نحو دور فاعل للمراجع الداخلى فى إدارة مخاطر الأمن السيبرانى فى الشركات المقيدة بالبورصة المصرية

إعـــــــداد

الأستاذ الدكتور / شحاته السيد شحاته

استاذ المحاسبة والمراجعة

كلية التجارة – جامعة الاسكندرية

١. مقدمة:

تلعب وظيفة المراجعة الداخلية الحديثة Internal Audit Function (IAF) دورًا حيويًا فى تحسين عمليات المنشآت، سواء الهادفة أو غير الهادفة لتحقيق الأرباح، **فضلا عن اعتبارها** بمثابة أحد الركائز الأساسية لحوكمة الشركات، جنبا إلى جنب، مع لجنة المراجعة والإدارة، **وكونها متطلبا ضروريا لتقييم** مختلف الجوانب الرقابية بهذه المنشآت بما يمكنها من تحسين عملياتها وإدارة مخاطرها ERM ومن ثم إضفاء المصداقية والشفافية على ما توصله قوائمها المالية من معلومات (PWC, 2018؛ شحاته، ٢٠٢١)،

وتلبية للحاجة الملحة لمواكبة التغيرات المتسارعة فى بيئة الأعمال والممارسة المهنية الحالية، أشار البعض (PWC, 2018؛ حامد، ٢٠١٩؛ شحاته، ٢٠٢٠)، **لمسايرة وظيفة** المراجعة الداخلية لتلك التغيرات، **من خلال قدرتها على القيام بدوريها** الاستشارى (الذى يستهدف تقديم المشورة والنصح والارشاد لمجالس إدارات الشركات) والتوكيدى (الذى يستهدف تحسين جودة ومحتوى المعلومات المفصح عنها بالتقارير الداخلية لأغراض خدمة متخذى القرارات بصفة عامة، ومجلس الإدارة بصفة خاصة، فى ذلك الصدد). **وذلك فى ثلاثة** مجالات رئيسية، وهى رقابة وإدارة مخاطر وحوكمة أنشطة وعمليات المنشأة.

ومن منظور المنشآت المقيدة بالبورصة تحديدًا فلديها دوافع تبنى العديد من أدوات تكنولوجية المعلومات الحديثة (كأدوات الذكاء الاصطناعى[٢٥] Artificial Intelligence) ورقمنة عملياتها Digitization Process، وهو ما أطلق عليه البعض (Almaleeh, 2019; Khanon, 2020؛ عبدالمنعم، ٢٠٢١) التحول الرقمى[٢٦] Digital Transformation (DT) للشركات، الأمر الذى أدى لوجود العديد

---

[٢٥] **يعتبر الذكاء الاصطناعى، أو ما يعرف بذكاء الآلة**، مصطلح شامل لمختلف التقنيات التكنولوجية التى يمكن استخدامها بمفردها أو بصورة مجتمعة لمحاكاة وتقليد السلوكيات المعرفية لدى الأفراد عند مواجهة المشاكل وتحليلها بصورة منطقية للوصول لحل ملائم لها (كالتعرف على الانماط المختلفة وتتبع النسب المالية الخاصة بالشركة وتحديد مدى التقلبات والانحرافات الملازمة لها) (Almaleeh, 2019; Adiloglu and Gungor, 2019)

[٢٦] **وفقا للبعض** (Mariia and Viktoria, 2020؛ Khanon, 2020؛ عبدالمنعم، ٢٠٢١) **يعرف التحول الرقمى على أنه؛** "عملية تغيير جذرى وتطوير للبنية التحتية لنماذج أداء الأعمال، عن طريق الاعتماد على التقنيات والتطورات التكنولوجية المستحدثة، سواء أكان ذلك بصورة جزئية أو بصورة كلية ، لاكتساب ميزة تنافسية وتحقيق قيمة مضافة والسعى نحو تحقيق الأهداف المرجوة من استراتيجيات الأعمال، بصفة عامة.

من المخاطر المصاحبة لتبنى تلك الأدوات، **التى من أهمها**، مخاطر الأمن السيبرانى Cybersecurity Risk، (Adiloglu and Gungor, 2019; Almaleeh, 2019).

وعليه أصبحت إدارات الشركات القائمة فى ظل بيئة التحول الرقمى (DT)، مقارنة بالفترة ما قبل التحول، **مسئولة بقوة عن تصميم وتنفيذ** وظيفة مراجعة داخلية ذات جودة، **من خلال التزامها** بالممارسات القياسية، **عند القيام بدوريها** الاستشارى والتوكيدى **فى مجالات** رقابة وإدارة مخاطر وحوكمة أنشطة وعمليات الشركة (KPMG, 2020b; Deloitte, 2020) **وذلك مع ضرورة الأخذ فى** الاعتبار لاحتمالية تأثير التداعيات التشغيلية والتنظيمية والمحاسبية للتحول الرقمى على كيفية أداء وظيفة المراجعة الداخلية الحديثة لدوريها، خاصة فى مجال إدارة مخاطر الأمن السيبرانى (KPMG, 2020a; IIA, 2020؛ Aditya *et al.*, 2018) **وهو ما يمكن** أن يؤثر، أيضا، على المردود الإيجابى لتلك الوظيفة ومساهمتها فى مساعدة الشركات على تحقيق أهدافها الحالية والمستقبلية، والحاجة لوجود دور فعال للمراجع الداخلى فى ذلك الصدد.

ونحن نعتقد بوجود ندرة فى الدراسات الأكاديمية والمهنية ذات الصلة بالدور الفاعل للمراجع الداخلى فى إدارة مخاطر الأمن السيبرانى، كأحد أدوار ومجالات وظيفة المراجعة الداخلية الحديثة فى ظل بيئة الأعمال الحالية، لذا ظهرت الحاجة المُلحة لتضييق الفجوة البحثية فى ذلك الصدد. **وعليه فيتضح أن السؤال المحورى**، الأكثر منطقية، **الآن إذا افترضنا** قيام الشركات المقيدة بالبورصة بالتحول الرقمى والاعتماد على التقنيات الحديثة فى مصر، **وبالتبعية حتمية** مواجهتها للعديد من مخاطر الأمن السيبرانى؛ **ما المقصود** بإدارة مخاطر الأمن السيبرانى؟، **وما هو الدور** الفعال للمراجع الداخلى فى إدارة مخاطر الأمن السيبرانى؟، **وأخيرا ما هى متطلبات** تفعيل هذا الدور فى ذلك الصدد؟. **هذا ما نستهدف الإجابة** عليه فى هذه الورقة وفق منهجية بحث تحليلية انتقادية.

وعليه تستهدف هذه الورقة عمل تحليل انتقادى للمصادر العلمية ذات الصلة بالدور الفعال للمراجع الداخلى فى إدارة مخاطر الأمن السيبرانى فى الشركات المقيدة بالبورصة المصرية. **ولذلك سوف تستكمل الورقة بأن تتناول ببعض التفصيل كلا من؛** إدارة مخاطر الأمن السيبرانى من منظور الإصدارات المهنية والدراسات الأكاديمية، الدوران الاستشارى للمراجع الداخلى فى إدارة مخاطر الأمن السيبرانى، متطلبات دعم فاعلية أداء المراجع الداخلى لدوريه فى مجال إدارة مخاطر الأمن السيبرانى، وأخيرا خلاصة الورقة وفرص البحث المحاسبى المستقبلية.

٢. إدارة مخاطر الأمن السيبرانى من منظور الإصدارات المهنية والدراسات الأكاديمية:

أشار البعض (Deloitte, 2018؛ Almaleeh, 2019؛ العيسوى وأبو النضر، ٢٠٢٠؛ Khanom, 2020؛ Mariia and Viktoriia, 2020)، **إلى إمكانية مصاحبة** تبنى الشركات لأدوت التحول الرقمى، (إلى جانب تداعياتها التشغيلية والتنظيمية والمحاسبية[٢٧]) **للعديد من المخاطر** المتعلقة بأمن المعلومات Information Security، و**المعروفة وفقا لبعض** (Deloitte, 2018; Perols, 2019; Badawy, 2021)، **بمخاطر الأمن السيبرانى** Cyber security Risks ، **التى تسلتزم، بصورة حتمية**، من إدارة

[٢٧] **فى ذلك السياق أشارت العديد من الدراسات التى منها (** Adiloglu and Gungor, 2019؛ Khanom, 2020؛ العيسوى وأبو النضر، ٢٠٢٠) **لوجود العديد** من التداعيات الناجمة عن تبنى أدوات التحول الرقمى، **التى من بينها**؛ تحسين كفاءة العمليات التشغيلية، تحسين جودة الخدمات والمنتجات المقدمة، زيادة رضا العملاء، إكتساب ميزة تنافسية، بناء شبكة علاقات قوية بين الشركة وعملاءها وموردیها، الإستجابة الفورية للتغيرات البيئية، التحليل الفورى والمنتظم للبيانات المحاسبية، وتخفيض الوقت اللازم لانجاز المهام والعمليات.

الشركات، تحديدها وتقييمها بشكل أكثر دقة وضرورة العمل على إدارتها للتغلب على (أو على الأقل الحد من) تداعياتها السلبية ماليا ونوعيا.

ويمكن النظر لماهية مخاطر الأمن السيبرانى وفقا للبعض (Perols, 2019; Florakis *et al.*, 2020; Badawy, 2021; Hartmann and Carmenate, 2021)، **على أنها؛ "مجموعة** المخاطر التكنولوجية والتشغيلية والتنظيمية التى تتعرض لها الشركات المستندة على تقنيات تكنولوجيا المعلومات الحديثة، والتى قد تنجم عن اختراق نظام الأمن السيبرانى لديها بما يحد من قدرته على تحقيق أهدافه المرجوة".

كما أنه فى ضوء تحليل الدراسات السابقة (فرج وأخرون، ٢٠١٧؛ على وفرج، ٢٠١٧؛ IIARF, 2018؛ Deloitte, 2018؛ Li *et al.*, 2019؛ Perols, 2019؛ Badawy, 2021؛ Hartmann and Carmenate, 2021) **يمكن تقسيم مخاطر الأمن السيبرانى** لمجموعتين رئيسيتين وهما؛ **مجموعة مخاطر الأداء المرتبطة** بتطبيق أدوات تكنولوجيا المعلومات الحديثة، **التى** تعبر عن فشل تلك الأدوات فى القيام بالمهام المخططة لها وتحقيق الاستفادة المرجوة منها. **ومجموعة المخاطر الأمنية** التى تتضمن ثلاثة مخاطر أساسية وهى؛ **خطر خرقات الحماية المادية** Physical Security Breaches المتعلق باختراق المكونات المادية للبنية التحتية التى تعتمد عليها الشركة فى خدمات تكنولوجيا المعلومات (**كالبحث فى مخلفات البنية التحتية** Dumpster Diving للشركة من أقراص مرنة أو أجهزة خاصة بالشبكات الالكترونية والتى قد تتضمن أى معلومات أو كلمات سر يمكن الاعتماد عليها لإتمام عملية الاختراق، **والتجسس الموجى** Eavesdropping on Emanations الذى يشير لاستخدام أجهزة متخصصة لالتقاط كافة المخرجات اللاسلكية من نظام تكنولوجيا المعلومات كالموجات الصوتية).

و**خطر خرق الحماية المتعلقة بالعاملين** Personnel Security Breaches المرتبط بالمخاطر الداخلية والخارجية المتعلقة بسلوك العاملين داخل الشركة، **مثل؛ قرصنة** البرامج الجاهزة Software Piracy، **إنتهاك** التصريح Authorization Violation (التى تنجم عن ضعف هيكل الرقابة الداخلية)، **الهندسة** الاجتماعية Social Engineering (التى تشير لقيام العاملين بالشركة بإستغلال علاقاتهم وظيفتهم للوصول غير المصرح به للمعلومات)، **واختلاس** المعلومات Hijacking Session).

وأخيرا خطر خرق الحماية المتعلقة بالمعلومات والاتصالات Communications and Information Security Breaches ، **الذى يتضمن؛ هجمات** البيانات Data Attacks (كالنسخ غير المصرح بها من البيانات Unauthorized Copying of Data)، **هجمات** البرامج الجاهزة Software Attacks (كالفيروسات والمصائد والأبواب الخلفية Traps and Back Doors)، **والقنوات** السرية Covert Channels.

كما أشار البعض (Florakis *et al.*, 2020 Hartmann and Carmenate, 2021)، **لانعكاس إختراق نظام الأمن السيبرانى بالشركات**، أيضا، **على العديد من الجوانب، التى منها؛** احتمال ارتكاب الجرائم الالكترونية والتصرفات غير القانونية الإلكترونية، احتمال ارتكاب الغش الإلكترونى، مدى الاستقرار المالى للشركة، مدى قوة الوضع التنافسى للشركة، سمعة الشركة واحتمال تعرضها للدعاوى القضائية. **وهو الأمر الذى يشير لحتمية قيام الشركات بإدارة مخاطر الأمن السيبرانى، حتى يمكن تجنب أثارها السلبية.**

وفى ذلك السياق أشار البعض (Li *et al.*, 2019; Florakis *et al.*, 2020; Badawy, 2021)، **إلى أن مسئولية الإدارة عن نظام الأمن السيبرانى تكمن، فى كل من؛** تحديد أهداف نظام الأمن السيبرانى،

تحديد مخاطر الأمن السيبرانى والإفصاح عنها، تقييم الأثار السلبية لمخاطر الأمن السيبرانى، تصميم وتنفيذ برنامج فعال لإدارة مخاطر الأمن السيبرانى، متضمنا الأساليب الرقابية الفاعلة لضمان تحقيق نظام الأمن السيبرانى لأهدافه، توفير توكيد على مدى فاعلية برنامج إدارة مخاطر الأمن السيبرانى[٢٨].

وعليه فيمكن تعريف برنامج إدارة مخاطر الأمن السيبرانى، وفقا لتتبع الدراسات السابقة التى منها دراسة Badawy (2021)، **على أنه؛ "مجموعة السياسات** والعمليات والأساليب الرقابية، **المصممة لحماية** المعلومات والأنظمة من الهجمات الالكترونية والاختراق الأمنى، و**التى قد تحد من** إمكانية تحقيق نظام الأمن السيبرانى لأهدافه المرجوة، المتمثلة فى الإتاحة والسرية وسلامة البيانات وسلامة العمليات التشغيلية[٢٩]". **وحتى يمكن لإدارة الشركات بناء برنامج فعال لإدارة مخاطر الأمن السيبرانى، يمكن الاستعانة بوظيفة المراجعة الداخلية الحديثة.**

٣. الدوران الاستشارى والتوكيدى للمراجع الداخلى فى مجال إدارة مخاطر الأمن السيبرانى:

تعتبر وظيفة المراجعة الداخلية (IAF) أحد الدعائم الرئيسية لتلبية احتياجات مختلف أصحاب المصالح، خاصة المساهمين والإدارة، **من خلال إعدادها** لتقرير عن مدى فعالية هيكل الرقابة الداخلية (ICS) **وتوفيرها نظرة** أكثر شمولية عن أداء مختلف إدارات وأقسام ومراكز الشركة والمخاطر التى تواجهها، **فضلا عن قدرتها** على متابعة قرارات مجالس الإدارات (PWC, 2018؛ شحاته، ٢٠٢٠). **ونتيجة للطلب** المتنامى على خدمات وظيفة المراجعة الداخلية انعكس ذلك على تطور أدوارها ومجالاتها.

وبدءا بماهية وظيفة المراجعة الداخلية الحديثة، فيمكن تعريفها، **وفقا لما جاء بالإصدار(2017) IIA،** المتسق مع الإصدار IIA (1999)، **والمؤيد من قبل أغلب** الدراسات(Parker and Johnson, 2017؛ PWC, 2018؛ حامد، ٢٠١٩؛ شحاته، ٢٠٢٠)، **بأنها** "نشاط توكيدى واستشارى مستقل وموضوعى مصمم

---

[٢٨] **فى ذلك السياق اشارت دراسة Badawy (2021)** إلى أنه حتى يمكن بناء برنامج فعال لإدارة مخاطر الأمن السيبرانى، **يجب أن يمر بعدة مراحل أساسية، وهى؛ التحديد الدقيق** لمخاطر الأمن السيبرانى وأولوية تعرض الشركة لكل منها، **تصميم نظام** للرقابة على الأمن السيبرانى متضمنا معايير وأسس واضحة للرقابة، **اختبار مدى فاعلية** نظام الرقابة على نظام الأمن السيبرانى، **إعداد تقريرى** للافصاح عن مخاطر الأمن السيبرانى وإدارة مخاطره، **وأخيرا توفير توكيد** مهنى على تقريرى الإدارة بشأن الإفصاح عن مخاطر الأمن السيبرانى وإدارة تلك المخاطر.

[٢٩] **وفقا لدراسة Badawy (2021)** يتم وضع برنامج إدارة مخاطر الأمن السيبرانى من قبل الإدارة العليا للشركة **بما يحقق عدة أهداف أساسية وهى؛ الإتاحة** Availability (التى تشير لإمكانية الوصول المستمر للمعلومات ووقتية الحصول عليها وإمكانية الاعتماد عليها فضلا عن دعم النظم التكنولوجية لمختلف العمليات التشغيلية)، **السرية** Confidentiality (التى تشير لحماية المعلومات ضد الاختراق والهجمات الالكترونية المتكررة والوصول غير المصرح به، بما فى ذلك حماية سرية وخصوصية المعلومات الشخصية لكافة المتعاملين مع الشركة)، **سلامة البيانات** Integrity of Data (التى تشير لحماية البيانات ضد الاختلاس أو التعديل أو التلف)، **وسلامة العمليات التشغيلية (المعالجة)** Integrity of Process (التى تشير لحماية العمليات التشغيلية من الاستخدام غير السليم أو التعديل أو التدمير لنظام تكنولوجيا المعلومات بصورة جزئية أو كلية)

لإضافة قيمة للوحدة لتحسين عملياتها، وهو يساعد الوحدة على تحقيق أهدافها بإيجاد منهج منظم وقوى لتقييم وتحسين كفاءة وفعالية عمليات إدارة المخاطر والرقابة والحوكمة"[٣٠].

ونحن نرى قدرة ذلك التعريف على تقديم صورة ورؤية جديدة لوظيفة المراجعة الداخلية نظرا لتحولها من مجرد التركيز على الرقابة والمساءلة المالية إلى التركيز على تحسين عمليات الشركات، وتحقيق قيمة مضافة لها، فضلا عن اعتبارها مسئولية الإدارة، فى المقام الأول، وامتداد نطاقها ليتضمن مختلف النواحى التشغيلية إلى جانب كافة النواحى المالية والمحاسبية، من خلال تقديمها نوعين من الخدمات فى ثلاثة مجالات، تساعد على تحقيق أهداف الشركات والعمل على خلق فرص تنافسية وضمان تحقيق الشفافية وزيادة وعى الإدارة العليا والعاملين بمهام وأدوار وظيفة المراجعة الداخلية الحديثة[٣١].

أما فيما يتعلق بمصفوفة أدوار ومجالات وظيفة المراجعة الداخلية الحديثة، فقد أشار البعض (على وشحاته، ٢٠١٨؛ PWC, 2018؛ حامد، ٢٠١٩) إلى أنه بناء على تعريف تلك الوظيفة، الصادر عن IIA (2017)، **فإنها تقوم بدورين** توكيدي Assurance وإستشارى Consulting[٣٢]، **وذلك فى ثلاثة مجالات**

---

[٣٠] أشار البعض (على وشحاته، ٢٠١٨؛ حامد، ٢٠١٩؛ شحاته، ٢٠٢٠) إلى مرور الاهتمام المهنى بالمراجعة الداخلية بأربع فترات زمنية رئيسية، والتى تزامنت جنبا إلى جنب مع التطورات فى هيكل الرقابة الداخلية، **فتتمثل المرحلة الأولى فى الفترة (١٩٠٠-١٩٤١)** وفيها تم إنشاء قسم منفصل لوظيفة المراجعة الداخلية، لأول مرة، بهدف تتبع مراجعة العمليات المالية والمحاسبية، **كما جاءت المرحلة الثانية خلال الفترة (١٩٤١- ١٩٧٧)** فيها تم الاعتراف بالمراجعة الداخلية، كمهنة، من خلال إنشاء معهد المراجعين الداخليين Institute of Internal Auditors (IIA) (الذى أشار لضرورة وجود معايير مهنية لممارستها وقواعد للسلوك المهنى مع ضرورة التعلم والتدريب المهنى المستمر لممارسيها). **وفى عام ١٩٤٧ قدم (IIA)**، تعريفا للمراجعة الداخلية على أنها " نشاط تقييمى مستقل يتم داخل الوحدة بقصد مراجعة العمليات كأساس لتقديم خدمات وقائية وبناءة للإدارة. **ونتيجة للتطور فى بيئة الأعمال، جاءت المرحلة الثالثة خلال الفترة (١٩٧٧-١٩٨٧)، التى قام فيها (IIA)** بتشكيل لجان لتطوير الإطار المتكامل لمعايير الأداء المهنى للمراجعة الداخلية، **فضلا عن قيامه فى ١٩٧١، بتعديل تعريفه للمراجعة الداخلية ليصبح** "نشاط تقييمى مستقل داخل الوحدة لمراجعة عملياتها بقصد تقديم الخدمات للإدارة " **(أى أنها بمثابة جزء** من نظام الرقابة المالية يعمل على قياس وتقييم فعالية نظم الرقابة الأخرى، ويهتم بتقييم عمليات الوحدة ككل). **وأخيرا تتمثل المرحلة الرابعة، والأخيرة، فى الفترة ما بعد عام (١٩٨٧)** وحتى الآن، وفيما امتد نطاق المراجعة الداخلية ليشمل تحسين عمليات الوحدة وإضافة قيمة لها، **فضلا عن تقديم (IIA) تعريف المراجعة الداخلية الحديثة عام (١٩٩٩)، والذى سيتم الاستناد عليه بورقة العمل الحالية.**

[٣١] **فى ذلك السياق أشار البعض** (على وشحاته، ٢٠١٨؛ شحاته، ٢٠٢٠) **لضرورة التزام القائم بوظيفة المراجعة الداخلية** بمجموعة من معايير الممارسة المهنية، والتى تنقسم إلى؛ **مجموعة معايير الصفات** Attribute Standards **التى** تعبر عن الصفات الواجب توافرها فى مؤدى وظيفة المراجعة الداخلية وأقسام المراجعة الداخلية **(**كالهدف والسلطة والمسئولية، والاستقلال والموضوعية)، **ومجموعة معايير الأداء** Performance Standards التى تتعلق بعملية تنفيذ كل عملية أو مهمة من عمليات أو مهام المراجعة الداخلية (كإدارة نشاط المراجعة الداخلية، طبيعة العمل، وتخطيط أعمال التكليف)

[٣٢] **وفقا للبعض** (Arens *et al.*, 2016؛ على وشحاته، ٢٠١٨؛ حامد، ٢٠١٩؛ ISAE No. 3000) **يمكن تعريف الدور التوكيدي لوظيفة المراجعة الداخلية**، الذى يعبر عن أداء القائم بتلك الوظيفة بخدمات توكيدية Assurance Services، **على أنه "علاقة ثلاثية** الأطراف بين موفر المعلومة ومن يضفى الثقة والصدق على هذه المعلومة ومن يعتمد على هذه المعلومات فى اتخاذ القرار"، **كما يحدد المراجع الداخلى** طبيعة ونطاق التوكيد ويقوم بالتقييم الموضوعى للأدلة المتحصل عليها، حتى يمكنه الوصول لرأى مستقل، أو تكوين إستنتاج بشأن عملية أو نظام محدد. **بينما يعرف الدور الاستشارى لوظيفة المراجعة الداخلية**، الذى يعبر عن أداء القائم بتلك الوظيفة بخدمات استشارية Consulting Services، **على أنه "علاقة ثنائية** الأطراف بين مقدم الخدمة ومتلقى الخدمة وذلك لإسداء النصح للإدارة"، **وفيها يقوم المراجع الداخلى** بتنفيذ تلك الخدمات وتحديد طبيعتها ونطاقها بناء على طلب الإدارة وبالاتفاق معها. **كما أشارت دراسة** حامد (٢٠١٩) **إلى وجود ثلاثة أنماط** (أشكال) للخدمات الاستشارية، **حيث يستهدف النمط الأول** تحديد المشاكل التى تواجه عمليات التشغيل وأسباب حدوث تلك المشاكل ومن ثم تقديم الحلول الملائمة للقضاء عليها، **بينما يستهدف النمط الثانى** توفير الأساس والإجراءات المعيارية بشأن أى عملية داخل الوحدة الاقتصادية لمساعدة العاملين على أداء وظائفهم، **وأخيرا يستهدف النمط الثالث** توفير مختلف المعلومات بشأن الإدارة المالية وإدارة المخاطر والرقابة الداخلية من خلال الدورات وورش العمل.

رئيسية هى الرقابة الداخلية وإدارة المخاطر وحوكمة الشركات[٣٣]. **واتساقا مع الهدف من هذه الورقة البحثية سيتم التركيز على هذين الدورين لوظيفة المراجعة الداخلية فى مجال إدارة مخاطر الأمن السيبرانى.**

وبدءا بماهية عملية إدارة المخاطر[٣٤] (ERM)، **فيمكن تعريفها، وفقا للإصدار COSO (2018)**، المتسق مع الإصدار COSO (2013)، **على أنها "عملية يتم تنفيذها** بواسطة مجلس الإدارة، والإدارة، والموظفين الآخرين، وتطبيقها فى استراتيجية الوحدة الاقتصادية، وتكون مصممة لتحديد الأحداث المحتملة، التى تواجه الوحدة وتؤثر عليها، وذلك لتدنية أثارها لمستوى مقبول ومن ثم توفير توكيد معقول بشأن تحقيق أهداف الوحدة الاقتصادية"[٣٥].

أما فيما يتعلق بالدورين الاستشارى والتوكيدى لوظيفة المراجعة الداخلية الحديثة فى مجال إدارة مخاطر[٣٦] **الأمن السيبرانى، فيتضح من تحليل** الإصدارات والدراسات السابقة (IIA, 2009; Mihret

---

[٣٣] **يعرف هيكل الرقابة الداخلية (ICS) وفقا للإصدار COSO (2018)، على أنه "**عملية متكاملة تتأثر بالعديد من الأطراف، مجلس الإدارة والإدارة والعاملين، وتتكون من سلسلة من الإجراءات والعمليات التى يتم تصميمها لتوفير توكيد معقول وليس مطلقاً، بشأن؛ إمكانية الاعتماد على التقارير المالية، كفاءة وفعالية كافة العمليات التشغيلية، والالتزام بالقوانين واللوائح ذات الصلة بالوحدة. **ذلك بالإضافة لإنطواء ذلك الهيكل على خمس مكونات رئيسية؛** بيئة الرقابة، أنشطة الرقابة، تقييم المخاطر، المعلومات والاتصال، والمتابعة. **كما تعرف حوكمة الشركات Corporate Governance وفقا لـ IIA (2013)** على أنها "العمليات التى تتم من خلال إجراءات تستخدم من قبل ممثلى أصحاب المصالح وذلك لإدارة المخاطر والرقابة عليها والتأكد من كفاية أساليب الرقابة لتجنب هذه المخاطر بما يساهم فى تحقيق أهداف وخطط الوحدة الاقتصادية". **كما أشارت دراسة** على وشحاته (٢٠١٨) لوجود نوعين من آليات الحوكمة، **حيث يختص النوع الأول** بالوحدة الاقتصادية ذاتها، ويشمل آليات تحقيق الرقابة على أداء الطرف الأول "الإدارة" (مثل؛ قوة إدارة المراجعة الداخلية، مدى الالتزام بتطبيق المعايير)، **بينما يختص النوع الثانى** بمراقب الحسابات، ويشمل آليات تحقق الرقابة على أداء الطرف الثانى "مراقب الحسابات" (مثل؛ التدوير الالزامى لمراقب الحسابات).

[٣٤] **يتضح من تحليل مختلف إصدارات لجنة COSO**، إضافة (2014) COSO **وتبعه فى ذلك** (COSO, 2017; COSO, 2018)، **إستجابة للاهتمام** بإدارة المخاطر (ERM)، **ثلاثة مكونات إضافية** لهيكل الرقابة الداخلية (ICS) إلى جانب مكوناته وفقا للإصدار(2013) COSO، المتسق مع الاصدار (1992) COSO، وهى؛ وضع الاهداف Objective Setting، تحديد (توصيف) الحدث Event Identification، رد فعل الإدارة تجاه المخاطر (الاستجابة للمخاطر) Risk Response. **كما** يتضح للباحث أيضا **تقنين الإصدار COSO (2013) لسبعة عشر مبدأ** لدعم المكونات الرئيسية لهيكل الرقابة الداخلية للعمل بصورة متكاملة ومدعمة لبعضها البعض. **وقد تطورت تلك المبادئ** حتى وصلت لعشرين مبدأ وفقا للإصدار (2017) COSO.

[٣٥] **على نفس النحو أوضح** IIA (2009) **إمكانية تعريف عملية إدارة المخاطر على أنها "** عملية متنظمة ومتناسقة ومتكاملة تطبق على مستوى الوحدة الاقتصادية لتحديد كيفية الاستجابة والتقرير عن الفرص والتهديدات التى تؤثر على تحقيق أهداف الوحدة الاقتصادية". **كما يعتقد الباحث باعتبار تعريف إدارة المخاطر وفقا للإصدار(2018) COSO تعريف أكثر شمولية للتحقق من ماهية (ERM) نظرا لتحديده القائم بها والهدف منها وموقعها فى رؤية ورسالة الوحدة الاقتصادية، مقارنة بتعريف IIA (2009)، لذا فسوف نتبنى تعريف COSO (2018) للتعبير عن (ERM).**

[٣٦] **إلى جانب قيام وظيفة المراجعة** الداخلية، بدوريها الاستشارى والتوكيدى فى مجال إدارة مخاطر أنشطة وعمليات الشركة، **أشار** حامد (٢٠١٩) وشحاته (٢٠٢٠) **إلى ضرورة قيام مدير إدارة المراجعة الداخلية** بدوريين، فى ذلك الصدد، وهما؛ **الأدوار الرئيسية لوظيفة المراجعة الداخلية Core Internal Audit Roles** (كمراجعة إدارة المخاطر وتوفير توكيد عن مدى صحة عملية تقييم المخاطر وإدارتها) **والأدوار المسموح بأدنها من قبل وظيفة المراجعة الداخلية Legitimate Internal Audit Roles** (كالحفاظ على تطوير عملية إدارة المخاطر وتدريب الإدارة على كيفية الاستجابة للمخاطر).

IIARF, 2018 ؛and Grant, 2017; Shahimi and Mahzan, 2018; Aditya *et al.*, 2018؛ على وشـــحاته، ٢٠١٨؛ حامد، ٢٠١٩؛ Li *et al.*, 2019؛ شـــحاته، ٢٠٢٠؛ Florakis *et al.*, 2020؛ Badawy, 2021؛ شـــحاته، ٢٠٢١) **إمكانية بلورة الدور الاســـتشـــارى** فى مجال إدارة مخاطر الأمن السيبرانى بأنشطة وعمليات الشركة، **والذى يرتكز** فى **الأساس على** قيام مدير إدارة المراجعة الداخلية **بتقديم النصح** لمجلس الإدارة بصدد تحديد وتوصيف وقياس مخاطر الأمن السيبرانى المحيطة ببيئة عمل الشركة التكنولوجية **وكيفية مواجهتها** وتفادى أثارها على تحقيق الشركة لأهدافها المرجوة.

ويتم تقديم الإستشارة والنصح بالعديد من النواحى، التى من منها؛ **القيام بالتحديث والمتابعة** الدورية لمختلف مخاطر الأمن السيبرانى، **فضـلا عن وضـع وتطوير الإطار** المسـتند عليه فى عملية إدارة مخاطر الأمن السـيبرانى، **مسـاعدة إدارة الشـركة فى وضـع** توصـيات للإدارة بشـأن كل من الحد الادنى المقبول لمستوى مخاطر الأمن السيبرانى وكيفية تحسين عمليات إدارة المخاطر فى ذلك الصدد، والمقترحات اللازمة لمواجهة مخاطر الأمن السيبرانى وتفاديها والاستجابة السريعة لها.

ذلك بالإضـافة إلى **تقديم المشـورة بشـأن؛ تحديد إدارة الشـركة** أفضـل طرق تحقيق أهدافها فى ظل مخاطر الأمن السـيبرانى الملازمة لتبنى الأدوات التكنولوجية ببيئة عمل الشـركة والمسـاعدة على تحديد احتمال تحقق تلك المخاطر، **تحديد وتنظيم** الدورات اللازمة للتعامل الكفء مع مخاطر الأمن السـيبرانى خاصـة فى ظل اعتبارها مخاطر مسـتحدثة وملازمة للتحول الرقمى، **وأخيرًا كيفية تطوير وتنمية الاستراتيجيات** المتبعة لإدارة مخاطر الأمن السيبرانى.

كما يمكن، أيضـا، بلورة الدور التوكيدى فى مجال إدارة مخاطر الأمن السـيبرانى، والذى يرتكز فى الأسـاس على قيام مدير إدارة المراجعة الداخلية بتقديم تقرير باسـتنتاج Conclusion بشـأن مدى صـدق التقارير المعدة من قبل المسئولين عن إدارة مخاطر الأمن السيبرانى بالشـركة، **فى توفير المراجع الداخلى استنتاج** بالعديد من النواحى **والتى منها؛ التقرير عن مدى** فاعلية تصميم وتشغيل عملية إدارة مخاطر الأمن السيبرانى، **التقارير المعدة من** قبل المسئولين عن عملية إدارة مخاطر الأمن السيبرانى (كالتقرير عن كيفية تحديد وتقييم وإدارة مخاطر الأمن السـيبرانى الجوهرية، والتقرير عن كيفية تحديد وتقييم وإدارة مخاطر الأعمال الرئيسية خاصة فيما يتعلق بالأمن السيبرانى)، **التقرير عن مدى** تنفيذ الاستراتيجيات الموضوعة لإدارة مخاطر الأمن السـيبرانى التى حدثت بالفعل، **وأخيرا التقرير عن** تحديد وتقييم مخاطر عدم وفاء الشركة بمتطلبات الالتزاماتها التعاقدية خاصة فيما يتعلق بالعقود الذكية فى ظل بيئة التحول الرقمى[٣٧].

---

[٣٧] **على نفس النحو أشار** (IIA, 2009؛ حامد، ٢٠١٩) **إلى ضرورة قيام المراجع الداخلى بالإدوار الرئيسية** Core Internal Audit Roles فى مجال إدارة المخاطر(**التى منها**؛ مراجعة إدارة المخاطر، تقييم عملية الافصاح عن المخاطر، تقييم عملية إدارة المخاطر، وتوفير توكيد عن مدى صحة عملية تقييم المخاطر وإدراتها)، **وكذلك القيام بالأدوار المسموح أدائها (المشروعة)** Legitimate Internal Audit Roles فى مجال إدارة المخاطر (**التى منها**؛ الحفاظ على تطوير عملية إدارة المخاطر، دعم إنشاء إدارة المخاطر، التنسيق بين أنشطة إدارة المخاطر، تدريب الإدارة على كيفية الاستجابة للمخاطر، والمساعدة فى تحديد وتقييم المخاطر) **ذلك بالإضافة لعدم قيام المراجع الداخلى بالأدوار التى لا ينبغى أن يقوم** بها Role that Internal Auditing Should not Undertake، فى مجال إدارة المخاطر (**التى منها**؛ تحديد قدرة الوحدة الاقتصادية على تحمل المخاطر، واتخاذ القرارات بشأن الاستجابة للمخاطر نيابة أو بديلا عن الإدارة والمساءلة عن إدارة المخاطر) **نظرا لانعكاسها** سلبا على موضوعيته واستقلاليته.

٤. متطلبات دعم فاعلية المراجع الداخلى فى إدارة مخاطر الأمن السيبرانى:

وفقا لتحليل الدراسات السابقة التى منها (Aditya *et al.*, 2018; Shahimi and Mahzan, 2018; IIARF, 2018; Li *et al.*, 2019; Flotakis *et al.*, 2020; Badawy, ٢٠٢٠؛ شحاته، 2021، فإننا نعتقد بأن هناك مجموعة من متطلبات دعم الدور الفاعل للمراجع الداخلى فى إدارة مخاطر الأمن السيبرانى فى مصر، **أهمها ما يلى:**

أ- **إرتقاء إدارات الشركات بثقافة النظر للمراجعة الداخلية كوظيفة مضيفة للقيمة:**

وذلك من خلال توفير الاستقلال التنظيمى لها، وتحدد حقوق وواجبات ومسئوليات المراجعين الداخليين بالشركات، **الأمر الذى** قد ينعكس على تدنية مستوى فجوة التوقعات فى المراجعة الداخلية، خاصة فجوة المعقولية، ويمكن المراجعين الداخليين من الأداء الأكثر فاعلية للأدوار والمسئوليات الملقاة على عاتقهم. **وكذلك تحديث اللوائح** المالية والإدارية والخريطة التنظيمية، بما يساعد على تفعيل عملية التفتيش على مدى وفاء وأداء المراجعين الداخليين لأدوارهم ومسئولياتهم الحالية والمستحدثة فى ظل بيئة التحول الرقمى للشركات. والتنسيق بين لجنة المراجعة وإدارة المراجعة الداخلية، ودعم الإدارة التكنولوجى والبشرى لإدارات المراجعة الداخلية وكذا التواصل مع التنظيم المهنى لوظيفة المراجعة الداخلية.

ب- تنظيم مهنة المراجعة الداخلية:

لأن إنشاء تنظيم مهنى للمراجعة الداخلية الحديثة سوف ينظم ويشرف على عمل المراجعين الداخليين، ويرخص لهم، ويحاسبهم أخلاقيا، وينمى قدراتهم العملية والعلمية بإستمرار، خاصة فى مجال تكنولوجيا المعلومات والتطورات المتلاحقة ببيئة الأعمال الحالية. **فضلا عن قدرة ذلك التنظيم على** إصدار الإرشادات والضوابط المهنية اللازمة للارتقاء بجودة المهنة[٣٨] ومستوى الكفاءة المهنية خاصة فى ظل الأدوار والمسئوليات المستحدثة فى بيئة التحول الرقمى للشركات, **على** أن يشترط ذلك التنظيم حصول المراجعين الداخليين على رخصة معتمدة منه. **وضع وتنفيذ ومتابعة برامج التنمية المهنية للمراجعين الداخليين،** تأخذ فى الاعتبار متغيرات بيئة تكنولوجيا المعلومات مثل إدارة مخاطر الأمن السيبرانى.

جـ - تطوير نظام التعليم المحاسبى:

وذلك من خلال إعادة النظر في برامج التعليم المحاسبي الرقمى وكذلك برامج التعليم المهنى المستمر، وتطعيمها **بمقررات ملائمة ذات صلة بالأدوار** والمسئوليات الحالية والمستحدثة، **التى تقع** على عاتق المراجعين الداخليين فى ظل بيئة التحول الرقمى، **وكيفية الإستفادة القصوى من** تقنيات تكنولوجيا المعلومات الحديثة وتجنب المخاطر الملازمة لها والعمل على إدارتها والوصول بها لمستواها المقبول. **فضلا عن** تضمين الخطة البحثية لأقسام المحاسبة بمختلف الجامعات إجراء بحوث ميدانية بشأن مشاكل الممارسة المهنية للمراجعين الداخليين فى ظل تبنى الشركات لأدوات التحول الرقمى، **وحتمية** إضطلاعها بإدارة مخاطر الأمن السيبرانى.

---

[٣٨] **أشارت دراسة** شحاته (٢٠٢٠) **لإمكانية تعريف جودة وظيفة المراجعة الداخلية (جودة مهنة المراجعة الداخلية فى ظل وجود تنظيم مهنى لها)، على أنها؛ قدرة المراجع الداخلى** على الالتزام بالممارسات القياسية، **لدورى وظيفة** المراجعة الداخلية التوكيدى والاستشارى، **لتحسين** عمليات الشركة وإيجاد منهج منتظم وقوى لتقييم وتحسين كفاءة وفعالية ، عمليات إدارة المخاطر والرقابة والحوكمة، **وذلك فى ضوء** التزامه بمعايير الممارسة المهنية وقواعدوآداب وسلوكيات مهنة المراجعة الداخلية.

د- تنظيم وتفعيل الإفصاح عن جودة وظيفة المراجعة الداخلية:

التي تشمل الإفصاح عن جودة وظيفة المراجعة الداخلية لأصحاب المصالح، خاصة المستثمرين، كما تزداد الحاجة لتطوير قواعد القيد والشطب بحيث تلزم الشركات بذلك خاصة فى ظل بيئة التحول الرقمى ومخاطر الأمن السيبرانى.

٥. خلاصة الورقة وفرص البحث المستقبلية:

استهدفت الورقة عمل تحليل إنتقادى للمصارد العليمة ذات الصلة بالدور الفعال للمراجع الداخلى فى إدارة مخاطر الأمن السيبرانى. **وفى ذلك الشأن خلصنا لإمكانية تعريف مخاطر الأمن السيبرانى، على أنها؛ "مجموعة** المخاطر التكنولوجية والتشغيلية والتنظيمية التى تتعرض لها الشركات المستندة على تقنيات تكنولوجيا المعلومات الحديثة، والتى قد تنجم عن اختراق نظام الأمن السيبرانى لديها بما يحد من قدرته على تحقيق أهدافه المرجوة". **والتى قد تنجم عن مجموعتين** من المخاطر (مخاطر الأداء المرتبطة بتطبيق أدوات تكنولوجيا المعلومات الحديثة والمخاطر الأمنية) وتستلزم وجود برنامج فعال لإداراتها.

فضلا عن إمكانية تعريف برنامج إدارة مخاطر الأمن السيبرانى، على أنه؛ "مجموعة السياسات والعمليات والأساليب الرقابية، **المصممة لحماية** المعلومات والأنظمة من الهجمات الالكترونية والاختراق الأمنى، **التى قد تحد من** إمكانية تحقيق نظام الأمن السيبرانى لأهدافه المرجوة، المتمثلة فى الإتاحة والسرية وسلامة البيانات وسلامة العمليات التشغيلية.

أما فيما يتعلق بالدورين الاستشارى والتوكيدى للمراجع الداخلى فى إدارة مخاطر الأمن السيبرانى، ووفقا لمسئولية الإدارة فى ذلك الشأن، فيمكن **بلورة الدور الاستشارى** فى مجال إدارة مخاطر الأمن السيبرانى، فى تقديم الاستشارة والنصح بالعديد من النواحى، التى منها؛ **القيام بالتحديث والمتابعة** الدورية لمختلف مخاطر الأمن السيبرانى، و**مساعدة إدارة الشركة فى وضع** توصيات للإدارة بشأن كل من الحد الادنى المقبول لمستوى مخاطر الأمن السيبرانى وكيفية تحسين عمليات إدارة المخاطر فى ذلك الصدد.

كما يمكن، أيضا، بلورة الدور التوكيدى فى مجال إدارة مخاطر الأمن السيبرانى، بصفة خاصة، فى توفير المراجع الداخلى استنتاج بالعديد من النواحى **التى منها؛ التقرير عن مدى** فاعلية تصميم وتشغيل عملية إدارة مخاطر الأمن السيبرانى، **التقارير المعدة من** قبل المسئولين عن عملية إدارة مخاطر الأمن السيبرانى، و**التقرير عن مدى** تنفيذ الاستراتيجيات الموضوعة لإدارة مخاطر الأمن السيبرانى التى حدثت بالفعل.

وأخيرا خلصت الورقة لوجود مجموعة من متطلبات دعم الدور الفاعل للمراجع الداخلى فى إدارة مخاطر الأمن السيبرانى أهمها؛ إرتقاء إدارات الشركات بثقافة النظر للمراجعة الداخلية كوظيفة مضيفة للقيمة، تنظيم مهنة المراجعة الداخلية، تطوير نظام التعليم المحاسبى، وتنظيم وتفعيل الافصاح عن جودة وظيفة المراجعة الداخلية.

وختاما فإننا نعتقد بأهمية اتجاه البحث المحاسبى فى مصر مستقبلا نحو المجالات التالية؛ إطار مقترح لاسناد وظيفة المراجعة الداخلية بدوريها الاستشارى والتوكيدى فى مجال إدارة مخاطر الأمن السيبرانى فى الوحدات الصغيرة ومتوسطة الحجم- دراسة تجريبية، اختبار العلاقة بين تقنية سلاسل الكتل وفاعلية هيكل الرقابة الداخلية بالشركات- دراسة تجريبية، أثر تبنى أدوات الذكاء الاصطناعى على جودة أداء وظيفة المراجعة الداخلية- دراسة تجريبية.

قائمة المراجع

المراجع العربية:

إبراهيم، السيد زكريا. ٢٠٢١. أثر استخدام تكنولوجيا سلاسل الكتل Block Chain على البيئة المحاسبية فى مصـــر- دراســـة نظرية ميدانية. **بحث غير منشـــور مقدم للمؤتمر العلمى الرابع لقســـم المحاســـبة والمراجعة**، كلية التجارة، جامعة الإسكندرية.

العيسوى، عبدالحميد وأيمن أبو النضـر. ٢٠٢٠. إنعكاسات التطورات التكنولوجية فى مجال سلاسل الكتل على أنشـطة ومهنة المراجعة مع دراسـة إسـتكشـافية فى البيئة المصـرية. ***مجلة الإسـكندرية للبحوث المحاسبية***، كلية التجارة، جامعة الإسكندرية، ٣(٤): ١-٩١.

حامد، سحر سعيد. ٢٠١٩. **أثر الإسناد والتوقيت والوضع الوظيفى للمراجعة الداخلية على قرار المراجع الخارجى بشـــأن مدى اعتماده على وظيفة المراجعة الداخلية- دراســـة تجريبية.** رســـالة دكتوراة غير منشورة، قسم المحاسبة والمراجعة، كلية التجارة جامعة دمهنور.

شحاته، السيد شحاته. ٢٠٢٠. إطار مقترح لإسناد وظيفة المراجعة الداخلية بدوريها الاستشارى والتوكيدى فى مجال إدارة المخاطر فى الوحدات الصغيرة ومتوسطة الحجم. ***المجلة العلمية التجارة والتمويل***، كلية التجارة، جامعة طنطا، ٤٠: ١٠٩-١٢٨

_____. ٢٠٢١. مصـــفوفة أدوار ومجالات المراجعة الداخلية الحديثة فى ظل جائحة كورونا. ***المجلة العلمية التجارة والتمويل***، كلية التجارة، جامعة طنطا، ١: ١-١٨.

عبدالمنعم، يوســـف طه. ٢٠٢١. التحول الرقمى على مهنة المحاســـبة والمراجعة فى ظل فيروس كورونا المسـتجد كوفيد ١٩ باسـتخدام برمجيات تخطيط موارد المؤسـسـات. **بحث غير منشـور مقدم للمؤتمر العلمى الرابع لقسم المحاسبة والمراجعة**، كلية التجارة، جامعة الإسكندرية.

على، عبد الوهاب نصـــر وشـــحاته الســـيد شـــحاته. ٢٠١٨. **الرقابة والمراجعة الداخلية الحديثة (مدخل الإستدامة وإدارة المخاطر وكشف الغش).** دار التعليم الجامعى- الإسكندرية.

_____ وهـانى خليـل فرج. ٢٠١٧. **مراجعـة النظم الالكترونيـة وفقـا لمعـايير المراجعـة الدولية.** دار الجامعين للطباعة والتجليد- الإسكندرية.

فرج، هانى خليل ودعاء حافظ إمام ومحمد فورى محمد وحســـام محمد. ٢٠١٧. **المراجعة الإلكترونية (الأثار- التحديات- التطبيقات).** دار التعليم الجامعى للطباعة والنشر- الإسكندرية

المراجع الأجنبية:

Adiloglu, B., and N. Gungor. 2019. Investigation of Increasing Technology use and Digitalization in Auditing. ***Global Business Research Congress (GBRC),*** 9: 20-23.

Aditya, B. R., R. Hartanto, and L. E. Nugroho. 2018. The role of IT Audit in the Era of Digital Transformation. **International Conference on Information, Engineering, Science and Technology (INCITEST),** Bandung, Indonesia.

Almaleeh, N. M. S. 2019. The Impact of Digital Transformation on Audit Quality: Exploratory Findings from a Delphi Study. Available at: www.sisc.journal.ekb.eg.

Arens, A. A., R. J. Elder, and M. S. Beasley. 2016. **Auditing and Assurance Services: An Integrated Approach 14th Edition**. Upper Saddle River, NJ: Prentice- Hall

Babayeva, A., and N. D. Manousaridis. 2020. The Effect of Digitalization on Auditing- A Study Investigating the Benefits and Challenges of Digitalization on the Audit Profession. Available at: *www.lup.lub.lu.sc.*

Badawy, H. A. 2021. The Impact of Assourance Quality and Level on Cybersecurity Risk Management Program on Non-Professional Egyptian Investors' Decisions: An Experimental Study. ***Alexandria Journal of Accounting Research*** 5(3): 1-56.

Committee of Sponsoring Organization of the Tradeway Commission (COSO). 1992. **Internal Control- Integrated Framework.** New Jersey, COSO. Available at: *www.coso.org.*

_____.

2004. **Enterprise Risk Management Integrated Framework**. New Jersey, COSO. Available at: *www.coso.org.*

_____.

2005**. Internal Control- Integrated Framework**: **Guidance for Smaller Public Companies Reporting on Internal Control over Financial Reporting**. New Jersey, COSO. Available at: *www.coso.org*

_____.

2013. **Internal Control – Integrated frame Work**, Executive Summary. New Jersey, COSO. Available at: *www.coso.org.*

Committee of Sponsoring Organization of the Tradeway Commission (COSO). 2014. **Improving Organizational Performance and Governance.** New Jersey, COSO. Available at: *www.coso.org.*

_____.

2015. **Leveraging COSO Across the Three Lines of Defense.** New Jersey, COSO. Available at: *www.coso.org.*

_____.

2017. **Enterprise Risk Management Integrating With Strategy and Performance.** New Jersey, COSO. Available at: *www.coso.org.*

_____.

2018. **Enterprise Risk Management Applying enterprise risk management to environmental, Social and Governance related Risks.** New Jersey, COSO. Available at: *www.coso.org*

Deloitte. 2020. Accounting Considerations Related to Coronavirus Disease 2019. Available at: *www.deloitte.com*.

Florakis, C., C. Louca, R. Michaely, and M. Weber. 2020. Cybersecurity Risk. Available at: *http://ssrn.com*

Hartmann, C. C., and J. Carmenate. 2021. Academic Research on the Role of Corporate Governance and IT Expertise in Addressing Cybersecurity Breaches: Implications for Practice, Policy, and Research. ***American Accounting Association*** 15(2): A9-423.

Khanom, T. 2020. The Accountancy Profession in the Age of Digital Transformation: Challenges and Opportunities. ***International Journal of Creative Research Thoughts (IJCRT)*** 8(2).

KPMG. 2020a. COVID-19 Role of Internal Audit Leaders. Available at: *www.hpmg.com*

_____. 2020b. COVID-19: The Impact on Internal Audit. Available at: *www.hpmg.com*

Li, H., W. G. No., and T. Wang. 2018.SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. ***International Journal of Accounting Information Systems*** 30:40-55.

Marria, N., and M. Viktoriia. 2020. Digitalization of Audit in the Condition of the COVID-19. Available at: *www.researchgate.net.*

Mihret, D. G., and B. Grant. 2017. The role of Internal Auditing on Corporate Governance: A foucauldian Analysis. **Accounting, Auditing & Accountability Journal** 30(3): 699-719

Parker, S., and L. A. Johnson. 2017. The development of Internal Auditing as a profession in the US during the twentieth Century. ***Accounting Historians Journal*** 44(2): 47-67.

PWC. 2018. **Internal Audit.** Available at: *www.pwc.org.*

Shahimi , S., and N. Mahzan. 2018. Building a research model and hypotheses development and findings of Exploratory Interviews. ***International Journal of Management Excellence*** 10(2): 1257-1283.

The Institute of Internal Auditors Research Foundation (IIARF). 2018. **The Future of Cybersecurity in Internal Audit.** Available at: *www.iiarf.org.*

The Institute on Internal Auditors (IIA). 2009. **IIA position Paper: the role of internal Auditing in enterprise-wide risk Management.** Available at: *www.na.theiia.org.*

_____. 2013. **Corporate Governance- Strategies for internal Audit.** Available at: *www.na.theiia.org*

_____. 2017. **International Professional Practices Framework.** Available at: *www.na.theiia.org.*

_____. 2018. **Staffing/ Resourcing Consideration for internal Audit Activity.** Available at: *www.na.theiia.org*.

_____. 2020. **Internal Audit in the COVID-19 ERA- a Global Glance at responses to the pandemic.** Available at: *www.na.theiia.org*