلبي أهدافها ، وفى هذا يحتاج الأمر إلى توكيده من خلال المراجعة الداخلية .

المراجعة الداخلية وتوكيدها لمخاطر الأمن السيبراني فى المؤسسات الحكومية

تتولى المراجعة الداخلية مسئولية توفير توكيد لمجلس الإدارة والإدارة التنفيذية عن مدى تقييم مخاطر الأمن السيبراني ، وإلا تواجه المؤسسة مخاطر تتعلق بأمنها وحمايتها (Deloitte , 2015) . تعد المراجعة الداخلية بدورها الوسيط للإدارة العليا ونظم الرقابة الداخلية كأحد أعمدتها المسئولة عن تقديم التوكيد عن المخاطر والحوكمة لهذه التكنولوجيا ، حيث أن المراجعة الداخلية أسندت إليها هذه المهمة من المعايير الدولية للممارسة المهنية لها (IIA,2017) ، بل والأكثر نادي بعض الباحثين (kahyaoglu & Caliyurt ,2018) بضرورة الحاجة إلى وجود خطة توكيد إلكتروني للتنفيذ فى المؤسسة كبرنامج قائم على المخاطر مستمر ، يكون قادر على تحديد مخاطر المؤسسة ، إجراءات الرقابة الداخلية ، ومعرفة الضوابط المطلوبة ومقارنتها بالموجودة ، ووضع خطة لتنفيذه الضوابط المفقودة بعد الاستعانة بأحد آليات حوكمة تكنولوجيا المعلومات للأمن والخصوصية ، ولهذا من الضروري أن يصبح المراجعون الداخليون "مستشارين إلكترونين موثوقين" من خلال المساهمة فى عملية توكيد الأمن السيبراني من خلال نتائجهم كخبراء متخصصين، ولذلك يتم تدريب المراجعين الداخليين على إطر الأمن السيبراني لتطوير خطة التوكيد على هذه الأطر ، بالإضافة إلى الحصول على شهادات (27001/2) وضرورة أن يغطي التوكيد على نطاق الأمن السيبراني الوظائف الخمسة لإطار NIST وهي التحديد ، الحماية ، الاكتشاف ، الاستجابة ، الاسترداد (الاستعادة) .

مما ينعكس على جودة التقارير المرفوعة للإدارة العليا من خلال لجنة المراجعة أو المخاطر التابعة له . ويساهم توكيد الأمن السيبراني الفعال فى زيادة فعالية وزيادة احتمال أن تكون المخاطر الإلكترونية والضوابط الرقابية لها فعالة وذلك لتقليل احتمالية التعرض للهجمات الإلكترونية (Boehm etal.,2010) فهي تتدخل فى مرحلة التخطيط والتنفيذ وإعداد التقارير للأمن السيبراني من خلال اشتقاق مقياس لقياس فعالية توكيد المراجعة الداخلية على الأمن السيبراني ، بالاعتماد على معايير الممارسة المهنية للمراجعة الداخلية التى توفر إطاراً إلزامياً لوظيفة المراجعة الداخلية وهي (COBIT5,NIST,2018,ISO27001/2) هذا ما يتم اختباره فى المحور التطبيقي للبحث .

المبحث الرابع : أثر تطوير الرقابة الداخلية بآليات حوكمة تكنولوجيا المعلومات على تقارير أجهزة الرقابة العليا فى مصر

تسعى أجهزة الرقابة العليا إلى تحقيق أكبر قدر ممكن من الكفاءة والفعالية فى أداء المهام الرقابية المسندة لها ، وذلك من خلال تطوير نظم الرقابة الداخلية للحد من الفساد المالي بالوحدات الحكومية ، عن طريق وضع نظام متكامل ومتطور لنظم الرقابة الداخلية يعتمد على بنود أساسية وهي :- بيئة رقابة سليمة وهى تشمل (تحديد السلطات والمسئوليات، ميثاق أخلاق، الالتزام بالأداب والسلوك المهني، درجة مشاركة الإدارة فى الرقابة)، نظم ضبط داخلي، - المراجعة الداخلية الفعالة (المراجعة الداخلية بما توفره من مراجعين داخليين مؤهلين لهم دور فى الحد من الفساد المالي)، - الاتصالات والمعلومات، -المتابعة وهى تعنى وضع إجراءات متابعة كافية لتقييم مدى كفاية الإجراءات الرقابية .

فوفقاً لأبعاد الرقابة الداخلية على تكنولوجيا المعلومات بصفتها أهم وسائل الكشف للإنحرافات Committee of sponsoring organization (COSO) وتقسيمها إلى : بيئة رقابية، تقييم المخاطر، الأنشطة الرقابية، المعلومات والاتصالات، المتابعة الرقابية .

أرشد دليل الممارسات الجيدة لتقويم وتحسين الرقابة الداخلية ، من خلال إتباع مدخل منتظم ومنضبط لتقييم وتحسين فعالية آليات إدارة المخاطر والرقابة والحوكمة (المراجعة الداخلية) وأن الرقابة الداخلية تقوم على عدد من المبادئ وهي : دعم أهداف المؤسسة ، تحديد الأدوار والمسئوليات ، تعزيز وترسيخ ثقافة التحفيز، الاستجابة للمخاطر ، توافر المهارات الكافية ، التواصل بشكل منتظم ، المتابعة والتقويم .

كذلك أسفر تطوير نظم الرقابة الداخلية بآليات حوكمة تكنولوجيا المعلومات لتوفير الأمن والخصوصية فى المعلومات المحاسبية المنتجة بالتقارير المالية للمؤسسات الحكومية فى الجزء السابق من البحث : عن أي دعم للمراجعة الداخلية بآليات حوكمة تكنولوجيا المعلومات (NIST) يوفر الأمن والخصوصية فى المعلومات مما ينعكس على جودة التقارير للمؤسسات الحكومية وفقاً للدليل الإرشادي لمنظمة الانتوساي "رقابة الأداء" وتعريفه لها بأنها هي عملية مستقلة وموضوعية يتم فيها التأكد من أن المؤسسات الحكومية وأنظمتها وعملياتها وبرامجها وأنشطتها ومؤسساتها تعمل وفقاً لمبادئ الاقتصاد والكفاءة والفعالية ، أي هل تدار الموارد بطرق اقتصادية ؟هل تعد نسبة المدخلات إلى الخدمات هي الطريقة المثلى ؟ هل تستطيع الجهة الحكومية الوصول إلى ما تم تحديده من أهداف ؟

وفقاً لمعيار مراجعة الأداء ISSAI-3 "المبادئ الأساسية لمراجعة الأداء" تعرف على أنها الفحص الذى يتم من خلال الأجهزة العليا للرقابة المالية وهو فحص مستقل وموضوعي وموثوق يؤكد أن المشروعات أو البرامج أو الأنشطة فى القطاع الحكومي قد تمت وفقاً لمبادئ الاقتصاد والكفاءة والفعالية ومدى إمكانية إجراء تحسينات عليها ، كما تساهم فى تقرير المساءلة والشفافية من خلال مساعدة المسئولين المعنيين بالحوكمة والرقابة لتحسين الأداء ، وتعزيز الشفافية من خلال منح أصحاب المصلحة نظرة ثاقبة عن إدارة الأنشطة المختلفة (Bring Selius , 2018) .

فى هذا أشار أحد الباحثين (HaniFah,2020) بتطبيق معايير الانتوساى وحوكمة تكنولوجيا المعلومات معاً بصورة تكاملية تزداد جودة تقارير الأجهزة العليا للرقابة .

توصلت دراسة (Saban,2012) التى تمت فى أندونيسيا إلى أن استخدام الحوكمة الإلكترونية (حوكمة تكنولوجيا المعلومات) للإدارة الحكومية بنسبة ٦٨٪ ، ساعد فى الحد من الفساد الإداري بنسبة ٦٦٪ .

أوصت دراسة (سويطي ، ٢٠٢٢) بضرورة إيلاء موضوع الرقابة الداخلية على تكنولوجيا المعلومات والاتصالات المتبعة فى إدارات المشتريات الحكومية الأهمية اللازمة للحد من الفساد .

مما سبق ترى الباحثة ، أنه من خلال تحقيق جودة تقارير المراجعة الداخلية فى تطبيق حوكمة تكنولوجيا المعلومات باستخدام آليات NIST للرقابة الداخلية لأمن وخصوصية المعلومات المحسوبية، ينعكس الأمر على تقارير الإدارة العليا التى ترفع من لجنة المراجعة المأخوذة من إدارة المراجعة الداخلية والتى تعتمد عليها الجهات الرقابية العليا (رقابة الجهاز المركزي للمحاسبات) مما ينعكس على جودة تقاريره عن المؤسسات الحكومية .

المبحث الخامس : الدراسة التطبيقية

تمهيد :

يتم تناول مجتمع الدراسة واختيار العينة، والأداة المستخدمة لتجميع البيانات واختبار مدى صدق محاور الأداة، وكذلك الأساليب الإحصائية المستخدمة فى معالجة البيانات التى تم جمعها وعرض اختبار فروض البحث من خلال نتائج التحليل الإحصائي.

مجتمع وعينة البحث :مجتمع الدراسة هو المراجعين الداخليين، وأعضاء الجهاز المركزي للمحاسبات لمراجعة الوحدات المحلية فى جمهورية مصر العربية . ولاختيار العينة من هذا المجتمع يتم وفقاً لقانون Moser(*) :

قانون Moser(*) ن د = ع٢ / (ع س د)٢، حيث أن : ن : حجم العينة المراد قياسها، ع س د = حد الثقة أو درجة الدلالة = ٢ / ١.٩٦ = ١، ع = الانحراف المعياري، ع س = حد الثقة أو درجة الدلالة للوسط الحسابي لمجتمع الدراسة / مستوى الثقة بافتراض أن الانحراف المعياري لمجتمع الدراسة ٢٠ ∴ ن د = (٢٠)٢ / (١)٢ = ٤٠٠ / ١ = ٤٠٠ مفردة ، وتم إعداد قوائم الاستبيان لتجميع البيانات، وكانت القوائم الواردة والصحيحة منها للتحليل الإحصائي ٣٠٠ قائمة موزعة (١٥٠) للمراجعين الداخليين، (١٥٠) لمراجعي الجهاز المركزي للمحاسبات، أى بنسبة = ٣٠٠ ÷ ٤٠٠ = ٧٥٪

تقويم أداء القياس وتحليل وتفسير نتائج البحث :

تتكون قائمة الاستبيان من قسمين رئيسيين وهما :

- القسم الأول : محاور الدراسة الموجهة لفئة المراجعين الداخليين . .
- القسم الثاني : محاور الدراسة الموجهة لفئة مراجعي الجهاز المركزي للمحاسبات

وتتناول محاور الدراسة ٤١ سؤالاً وهى موزعة على المحاور الآتية :

- المحور الأول : مراحل أو مجالات تطوير المراجعة الداخلية على أساس الخطر وعلاقتها بحوكمة تكنولوجيا المعلومات .
- المحور الثاني : توافر آليات حوكمة تكنولوجيا المعلومات وفقاً لإطار NIST Risk management Frame (RMF) Sp 800-37 للرقابة الداخلية وعلاقتها بمخاطر الحوسبة السحابية .
- المحور الثالث : حوكمة تكنولوجيا الحوسبة السحابية وفقاً لإطار NIST Sp 800-37 للرقابة الداخلية وعلاقتها بجودة المراجعة الداخلية للوحدات المحلية الحكومية .
- المحور الرابع : أثر دعم المراجعة الداخلية فى ظل مخاطر الحوسبة السحابية بإطار NIST على تحسين تقارير الجهاز المركزي للمحاسبات المصري .

صدق وثبات أداة الدراسة :

الجدول رقم (١) يوضح جميع معاملات الارتباط فى جميع مجالات الاستبيان دالة إحصائية عند مستوى معنوية ٠.٠٥ وبذلك تعتبر جميع محاور الاستبيان صادقة لما وضعت لقياسه كالآتي :

جدول (١) معامل الارتباط بين درجة كل محور من محاور الاستبيان والدرجة الكلية للاستبيان

المحـور	معامل بيرسون للارتباط			القيمة الاحتمالية (Sig)
	الأساسية	المتقدمة	الحوسبة السحابية	
١) مراحل أو مجالات تطوير المراجعة الداخلية وعلاقتها بحوكمة تكنولوجيا المعلومات.	٠.٦٢٠ -	٠.٤٦٥-	٠.٥٧٦+	صفر
٢) توافر آليات حوكمة تكنولوجيا المعلومات وفقاً لإطار NIST للرقابة الداخلية وعلاقتها بمخاطر الحوسبة السحابية فى المؤسسات الحكومية المصرية.	٠.٥٦٨ +			صفر
٣) حوكمة تكنولوجيا الحوسبة السحابية وفقاً لإطار NIST وعلاقتها بجودة المراجعة الداخلية فى المؤسسات الحكومية المصرية .	٠.٧٦٥			صفر
٤) أثر دعم المراجعة الداخلية فى ظل حوكمة تكنولوجيا الحوسبة السحابية لإطار NIST على تحسين تقارير الجهاز المركزي للمحاسبات المصرى .	٠.٨١١			صفر

المصدر : من أعداد الباحثة بناءا على مخرجات SPSS

الارتباط دال إحصائياً عند مستوى معنوياً ٥٪

جدول (٢) معامل ألفاكرونباخ

المحـاور	عدد الفقرات	معامل ألفا كرونباخ	الدلالة
مراحل أو مجالات تطوير المراجعة الداخلية وعلاقتها بحوكمة تكنولوجيا المعلومات.	١٩	٠.٧٤١	٥٪ >
توافر آليات حوكمة تكنولوجيا المعلومات وفقاً لإطار NIST للرقابة الداخلية والحد من مخاطر الحوسبة السحابية فى المؤسسات الحكومية المصرية.	٦	٠.٩٤٨	٠.٠٥ >
حوكمة تكنولوجيا الحوسبة السحابية وفقاً لإطار NIST وجودة المراجعة الداخلية فى المؤسسات الحكومية المصرية .	١١	٠.٩٤٨	٠.٠٥ >
أثر دعم المراجعة الداخلية فى ظل حوكمة تكنولوجيا الحوسبة السحابية لإطار NIST على تحسين تقارير الجهاز المركزي للمحاسبات المصرى .	٥	٠.٩٦٣	٠.٠٥ >
الاستبيان ككل	٤١	٠.٨٨٥	٠.٠٥ >

واضح من النتائج أن قيمة معامل ألفاكرونباخ لجميع عبارات الاستبيان ٠.٨٨٥، وهذا يعنى أن معامل الثبات مرتفع، وبذلك تأكدنا من صدق وثبات الاستبيان وصلاحيته.

اختبار كولمجروف – سمرنوف (Kolmogorov - Smironov - Z) :

جدول (٣) (Kolmogorov - Sminorov - Z)

المحاور	نتيجة الاختبار	القيمة الإجمالية	الدلالة
١) مراحل أو مجالات تطوير المراجعة الداخلية وعلاقتها بحوكمة تكنولوجيا المعلومات.	٠.٨٦٦	٠.٢٤٠	< ٥٪
٢) توافر آليات حوكمة تكنولوجيا المعلومات وفقاً لإطار NIST للرقابة الداخلية والحد من مخاطر الحوسبة السحابية فى المؤسسات الحكومية المصرية.	٠.٨٨١	٠.٢١٥	< ٥٪
٣) حوكمة تكنولوجيا الحوسبة السحابية وفقاً لإطار NIST وجودة المراجعة الداخلية فى المؤسسات الحكومية المصرية .	٠.٨٨١	٠.٢١٥	< ٥٪
٤) أثر دعم المراجعة الداخلية فى ظل حوكمة تكنولوجيا الحوسبة السحابية لإطارNIST على تحسين تقارير الجهاز المركزي للمحاسبات المصرى .	٠.٨٨٣	٠.٢٠٦	< ٥٪
الاستبيان ككل	٠.٦١١	٠.٢١٠	< ٥٪

يتضح من الجدول السابق أن الفروض تتبع التوزيع الطبيعي لأن مستوي الدلالة أكبر من ٠.٠٥ مما يتيح إجراء الاختبارات المعملية .

اختبار فرضيات البحث :

تحليل النتائج الإحصائية للفرض الأول : توجد علاقة معنوية ذات دلالة إحصائية بين مراحل أو مجالات المراجعة الداخلية وحوكمة تكنولوجيا المعلومات :

يهدف هذا الفرض إلى معرفة فيما إذا كان هناك أثر ذو دلالة إحصائية بين مراحل ومجالات تطوير المراجعة الداخلية وحوكمة تكنولوجيا المعلومات، وتم استخدام الانحدار الخطي البسيط لاختبار هذا الفرض، حيث يتمثل المتغير المستقل فى المتغيرات الآتية : الأساسية، المتقدمة، الحوسبة السحابية، والمتغير التابع هو

حوكمة تكنولوجيا المعلومات، حيث تم اختبار القدرة التفسيرية للنموذج ومن ثم معالجة الانحدار الخطي البسيط، وكانت النتائج كما هو موضح بالجدول التالي :

جدول (٤) نتائج اختبار القدرة التفسيرية لنموذج الانحدار البسيط (الفرض الأول)

المجالات الثلاثة	معادلة الانحدار	معامل التحديد R_2	معامل الارتباط	اختبار F	القيمة الاحتمالية Sig
الأساسية	y=٥.٠٩-٠.٧٥٣×	٣٨.٤٪	-٠.٦٢٠	٩٢.٣٨٥	٠.٠٠٠١[b]
المتقدمة	y=٥.٤٢١-٠.٧٨٩×	٢١.٦٪	-٠٤٦٥	٤٠.٨٧٤	٠.٠٠٠١[b]
الحوسبة السحابية	y=٥.٠٨٤-٠.٧٦٣×	٣٣.١٪	+٠.٥٧٦	٧٣.٣٢٧	٠.٠٠٠١[b]

١) معامل الارتباط بين المتغير المستقل والتابع فى المرحلة الأساسية لاحتياج المراجعة الداخلية لحوكمة تكنولوجيا المعلومات = - ٠.٦٢ أى أنها علاقة عكسية وقوية .

٢) معامل الارتباط بين المتغير المستقل والتابع فى المرحلة المتقدمة لاحتياج المراجعة الداخلية لحوكمة تكنولوجيا المعلومات = - ٠.٤٦٥ أى أنها علاقة عكسية وقوية لكنها أقل من الأساسية، وهذا يفسر أنها قد تحتاج فى هذه المرحلة .

٣) معامل الارتباط بين المتغير المستقل والتابع فى مرحلة الحوسبة السحابية لاحتياج المراجعة الداخلية لحوكمة تكنولوجيا المعلومات = + ٠.٥٧٦ أى أن العلاقة طردية وقوية . نستنتج من هذا الجدول ونتائج تحليل الارتباط الآتي :

أن كل مرحلة للمراجعة الداخلية (المرحلة الأساسية أوالتقليدية، المرحلة المتقدمة) يكون الاحتياج لحوكمة تكنولوجيا المعلومات غير مجدي وليس ذو أهمية على الرغم أنه فى المرحلة المتقدمة كانت العلاقة عكسية لكنها ضعيفة، أما فى المرحلةالأخيرة وهى وجود الحوسبة السحابية فإن العلاقة طردية وقوية وذو دلالة معنوية .

لـذلك نـرفض الفـرض العـدم ونقبـل الفـرض البـديل لكـل مـن المرحلـة الأساسـية والمتقدمة . أما بالنسبة للمرحلة الثالثة الخاصة بالحوسبة السحابية، فإننا نرفض الفرض البديل ونقبل الفرض العدم .

تحليل النتائج الإحصائية للفرض الثاني : توجد علاقة معنوية ذات دلالة إحصائية بين آلية NIST للرقابة الداخلية والحد من مخاطر الحوسبة السحابية فى الوحدات المحلية الحكومية فى مصر :

عدد البيانات المستخدمة (١٥٠) بمعني أنه تم استخدام كل المشاهدات، وبلغ كل من المتوسط الحسابي والانحراف المعياري القيم ٣.١٢٥، ١.٣٥٦ لأسئلة المحور الثاني.

جدول (٥) نتائج اختبار القدرة التفسيرية لنموذج الانحدار البسيط (الفرض الثاني)

معادلة الانحدار	معامل التحديد R_2	معامل الارتباط	اختبار F	القيمة الاحتمالية Sig
٠.٨٢٩+٠.٩١٨×	٨٤.٣٪	٠.٤٢٣	٧٩٦.١٨	٠.٠٠٠١[b]

من خلال ما سبق يتضح أن معامل الارتباط بين المتغير المستقل والمتغير التابع يساوى ٠.٩١٨ (العلاقة طردية وقوية)، وأن معامل التحديد R_2 يساوي ٠.٨٤٣ أى ٨٤.٣٪ من التغير فى المتغير التابع ترجع إلى المتغير المستقل وخط الانحدار، p.(Value) مستوى الدلالة المعنوية تساوى ٠.٠٠٠١ وهى أقل من مستوي المعنوية ٥٪ أى أن نموذج الانحدار معنوي، وأن معادلة الانحدار هى ٠.٨٢٩ + ٠.٩١٨ وهى تعبير عن B، Beta وأن B عن مستوي معنوية ٠.٠٠٠، Beta عند مستوي معنوية ٠.٠٠٠١ مما يدل على أن العلاقة طردية . وهنا يتم قبول الفرض العدم ورفض الفرض البديل.

تحليل النتائج الإحصائية للفرض الثالث : توجد علاقة معنوية ذات دلالة إحصائية بين حوكمة تكنولوجيا الحوسبة السحابية وفقاً لإطار NIST وجودة المراجعة الداخلية فى الوحدات المحلية الحكومية فى مصر:

تم استخدام البيانات لـ (١٥٠) مفردة أى كل المشاهدات، وبلغ كل من المتوسط الحسابي والانحراف المعياري القيم ٣.٧٦٥، ١.٢٤١ لكل أسئلة المحور الثالث. وفيما يلي جدول نتائج التحليل الإحصائي :

جدول (٦) نتائج اختبار القدرة التفسيرية لنموذج الانحدار البسيط (الفرض الثالث)

معادلة الانحدار	معامل التحديد R_2	معامل الارتباط	اختبار F	القيمة الاحتمالية Sig
٠.٧٦٥× +٠.٦٧٧	٥٨.٦٪	٠.٦٧٧	٢٠٩.٢٥	٠.٠٠٠١[b]

مما سبق يتضح أن معامل الارتباط بين المتغير المستقل والمتغير التابع يساوى ٠.٦٧٧ (العلاقة طردية)، وأن معامل التحديد R_2 يساوي ٥٨.٦٪ من التغير فى المتغير التابع ترجع إلى المتغير المستقل وخط الانحدار، وأن p.(Value) مستوى الدلالة المعنوية تساوى ٠.٠٠٠١ وهى أقل من ٠.٠٥ أى أن نموذج الانحدار معنوي، ولهذا يتم قبول الفرض العدم ورفض الفرض البديل.

تحليل النتائج الإحصائية للفرض الرابع : توجد علاقة معنوية ذات دلالة إحصائية بين دعم المراجعة الداخلية بحوكمة تكنولوجيا الحوسبة السحابية باستخدام إطار NIST وتحسين تقارير الجهاز المركزي للمحاسبات فى مصر :

تم استخدام جميع مفردات العينة للجهاز المركزي للمحاسبات (١٥٠) لكل المشاهدات، وتبين الآتى : معامل الارتباط بين المتغيرين المستقل والتابع يساوى ٠.٨١١ أى أن (العلاقة طردية وقوية)، وأن معامل التحديد R_2 يساوي ٦٥.٨٪ أى

أن ٦٥.٨٪ من التغير فى المتغير التابع يرجع إلى المتغير المستقل وخط الانحدار، . وفيما يلي جدول نتائج التحليل الإحصائي :

جدول (٧) نتائج اختبار القدرة التفسيرية لنموذج الانحدار البسيط (الفرض الرابع)

معادلة الانحدار	معامل التحديد R_2	معامل الارتباط	اختبار F	القيمة الاحتمالية Sig
٠.٨١١× +٠.٤٥٢	٦٥.٨٪	٠.٨١١	٢٨٤.٣٧	٠.٠٠٠١[b]

ومستوى الدلالة المعنوية تساوى ٠.٠٠٠١ وهى أقل من مستوى المعنوية ٠.٠٥ = α أى أن المتغير المستقل ذو تأثير معنوي، وأن معادلة الانحدار Beta + B تدل على علاقة قوية وطردية، مما نستنتج قبول الفرض العدم ورفض الفرض البديل.

النتائج والتوصيات والرؤيا المستقبلية :

أولاً : النتائج :

خلصت الباحثة إلى النتائج الآتية :

- لا توجد علاقة معنوية ذات دلالة إحصائية بين المراجعة الداخلية التقليدية (فى المرحلة الأساسية) وحوكمة تكنولوجيا المعلومات .
- لا توجد علاقة معنوية ذات دلالة إحصائية بين المرحلة المتقدمة للمراجعة الداخلية وحوكمة تكنولوجيا المعلومات .
- توجد علاقة معنوية ذات دلالة إحصائية بين مرحلة الحوسبة السحابية للمراجعة الداخلية وحوكمة تكنولوجيا المعلومات .
- توجد علاقة معنوية ذات دلالة إحصائية بين آلية NIST Sp 800-37 للرقابة الداخلية والحد من مخاطر الحوسبة السحابية فى الوحدات المحلية فى مصر .
- توجد علاقة معنوية ذات دلالة إحصائية بين حوكمة تكنولوجيا الحوسبة السحابية وفقا لإطار NIST Sp 800-37 وجودة المراجعة الداخلية فى الوحدات المحلية فى مصر .

ثانياً : التوصيات :

من خلال تناول موضوع البحث فى الجزء النظري والميداني وفى ضوء نتائجه، يخرج البحث بالتوصيات الآتية :

١ – الاهتمام بالتطورات المستحدثة فى نظم المعلومات والاتصالات بصورة مستمرة، وبالإرشادات التى تصدرها المنظمات المهنية فى هذا الشأن، وخاصة الـ ٩٠ إرشاد التى أصدرتهم NIST من أجل مواكبة كل التغييرات، وأخذها فى الحسبان لمساعدة متخذي القرارات فى المؤسسات .

٢ – العمل الدائم على إيجاد وسائل للتقييم المستمر لآليات الرقابة الداخلية، لما لها من دور وتأثير على المراجعة الداخلية وينعكس بالتالي دورها على المراجعة الخارجية وتقاريرها.

٣ – الاهتمام بدور المراجعة الداخلية فى المؤسسات، وخاصة الحكومية منها وبأهمية الحفاظ على استقلاليتها، من أجل دورها التوكيدى والاستشاري لمحاربة الفساد والاحتيال وعدم الإسراف فى استخدام الموارد التى دائماً ما تتصف بالندرة النسبية.

٤ – أهمية الالتزام بتطبيق آليات الرقابة الداخلية، وخاصة آلية NIST لمواجهة مخاطر الاختراق والبرامج الخبيثة المصاحبة للتطبيقات التكنولوجية ، ولاسيما الحوسبة السحابية كما تناولها هذا البحث من أجل توفير الأمن والخصوصية فى المعلومات وبصفة خاصة للمؤسسات الحكومية منها لأنها تتصف بالعمومية.

٥ – الحرص على توافر هياكل تنظيمية فى المؤسسات الحكومية المصرية من أجل تطبيق إجراءات الرقابة الداخلية للحد من الفساد المالى والإداري ولإمكانية تطبيق الآلية المقترحة .

ثالثاً : الرؤيا المستقبلية :

تقترح الباحثة فى ضوء دراستها وما توصلت إليه من نتائج الآتي :

- إبراز دور المراجعة وتأثيرها على الأداء الحكومي والإيرادات الضريبية من خلال دورها فى مكافحة الفساد .
- الدور الحكومي لتكنولوجيا المعلومات فى معالجة مخاطر الرهن العقاري فى مصر .
- استخدام آلية NIST للرقابة الداخلية لأمن وخصوصية المعلومات ودورها فى حوكمة تكنولوجيا المعلومات على البيانات الضخمة، الربوتات، أدوات الذكاء الاصطناعي، والبلوك تشين (Block-Chain) .

المراجع : أولاً : المراجع العربية :

١) الأربانى، أروى، العريقى، سماح عبد العزيز، (٢٠١٧) . "استقصاء وعى مسئولى إدارات تكنولوجيا المعلومات للانتقال إلى خدمة الحوسبة السحابية حالة دراسية : مؤسسات يمنية"، **مجلة الفرى للعلوم الاقتصادية والإدارية**، مجلد ١٤، العدد ١، ص ص ١٩٤ – ١٩٦ .

٢) البلقاسى، منال صبحي على، (٢٠١٨) . "اثر تطبيق حوكمة تكنولوجيا المعلومات وفقاً لـ Coblt5 على مخاطر نظم المعلومات الإلكترونية"، دراسة ميدانية على المعاهد العالية الخاصة، **المجلة المصرية للدراسات التجارية**، مجلد٤٢، العدد١، ص ص٧٨ – ١١٩ .

٣) العبيدي، أحمد جاسم حمودى، (٢٠١٩) . "التكامل بين إطار حوكمة تقنية المعلومات Cobit5 وإطار الرقابة الداخلية التكامل المحدث ودوره فى تعزيز مصداقية القوائم المالية"، دراسة تطبيقية، **رسالة دكتوراه، كلية الإدارة والاقتصاد، الجامعة المستنصرية – العراق**، Available at:https://uomustansir/yah.edu.19

٤) الفقي، مصطفى إبراهيم، صقر، أحمد على غازي، المكصوصي، على عبد الكريم هادى، (٢٠٢٣) . "أثر التكامل بين معايير الإنتوساى وحوكمة تكنولوجيا المعلومات على جودة تقارير الأجهزة العليا للرقابة"، دراسة ميدانية بالعراق، **المجلة المصرية للدراسات التجارية، كلية التجارة – جامعة المنصورة**، العدد ٢، ص ص ٣٢٧ – ٣٥٢ .

٥) المرى، راشد محمد، (٢٠٢٣) . "أثر تكنولوجيا المعلومات فى النظام الأمنى والرقابة الداخلية"، **مجلة البحوث الفقهية والقانونية، كلية الشريعة والقانون بدمنهور، جامعة الأزهر**، العدد ٤٠، ص ١٣٠٣ – ١٣٧٣ .

٦) المطيرى، نواف بندر على نهار، وهدان، محمد على، عبد الرحمن، مروة أجمد، (٢٠٢٢) . "دور آليات التحول الرقمي فى تفعيل مدخل المراجعة على أساس المخاطر لتعزيز جودة عملية المراجعة"، **المجلة العلمية للدراسات والبحوث المالية والإدارية، كلية التجارة – جامعة مدينة السادات**، المجلد ١٣، العدد ٢ .ص ص٣٤–٧٢

٧) الانتوساى، (٢٠١٧) . "دليل إرشادي لرقابة إطار العمل المؤسسي لمكافحة الفساد . **https:llidi.no/elibrary/well-gorerned-sais/saisfighting-corruption /703-final-gwdancein-arabic/file**

٨) جودي، حمائى موسي، (٢٠١٢) . "حوكمة تقنية المعلومات أداة إستراتيجية لحماية امن المعلومات"، **الملتقي الوطني حول حوكمة الشركات كأداة من الفساد المالي والإداري، جامعة محمد حيضر – الجزائر**، ص٨ .

٩) سليمان، حنان وكريا محمد، (٢٠١٩) . "أثر حوكمة تكنولوجيا المعلومات على جودة التقارير المالية – دراسة ميدانية"، **رسالة ماجستير، كلية التجارة – جامعة بنها** .

١٠) سويطى، شبلى إسماعيل، (٢٠٢٢) . "دور الرقابة الداخلية فى مكافحة الفساد فى وحدات المشتريات فى مؤسسات القطاع العام الفلسطيني"، **المجلة العربية للإدارة**، مجلد ٤٢، العدد الأول، ص٩٠ .

١١) شحاته، محمد على موسي، (٢٠٢٠) . "قياس أثر تفعيل أنشطة المراجعة الداخلية لآليات التحول الرقمي على تعزيز المساءلة والشفافية وتحسين الأداء الحكومي مع دليل ميداني بالبيئة المصرية"، **المجلة العلمية للدراسات المحاسبية**، مجلة كلية التجارة – جامعة قناة السويس، مجلد٢، ص ص ٧٠٣ – ٧٨٧ .

١٢) عطية، احمد محمد صلاح، (٢٠٢١) . "التحول الرقمي فى مصر على يلقي بمسئوليات جديدة على المراجع؟"، **مجلة البحوث التجارية**، كلية التجارة – جامعة الزقازيق، مجلد ٤٣، العدد ١، ص ٥١ – ٦٥ .

١٣) على، احمد محسن إسماعيل على، سلامة، نبيل فهمي، محمد محمود، (٢٠٢٣) . "الأساليب التكنولوجية المعاصرة فى الفكر المحاسبي ومخاطرها، **مجلة البحوث المالية والتجارية**"، كلية التجارة – جامعة بور سعيد، المجلد ٢٤، العدد الأول، ص ٣٥٥ – ٣٥٦ .

١٤) مجدوب، خيرة، زيانى، عبد الحق،(٢٠١٨) "فعاليات عمليات COBIT5 الحد من مخاطر الحوسبة السحابية"، دراسة استطلاعية على مجموعة من البنوك التجارية بولاية تيارات–الجزائر ،**مخبر تطوير المؤسسات الاقتصادية الجزائرية**،جماعة ابن خلدون، ص١–١٦ .

١٥) محمود، منصور حامد، رمضان، عماد جابر، (٢٠١٧) . "مدخل محاسبي مقترح لترشيد نفقات الأداء الحكومي للخدمات الإلكترونية فى ظل الحوسبة السحابية"، **المجلة العلمية للدراسات التجارية والبيئية**، المجلد الثامن، ملحق العدد الثالث، الإسماعيلية، ص ٣٣٤ – ٣٦٠ .

١٦) مسرحد، بلال، (٢٠١٩) . "تصور حوكمة الحوسبة السحابية فى المؤسسات الحكومية"، **مجلة الإستراتيجية والتنمية**، كلية العلوم الاقتصادية والتجارية وعلوم التيسير – الجزائر، المجلد ٩، العدد ٣، الجزء الأول، ص ١٧٥ – ١٩٨ .

١٧) منظمة التنمية والتعاون الدولى(OECD)، ٢٠١٩، الرقابة الداخلية وإدارة المخاطر من أجل النزاهة العامة فى **منطقة الشرق الأوسط وشمال إفريقيا** ، ص ٦١ – ٦٣ .

١٨) ناكره، شلير عبد الرحمن رشيد، على، أسامة حسين، (٢٠٢٠) . "دور آليات حوكمة تقنيات المعلوماتفى تفعيل إدارة مخاطر نظم المعلومات المحاسبية المحوسب وفق إطار NIST للرقابة الداخلية"، **مجلة قه لاى زانست العلمية، الجامعة اللبنانية الفرنسية – أربيل**، كوردستان، العراق، المجلد ٥، العدد ٣، ص ٤٩٨ – ٥٣١ .

١٩) وهدان، محمد على، (٢٠٢٢) . "دور المراجعة الداخلية فى تحقيق الإصلاح الحكومي : رؤية تحليلية مستقبلية"، **المجلة العلمية للبحوث التجارية، كلية التجارة** – جامعة المنوفية، العدد ٣، ص ١ – ٣٤

٢٠) خدمات التعاون فى مكافحة الجريمة السيبرانية https://www.interpol.int/ar14/616

ثانياً : المراجع الأجنبية :

1) Abu-Musa , A.,A.(2006) “Investigating the perceived threats of computerized accounting information systems in developing countries : An Empirical/ study on Saudi organizations , journal of king saud university - Computer and information sciences , 18,1-30

2) Administrative control authority . (2019) , “National Anti - corruption strategy” , (ACA) .

3) Betti,N.,Sarens,G. and poncin , I.(2021) , "Effects of digitalization of organizations on internal audit activities and practices , managerial auditing journal , 36(6) , pp.872-888 .
4) ----------. (2021) , "Understanding the internal audit function in a digitalized business environment" , Journal of accounting & organizational change , 17(2) , pp.197-216 .
5) Boehm,J.,Curcio N., Merrath , P.,Shenton , L., & Stahle, T.(2019) "The risk - based approach to cyber security" available at : https://www.mckinsey.com
6) Bring selius,L.,(2018) , "Efficiency , economy and effectiveness - but what about elhics? supreme audit institutions at a critical juncture , public money & management , 38 (2) , pp.105-110 .
7) Bubilek,O.,(2017) , "Importance of internal audit and internal control in an organization" - case study , unpublished degree thesis, Fenlinda .
8) Chambers,R.,(2017) , "Digital transformation what Does this Mean to internal Audit ? available at :
https://www.dallasiia.org/wp.content/uploads/2017j11/digital-tranformation-whatdoes-this-mean-to-internal-audit-clint-Mcpherson.pdf .
9) -------- . (2021) "How does digitalization change the role and way of working of internal audit : An Exploratory overview, https://www.iia.ni/actualititeit /nieuws/how-does-digitalization-change-the-role-and-way-of-working-of-internal-audit-an-expolatory-overview .
10) Cloud security alliance , (2011) , "security guidelines for critical areas of focus in cloud computing , v3.0.
11) Deloitte , (2015), "Cybersecurity : the changing role of audit committee and internal audit , available at : www2.deloitte.com
12) Eric,K.,& Galen,G.,(2018) "What cloud computing really means" Info world , available at :
www.infoworld.corn.article/08/04/07/15fe-cloud.computing-reality-1.html.
13) Fisher,M., Imgrunda , F., Janiescha, B.C., Winkelmann , A . (2020) , "Strategy archetypes for digital transformation : Defining Meta objectives using business process management" , information & Management journal home page, 1-13 :
. www.Elsevier.com/locate/IM

14) Grembergen , Wimvan & Haes , Stven De (2019) , "Introduction to the Mine track on it governance and its mechanisms" proceedings of the NIST Hawaii international conference on system science / 2019 , p.4 .
15) Hamdan, M., N.,(2017) , "The relationship between network security policies and audit evidence documentation : the accounting information security culture as a mediator , International journal of business and management , http://doi.org/10.5539/ijbm.v12n12p168
16) Hanifah, S., (2020) , "The effect of level of education , accounting knowledge , and utilization of information technology toward quality the quality of MSME'S Financial reports" , Conference of economic, Business and social science , Jakarta : universities Mercu Buana Jakarta .
17) Haren,Van, (2018 - 2019) , "Global standards and publications: , van Haren publishing , pp.50-54 .
18) Hwang,I.,Wakefield,R., Kim,S., & Kim,T.(2019) . Security awareness : the first step in information security compliance behavior , journal the first step in information security compliance behavior , journal of computer information systems , pp.1-12 , available at : http://doi.org//0.1080/08874417.2019.1650676.
19) IASCA(2012) , "COBIT 5 , https://cobitonline.isaca.org .
20) Ibrahim,A., Valli, C., Msateer , J., (2018) , "A security review of local government using NIST CSF : a case study , the journal of supercomputing , 74(10) , 5171-5186, available at : https//ro.edu.au/ecuworks/post2013/4844 .
21) IIA.(2021) , "Internal audit's digital transformation imperative : Advances Amid crisis , published by the intenal audit foundation : http://iia.no/wp-content/uploads/2021/04/2021-IAS Dig transf - Imperative report - audit board .
22) Institute of internal auditors (IIA) , international standards for the professional practice of internal auditing standards,(2016) , available at : https://theiia.org .
23) Johnsen,A., Reichborn-kjennerud,K.,Carrington , T., Jeppesen,K. k.,Taro, K., & Vakkuri, J.(2019) , "Supreme audit institutions in a high - impact context : A comparative analysis of performance audit in four Nordic Countries , financial accountability & management , 35 (2) , pp. 158-181 .
24) Jordan , Ernest , (2004) , "It Governance and corporate governance : Risk and systems . available at : http://ssrn.com .

25) Kalpesh , M. and Saurabh , B. (2019) , "Impact of digital on the future of internal Audit" , Ex/ service Holdings , Inc , available at : www.ex/service.com/legal-disclaimer
26) Kahyaoglu,S. & Caliyurt , K.(2018) " Security assurance process from the internal audit perspective" , Managerial auditing journal , 33(4) , pp.360-376 .
27) Kahyaoglu,S.B. and Caliyurt, K. (2018) , "Cyber security assurance process from the internal audit perspective" , Managerial auditing journal , vol.33 , No.4 , pp.360-376 . http://doi.org//0.1108/MAJ-02-2018-1804 .
28) Masanja , N., M. & Masimba , A.,(2020) , "The effectiveness of internal control system on the efficiency of financial management for selected training institutions in Arusha " , Contemporary journal of education and business (C1EB) , Vol.1,ISS,1,2020, PP.55-73 , www.ijieb.co.tz/cjeb,ISSN2738-9294
29) Metalia,M., Zakasyi, S .W.,& Sugarman,H.(2020) , "Factors affecting the performance of Indonesian government's internal supervisory , Utopia Y praxis Latino Americana , 25 (ESP.10) 498-513 .
30) Nambisam,S.,Wright,M., & Feldman,M., (2019) . the digital transformation of innovation and entrepreneurship : progress challenges , and Key themes, Research police , 48(8) .
31) NIST, (2014) , "Framework for improving critical infrastructure cyber security :
version1.0.http://www.nist.gov/sites/default/files/documents/ syberframework/sybersecurity-framework-021214-pdf .
32) ------- (2018) , "Risk management framework for information systems and organizations" : national institute of standards and technology , publisher , (U.S.A) , Available at :
http://doi.org/10-6028/Nist.sp.800-37 .
33) Otero,A.R.,(2015) , "An information security control assessment methodology for organizations" financial information , International journal of accounting information systems , 18,26-45
34) Price water house coopers risk (pwc) , Davydova Anna , (2019) , "Services state of the internal audit profession study" , Elevating internal audit's role : the digitally fit function , available at : www.pwc.com/sg,internal/Audit .
35) Sabani , A., (2019) , "Indonesia in the spotlight : Combating corruption through ICT enabled governance", Melbourne : procedia computer science journal , vol.2 , No.161,pp324-332

36) The institute of internal auditors, (IIA) , (2004) , "The role of internal audit in enterprise - wide risk management" , available at : www.iia.org.uk .

37) Tian, H., Nan , F., Jiang, H., Chang , C.C.,Ning, J., & Huang,4(2019) , "Public auditing for shared cloud data with efficient and secure group management information sciences" , 472, 107-125. http:doi.org//0.1016/j.ins.2018.9.009 .

38) Vuko,T.,Slapnicar,S.,Cular, M.,& Drascek, M.(2021) , "Key drivers of cyber security audit effectiveness : the neo- institutional perspective" , available at SSRN : http://ssrn.com/abstract=3932177 or http :// dx.doi.org/10.2139/ssrn.3932177

39) Yang,G.,Yu,J.,Shen, W.,Su,Q.,Fu,Z., & Hao, R . (2016) . « Enabling public auditing for shared date in cloud storage supporting identity privacy and traceability , journal of systems and software , 113 , pp.130-139 .

40) World Economic forum. (2020) , "Hacking corruption in the digital era : How tech is shaping the future of integrity in times of crisis" , http://www3.weforum.org/docs/WEF-GFC-On transparency -and - AC - Agenda - For -Business Integrity - pillar - 3 - 2020 - pdf

41) Zaydi,M.,& Nassereddine, B.(2019), "A new comprehensive solution to handle information security governance in organizations , ACM International conference proceeding series part F 1481 , 1-5 , https://doi-org//0-1145-3320326.3320382