مجلة البحوث المالية والتجارية
المجلد (٢٣) – العدد الثالث – يوليو
٢٠٢٢

استخدام المنهجية الرشيقة في تطوير أداء المراجعة الداخلية لمواجهة مخاطر الأمن السيبراني

Using the Agile Approach in Developing Internal Audit Performance to Confront Cybersecurity Risks

د. رمضان عارف رمضان محروس
مدرس بقسم المحاسبة
كلية التجارة– جامعة جنوب الوادي

د. أبوالحمد مصطفى صالح
أستاذ مساعد بقسم المحاسبة
كلية التجارة– جامعة جنوب الوادي

رابط المجلة: https://jsst.journals.ekb.eg/

ملخص

هدفت هذه الدراسة إلى تطوير أداء المراجعة الداخلية في منظمات الأعمال المصرية لمواجهة مخاطر الأمن السيبراني، وذلك عن طريق استخدام المنهجية الرشيقة **Agile Approach**، كأحد مناهج التطوير الحديثة، بالإضافة إلى تقديم مجموعة من المقترحات توضح طريقة ومراحل تطبيق المراجعة الداخلية الرشيقة لمواجهة مخاطر الأمن السيبراني، واستكشاف مدى استعداد منظمات الأعمال المصرية لتطبيق هذه المنهجية؛ وتمت الدراسة من خلال استطلاع آراء ١٢٧ مفردة من الإدارة العليا ومسئولي تكنولوجيا المعلومات والمراجعين الداخليين في منظمات الاعمال المصرية والباحثين من أساتذة الجامعات، وباستخدام اختبار **Kruskal-Wallis** توصلت الدراسة إلى عدم وجود اختلافات معنوية بين آراء فئات المستقصى منهم بشأن التزايد المستمر لمخاطر الأمن السيبراني وتأثيراته على مستوى منظمات الأعمال وعلى المستوى القومي، وعدم وجود اختلافات معنوية بين آراء فئات المستقصى منهم بشأن قصور أداء المراجعة الداخلية التقليدية في مواجهة مخاطر الأمن السيبراني واسباب هذا القصور، بالإضافة إلى عدم وجود اختلافات معنوية بين أراء المستقصى منهم بشأن إمكانية تطوير أداء المراجعة الداخلية من خلال استخدام المنهجية الرشيقة في مواجهة مخاطر الأمن السيبراني.

المصطلحات الأساسية: الأمن السيبراني، مخاطر الأمن السيبراني، المراجعة الداخلية، المنهجية الرشيقة، المراجعة الداخلية الرشيقة.

Abstract

This study aimed to develop the performance of internal auditing in Egyptian business organizations to confront cybersecurity risks, by using the Agile Approach, as one of the modern development approaches, in addition to presenting a set of proposals that illustrate the method and stages of applying agile internal audit to confront cybersecurity risks, and exploring the extent of Egyptian business organizations' readiness to apply this approach. The study was conducted through a survey of the opinions of 127 usable responses including senior management, information technology officials, internal auditors in Egyptian business organizations, and researchers from university professors. Using the Kruskal-Wallis test, it was found that there are no significant differences between the opinions of the study groups regarding the continuous increase in cybersecurity risks and its effects at the level of business organizations and at the national level, and there are no significant differences between the opinions of the study groups regarding the inadequacy of traditional internal audit performance in confronting cybersecurity risks and the reasons for this deficiency. Moreover, the absence of significant differences between the opinions of the study groups regarding the possibility of developing the performance of the internal audit through the use of the agile approach to confront cybersecurity risks.

Keywords: Cybersecurity, Cybersecurity risks, Internal Audit, Agile Approach, Agile Internal Audit.

١- الإطار العام للدراسة

١/١ المقدمة:

حدد تقرير مخاطر الأعمال المتوقعة لعام ٢٠٢٢ الصادر عن معهد المراجعين الداخليين الأمريكي اثني عشر خطرا يهدد منظمات الأعمال بمختلف أنواعها وأحجامها، ويأتي في مقدمتها مخاطر الأمن السيبراني، حيث تتزايد بشكل مستمر الهجمات السيبرانية المتنوعة والمعقدة، وتلحق أضرارا بالغة بالعلامات التجارية وسمعة منظمات الأعمال، وينتج عنها في الغالب آثار مالية كارثية (Institute of Internal Auditors "IIA", 2021). ويشير المعهد الوطني للمعايير والتكنولوجيا National Institute of Standards and Technology "NIST" إلى أن المخاطر السيبرانية تؤثر على صافي أرباح المنظمات، حيث يمكن أن تؤدي إلى زيادة التكاليف وتخفيض الإيرادات، كما أنها قد تضر بقدرة المنظمة على الابتكار واكتساب العملاء والحفاظ عليهم، بالإضافة إلى أن الأمن السيبراني يمكن أن يكون أحد المكونات الأساسية والهامة لإدارة المخاطر الشاملة (NIST, 2018).

ونتيجة لتفشي وباء كورونا فقد اضطرت منظمات الأعمال التي كانت تدير أنشطتها الآلية بشكل تدريجي إلى التعجيل بالتحول الرقمي، وتحول الجميع وبشكل مفاجئ إلى تطبيق أسلوب العمل عن بعد في ظل بيئة رقمية، والتي لم تكن بعض المنظمات قد استعدت لها بشكل كافي (Asian Confederation of Institutes of Internal Auditor "ACIIA" and SyCip Gorres Velayo& Co. "SGV", 2021)؛ وقد ساهم ذلك في زيادة مخاطر الأمن السيبراني بسبب استخدام برامج الاجتماعات الافتراضية، والتوسع في استخدام الحاسبات الشخصية وشبكات الإنترنت الخاصة بالأنظمة (IIA, 2020; Sharton, 2020).

وقد أشارت دراسة Pulse التي أجراها معهد المراجعين الداخليين بأمريكا الشمالية في مارس ٢٠٢٢ إلى أن مخاطر الأمن السيبراني ما زالت تتصدر قمة أولويات منظمات الأعمال في جميع الصناعات، حيث أشار قادة المراجعة الداخلية المشاركين في الدراسة إلى أن مخاطر الأمن السيبراني تأتي في المرتبة الأولى من بين ١٣ خطر، وأعطى ٨٥% من المشاركين في استطلاع الرأي هذا الخطر مستوى أهمية مرتفع أو مرتفع للغاية (IIA, 2022a). كما توصلت دراسة معهد المراجعين الداخليين في الاتحاد الأوربي إلى أن مخاطر الأمن السيبراني تعد من بين أعلى خمسة مخاطر تهدد بيئة الأعمال (European Confederation of Institutes of Internal Auditor "ECIIA", 2020).

ويعتقد معظم المديرين التنفيذيين أن مخاطر الأمن السيبراني على صلة وثيقة بمنظماتهم، إلا أن المعرفة الشخصية بهذه المخاطر لا تزال منخفضة لدى معظم الأطراف التنفيذية ومنهم الرؤساء التنفيذيين للمراجعة، وقد يرجع ذلك إلى الطبيعة المتطورة للتهديدات والمخاطر السيبرانية (IIA, 2021).

وتوصي مبادئ الإدارة السليمة للمخاطر بتنظيم إدارة مخاطر الأمن السيبراني في ثلاثة خطوط دفاع كما يلي (Slapnicar, 2022):

خط الدفاع الأول: مديري وحدات التشغيل ووظيفة تكنولوجيا المعلومات، ويأخذ مسئولي هذا الخط في اعتبارهم مخاطر الأمن السيبراني كجزء أصيل من وظيفتهم، كما أن عليهم تصميم ضوابط مناسبة لإدارة المخاطر.

خط الدفاع الثاني: وظيفة أمن المعلومات، والتي تقدم الخبرة في مجال تنفيذ ورقابة فعالية ضوابط الأمن السيبراني.

خط الدفاع الثالث: وظيفة المراجعة الداخلية، التي تقدم تأكيد مستقل لمجلس الإدارة ولجان المخاطر ولجان المراجعة بأن كل من استراتيجية إدارة المخاطر، والسياسات، والإجراءات، والضوابط الرقابية تعمل بفعالية، ويتضمن ذلك مراجعة مدى كفاية العمل الذي تم إنجازه بواسطة خطي الدفاع الأول والثاني.

ويمكن أن تؤدي وظيفة المراجعة الداخلية من خلال دورها الاستشاري دورا فعالا في مساعدة منظمات الأعمال على التطور لمواجهة التحديات المتصاعدة وأهمها مخاطر الأمن السيبراني، والتأكد من الالتزام وفعالية الرقابة على أنشطة المنظمات، وحتى تستطيع المراجعة الداخلية أن تواكب تلك الاحتياجات الاستراتيجية، وأن تؤدي دورها المنشود في مواجهة مخاطر الأمن السيبراني ينبغي أن تتبنى المنهجية الرشيقة Agile Approach في أداء دورها، كما يجب أن تكون قادرة على التعامل مع التكنولوجيا، وقائمة على أساس المخاطر (ACIIA and SGV, 2021).

وتعني المنهجية الرشيقة Agile Approach القدرة على التحرك بسرعة وسهولة، والقدرة على التفكير بطريقة ذكية، للتعامل مع الاحتياجات المتغيرة لأصحاب المصالح، وبالتالي تعد المراجعة الداخلية الرشيقة Agile Internal Audit طريقة للتفكير تركز على احتياجات أصحاب المصالح، والإسراع بدورات المراجعة، وتقديم أفكار وتصورات في الوقت المناسب، مما يؤدي إلى زيادة جودة المراجعة وتقليل الفاقد في الموارد (Agarwal, 2021).

وقد تناول الجزء الثاني من تقرير White Paper تأثير استخدام المنهجية الرشيقة على وظيفة المراجعة الداخلية كما يلي (KPMG, 2020a):

١- تساعد المنهجية الرشيقة في تقديم نصائح ورؤى بشكل متواصل بالاعتماد على دورات مراجعة قصيرة الأجل؛ فالمراجعة الداخلية الرشيقة قادرة على الاستجابة بشكل أكثر مرونة وأكثر سرعة في تلبية الاحتياجات المتغيرة للمنظمات.

٢- تسهم المنهجية الرشيقة في تقديم مجموعة واسعة من المنتجات، حيث تقوم المراجعة الداخلية الرشيقة بتكييف منتجاتها وخدماتها وفقا للاحتياجات المتغيرة لأصحاب المصالح.

٣- يؤدي استخدام المنهجية الرشيقة إلى تحويل مقاييس الأداء الرئيسية للمراجعة من المقاييس التقليدية (مثل إكمال خطة المراجعة، ونتائج المراجعة، وجودة الأداء) إلى التركيز على رضاء العملاء، وعدد مرات التفاعل مع الخاضعين للمراجعة والوقت المستغرق في أعمال المراجعة.

٤- يعمل استخدام المنهجية الرشيقة على تكوين فريق مراجعة على أساس الكفاءات والخبرات المطلوبة لأداء مهام المراجعة والأنشطة المتنوعة، والتركيز على فرق المراجعة متعددة التخصصات ذات المعرفة بتطبيق مبادئ المنهجية الرشيقة.

٥- يتطلب استخدام المنهجية الرشيقة مراجعين قادرين على تعديل طريقة تفكيرهم لأداء العمل، والاستجابة السريعة لاحتياجات المنظمة؛ وذلك بهدف تقديم نصائح وأفكار وتصورات بشكل مستمر إلى جانب خدمات التأكيد.

٢/١ مشكلة الدراسة:

وفقا لما جاء في تقرير **IIA** الصادر في أبريل ٢٠٢٢ تتزايد الهجمات السيبرانية بشكل كبير كنتيجة لمزيج من الأزمات، مثل أزمة أوكرانيا والتهديدات التي لا تزال مستمرة نتيجة وباء كورونا، بالإضافة إلى التوترات بين الولايات المتحدة الأمريكية والصين، وهذه الأزمات والتوترات اجتمعت مع متغيرات أخرى لتدفع مخاطر الأمن السيبراني إلى قمة أولويات المراجعة الداخلية **(IIA, 2022b)**.

كما شهد عام ٢٠٢٢ تطورات كبيرة تتعلق بالأمن السيبراني والتي سوف تؤثر على جميع أنواع منظمات الأعمال، وسوف يتطلب فهم هذه التطورات وتأثيراتها المتعددة مزيدا من الوقت والجهد؛ ويأتي في مقدمة هذه التطورات المقترحات التنظيمية الصادرة عن لجنة تداول الأوراق المالية والبورصات الأمريكية **U.S. Securities and Exchange Commission "SEC"**، والتي تضمنت مطالبة منظمات الأعمال المدرجة بالسوق الأمريكية بالإفصاح عن سياسات وإجراءات واستراتيجيات الحوكمة ومعرفة مجلس الإدارة وخبراته في مجال الأمن السيبراني.

وسوف تمثل هذه التطورات مجالا جديدا لوظائف المراجعة الداخلية، والتي يمكن أن تؤدي دورا محوريا في مواجهة مخاطر الأمن السيبراني؛ ولا شك أن التعامل مع مخاطر الأمن السيبراني لا يتسق معه تطبيق المنهج التقليدي للمراجعة، كما أنه يتطلب توافر عدة مقومات غير موجودة بالمنهج التقليدي للمراجعة. لذا يتطلب الدور المأمول للمراجعة الداخلية اتباع منهجيات حديثة تتوافق مع بيئة الأعمال المتغيرة وسرعة وتعقيد الهجمات السيبرانية.

وتأتي المنهجية الرشيقة **Agile Approach** كأحد أهم المنهجيات التي تهدف إلى تطوير أداء المراجعة الداخلية، والانتقال بها من المنهج التقليدي إلى منهج يعتمد على المرونة وسرعة أداء المهام، والتواصل والتفاعل مع مختلف أصحاب المصالح بالمنظمات، مما يتيح ظهور مفهوم جديد هو المراجعة الداخلية الرشيقة **Agile Internal Audit** والتي تتسم بالقدرة على التعامل الفعال مع مخاطر الأمن السيبراني.

بناء على ما سبق، يمكن صياغة مشكلة الدراسة في تساؤل رئيسي هو "كيف يمكن تطوير أداء المراجعة الداخلية من خلال استخدام المنهجية الرشيقة لمواجهة مخاطر الأمن السيبراني؟ " ويمكن تقسيم هذه التساؤل إلى عدة تساؤلات فرعية كما يلي:

١- ما هي مخاطر الأمن السيبراني وما هي تأثيراتها؟ وما هي الجهود الدولية والمحلية في مجال مواجهة هذه المخاطر؟

٢- هل تؤدي المراجعة الداخلية التقليدية دورا فعالا في مواجهة مخاطر الأمن السيبراني؟

٣- ما هي أبعاد المنهجية الرشيقة وكيف تستخدم في تطوير أداء المراجعة الداخلية؟

٤- ما هو دور المراجعة الداخلية الرشيقة في مواجهة مخاطر الأمن السيبراني؟

٣/١ أهداف الدراسة:

تهدف هذه الدراسة إلى تطوير أداء المراجعة الداخلية في منظمات الأعمال المصرية لمواجهة مخاطر الأمن السيبراني من خلال استخدام المنهجية الرشيقة، وذلك عن طريق تحقيق الأهداف الفرعية التالية:

١- التعرف على مخاطر الأمن السيبراني والآثار المترتبة على الهجمات السيبرانية.

٢- التعرف على أهم الجهود الدولية والمحلية في مواجهة مخاطر الأمن السيبراني.

٣- تقييم أداء المراجعة الداخلية التقليدية في مواجهة مخاطر الأمن السيبراني.

٤- تحديد مفهوم وأبعاد المنهجية الرشيقة، وكيفية تطوير أداء المراجعة الداخلية في ظل استخدام هذه المنهجية.

٥- تقديم مجموعة من المقترحات التي تساعد في تطبيق المراجعة الداخلية الرشيقة لمواجهة مخاطر الأمن السيبراني، واستكشاف مدى استعداد منظمات الأعمال المصرية لتطبيقها.

١/٤ أهمية الدراسة:

تأتي أهمية الدراسة الحالية من عدة مبررات تتمثل فيما يلي:

١- تزايد المخاوف من استمرار تصاعد الهجمات السيبرانية وما تلحقه من أضرار على مستوى منظمات الأعمال وعلى المستوى القومي، وتركيز الاهتمام على البحث عن أدوات تحد من مخاطر هذه الظاهرة.

٢- تزايد اهتمام الجمعيات المهنية بدور المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني، ومحاولة تطوير أداء المراجعة الداخلية في هذا المجال من خلال استخدام منهجيات حديثة للتطوير مثل المنهجية الرشيقة.

٣- ندرة الدراسات السابقة في مجال استخدام المنهجية الرشيقة لتطوير أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني، وهذا ما سوف تركز عليه الدراسة الحالية.

٤- اقتصرت معظم الدراسات التي تناولت دور المراجعة الداخلية في مواجهة مخاطر الامن السيبراني، على تقييم دور المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني في البنوك، على الرغم من تعرض جميع أنواع المنظمات لهذا النوع من المخاطر في ظل التوجه العام نحو التحول الرقمي، وسوف تركز الدراسة الحالية على تطوير أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني في جميع أنواع منظمات الأعمال.

٥- توفير أدلة تجريبية من البيئة المصرية تساعد في التعرف على مدى إدراك منظمات الأعمال لمخاطر الأمن السيبراني وتأثيراتها، وتقييم أداء المراجعة الداخلية التقليدية في مواجهة هذه المخاطر، ومدى استعداد منظمات الأعمال المصرية لتطبيق المراجعة الداخلية الرشيقة.

١/٥ تنظيم الدراسة:

تم تنظيم ما تبقى من هذه الدراسة في ستة أقسام، يتناول القسم الثاني عرض وتحليل الدراسات السابقة، ويناقش القسم الثالث مخاطر الأمن السيبراني والمراجعة الداخلية، ويعرض القسم الرابع المنهجية الرشيقة كأحد مناهج تطوير أداء المراجعة الداخلية، ويتناول القسم الخامس إطار مقترح لاستخدام المنهجية الرشيقة في تطوير أداء المراجعة الداخلية، ويعرض القسم السادس الدراسة الميدانية، وتختتم الدراسة بالقسم السابع ويتناول النتائج والتوصيات والدراسات المستقبلية.

٢- عرض وتحليل الدراسات السابقة

يمكن تقسيم الدراسات السابقة التي تناولت موضوع الدراسة الحالية إلى قسمين كما يلي:

١/٢ دراسات تناولت قضية الأمن السيبراني وعلاقتها بالمراجعة الداخلية:

استطلعت دراسة (Steinbart et al., 2013) آراء ٤٧ مراجع داخلي من أعضاء جمعية المراجعة والرقابة على نظم المعلومات International Systems Audit and Control Association "ISACA"، للتعرف على تصوراتهم بشأن العلاقة بين وظيفة أمن المعلومات ووظيفة المراجعة الداخلية، وتأثير هذه العلاقة على جهود أمن المعلومات في منظمات الأعمال؛ وتوصلت إلى أن زيادة تكرار المراجعة لأنشطة أمن المعلومات تسهم في تحسين جودة العلاقة بين الوظيفتين مع التركيز على الجانب الاستشاري أكثر من الرقابة البوليسية؛ كما أن تكرار المراجعات يزيد من نتائج المراجعة الخاصة بأنشطة أمن المعلومات إلا انه لا يؤثر في حوادث أمن المعلومات.

وبحثت دراسة (Alina et al., 2017) دور المراجعة الداخلية في الأمن السيبراني؛ وتوصلت إلى أن وظيفة المراجعة الداخلية تؤدي دورا أساسيا في تقييم المخاطر السيبرانية كجزء من المخاطر الاستراتيجية، وتحديد فجوات الرقابة التشغيلية على مستوى الأعمال؛ كما أنها تعمل مع الإدارة على تطوير والحفاظ على قدرة المنظمات على التكيف مع الأنواع المختلفة من المخاطر لتحقيق استمرارية النشاط.

وهدفت دراسة (KPMG, 2017) إلى استطلاع آراء المراجعين الداخليين المهنيين في البحرين بشأن تغير دور المراجعة الداخلية في ظل مخاطر الأمن السيبراني؛ ومن خلال ردود ٥٥ مراجع داخلي توصلت الدراسة إلى أن الأمن السيبراني يأتي في المرتبة الأولى ضمن أولويات المراجعة الداخلية الرئيسية؛ وأشارت الدراسة إلى أنه على الرغم من مسئولية الجميع عن تبني ممارسات جيدة للحماية من الهجمات الإلكترونية، إلا أن المراجعة الداخلية تحتاج إلى توسيع نطاق تركيزها ليشمل المخاطر الناشئة عن التطور التكنولوجي إلى جانب المخاطر التشغيلية.

وهدفت دراسة (Crowe and Internal Audit Foundation "IAF", 2018) إلى تقديم تصورات بشأن الدور المستقبلي للمراجعة الداخلية في قضية الأمن السيبراني؛ وباستطلاع آراء رؤساء مراجعة داخلية ومراجعين داخليين وكبار المسئولين التنفيذيين، توصلت الدراسة إلى تطور مسئوليات المراجعة الداخلية في الأمن السيبراني مما يتطلب تطوير الفهم بمبادئ أمن البيانات والأطر الإلكترونية، وزيادة الحاجة إلى الخبرة الفنية والخبرات ذات الصلة بالأمن

السيبراني، بالإضافة إلى حاجة المراجعة الداخلية إلى تعزيز العلاقات داخل منظمات الأعمال لتوفير التوجيه والدعم المالي اللازم.

وهدفت دراسة (Islam et al., 2018) إلى تحديد العوامل المؤثرة في الأمن السيبراني والتي تكون على علاقة بالمراجعة الداخلية، ومن خلال استطلاع آراء ٩٧٠ مراجع داخلي في ١٦٦ دولة، توصلت الدراسة إلى أن قيام المراجعين الداخليين بالتقييم الشامل للمخاطر له تأثير إيجابي كبير في مراجعة الأمن السيبراني، كما أن كفاءة المراجعين الداخليين تؤثر أيضا في مراجعة الأمن السيبراني. وفي نفس السياق بحثت دراسة (Shamsuddin et al., 2018) أثر فعالية المراجعة الداخلية في إدارة الأمن السيبراني في البنوك العاملة في ماليزيا، ومن خلال استطلاع آراء ١٢٠ مراجع داخلي يعمل في مجال البنوك توصلت الدراسة إلى أن وعي المراجعين الداخليين بالأمن السيبراني، والسياسات التنظيمية للأمن السيبراني المرتبطة بالمراجعة الداخلية تؤثر في إدارة الأمن السيبراني بقطاع البنوك.

وتناولت دراسة (الرشيدي، عباس، ٢٠١٩) الإفصاح عن المخاطر السيبرانية وكيفية إدارة هذه المخاطر في منظمات الأعمال العاملة بمجال التكنولوجيا والقطاع المالي في مصر، وأوصت تلك الدراسة بضرورة قيام المراجعة الداخلية بدور فعال من خلال توفير أدوات الرقابة الداخلية المناسبة لتحسين الأمن السيبراني، بالإضافة إلى ضرورة تنمية مهارات أعضاء فريق المراجعة الداخلية وتوفير الكفاءات اللازمة لتحقيق الأمن السيبراني ومواكبة التطور التكنولوجي في بيئة الأعمال الحديثة.

وتناول تقرير (Deloitte, 2020) المخاطر الناشئة التي يجب أن تأخذها المراجعة الداخلية في الحسبان لعام ٢٠٢١؛ وحدد التقرير ١١ موطن خطر منها الأمن السيبراني، حيث زادت مخاطر الهجمات السيبرانية مع التوسع في العمل عن بعد نتيجة تفشي فيروس كورونا؛ وأشار التقرير إلى أن هذه المخاطر لا تقتصر على مخاطر الهجمات السيبرانية الخارجية، ولكنها تشمل تسبب الموظفين في تعريض أمن الأعمال للخطر بقصد أو بدون قصد، وهذا يتطلب قيام المراجعة الداخلية بدور فعال في تحقيق الأمن السيبراني.

وتناول تقرير (KPMG, 2020b) تحديد الموضوعات الرئيسية والمخاطر التي يجب أن يتم مراعاتها عند وضع خطط المراجعة الداخلية لعام ٢٠٢١، وأشار التقرير إلى ضرورة أن تحتوي خطط المراجعة الداخلية على التدابير اللازمة للتعامل مع قضية الأمن السيبراني، في ظل بيئة الأعمال الموسعة وزيادة تكرار وتعقد الهجمات السيبرانية وعمليات الاحتيال.

وبحثت دراسة (عطية، ٢٠٢١) العلاقة بين المراجعة الداخلية والأمن السيبراني، حيث يتوقف نجاح مراجعة الأمن السيبراني على مساهمات كل من إدارة المنظمة، وإدارة المخاطر، والمراجعة الداخلية؛ وحددت الدراسة مسئوليات المراجعة الداخلية في مراجعة الضوابط الرقابية، والتحقق من الالتزام بالضوابط الرقابية، ومراجعة إدارة المخاطر بالمنظمة، بالإضافة إلى مراجعة التعديلات والتحديثات الخاصة بالأمن السيبراني، ومراجعة ردود الأفعال للانتهاكات والهجمات السيبرانية.

واختبرت دراسة (Lois et al., 2021) العوامل المؤثرة في الأمن السيبراني وذات الصلة بالمراجعة الداخلية؛ ومن خلال استطلاع آراء ٧٢ من المراجعين الداخليين بمنظمات الأعمال المقيدة ببورصة أثينا، توصلت الدراسة إلى أن درجة وطبيعة التعاون بين موظفي تكنولوجيا المعلومات والمراجعين الداخليين، وتدريب المراجعين على تكنولوجيا المعلومات من العوامل الأساسية المؤثرة في الأمن السيبراني.

واختبرت دراسة (الزيود، ٢٠٢١) أثر المراجعة الداخلية في الحد من مخاطر الأمن السيبراني في البنوك الأردنية، ومن خلال استطلاع رأي ١٦٩ مراجع خارجي توصلت الدراسة إلى أن كفاءة المراجعة الداخلية وموقعها التنظيمي في البنك يؤثر في الحد من مخاطر الأمن السيبراني بالبنوك الأردنية.

وهدفت دراسة (IIA, 2021) إلى تحديد المخاطر المتوقعة التي تواجه المنظمات في بيئة الأعمال المعاصرة لعام ٢٠٢٢، والتي تتطلب اهتماما خاصا من المراجعة الداخلية؛ ومن خلال إجراء مقابلات مع ٣٠ عضو مجلس إدارة و٣٠ من الإدارة العليا التنفيذية في منظمات الأعمال، توصلت الدراسة إلى وجود ١٢ خطر يهدد المنظمات في عام ٢٠٢٢ ويحتل الأمن السيبراني المرتبة الأولى من بين هذه المخاطر، حيث تنامت الهجمات السيبرانية واتسمت بالتنوع والتعقيد، كما أن منظمات الأعمال أصبحت مهددة بخسائر مالية ضخمة وفقد للسمعة بسبب هذه الهجمات، مما يتطلب تعاون المراجعة الداخلية كخط دفاع ثالث مع خطي الدفاع الأول والثاني لمواجهة هذه التهديدات.

وهدفت دراسة (Slapnicar et al., 2022) إلى تحليل فعالية المراجعة الداخلية في تقديم خدمات تأكيد الأمن السيبراني؛ وعن طريق استطلاع أراء ١٨٣ مفردة من المراجعين ورؤساء المراجعة الداخلية في معهد المراجعين الداخليين الأوروبي وأستراليا ونيوزيلاندا وفي صناعات متنوعة، وباستخدام مؤشر من ١٠٠ نقطة يغطي ثلاثة أبعاد هي التخطيط والتنفيذ والتقرير،

توصلت الدراسة إلى وجود ارتباط طردي قوي بين التخطيط والتنفيذ وتأكيدات الأمن السيبراني، بينما كان الارتباط أقل بين التقرير إلى مجلس الإدارة وإدارة مخاطر الأمن السيبراني.

ويبدو من عرض وتحليل هذا القسم من الدراسات السابقة أن تلك الدراسات تتفق على تنامي مخاطر الأمن السيبراني، والدور الهام للمراجعة الداخلية كأحد خطوط الدفاع الثلاثة في مواجهة هذه المخاطر؛ إلا أن قيام المراجعة الداخلية بدورها بشكل فعال يتوقف على تكرار عمليات المراجعة والتعاون مع خطي الدفاع الأول والثاني، ومعرفة المراجعين الداخليين بتكنولوجيا المعلومات ومفاهيم الأمن السيبراني، بالإضافة إلى الحفاظ على العلاقات الجيدة مع إدارة تكنولوجيا المعلومات والتركيز بشكل أكبر على الدور الاستشاري للمراجعة الداخلية؛ ويتطلب أداء المراجعة الداخلية لدورها بفعالية في مواجهة مخاطر الأمن السيبراني تطوير المنهج التقليدي للمراجعة، والبحث عن منهج حديث يلائم دورها في مجال الأمن السيبراني، وهو ما سوف تركز عليه الدراسة الحالية من خلال طرح المنهجية الرشيقة كأحد مناهج التطوير المقترحة لوظيفة المراجعة الداخلية.

٢/٢ دراسات تناولت استخدام المنهجية الرشيقة كأداة لتطوير المراجعة الداخلية:

تناول تقرير (KPMG, 2019) التحولات التي شهدتها المراجعة الداخلية خلال السنوات الأخيرة لدى عملائها؛ حيث أشار التقرير إلى أن المراجعة الداخلية تحولت من الأسلوب التفاعلي إلى الاعتماد على الطرق الاستباقية، كما أنها تحولت من تقديم خدمات التأكيد فقط إلى التوسع في تقديم الاستشارات والتصورات، بالإضافة إلى التوجه نحو تطبيق المنهجية الرشيقة في المراجعة؛ وأشارت الدراسة إلى أن منظمات الأعمال بدأت بتطبيق المراجعة الرشيقة لتكنولوجيا المعلومات وتحولت بعد ذلك إلى تطبيق المنهجية الرشيقة أثناء تخطيط وتنفيذ جميع عمليات المراجعة الداخلية.

وهدفت دراسة (القنبري، ٢٠٢٠) إلى توضيح فكرة المراجعة الداخلية الرشيقة وفوائدها وخطوات تطبيقها، بالإضافة إلى تحديد أهم الاختلافات بينها وبين المراجعة الداخلية التقليدية؛ وتوصلت الدراسة إلى عدة نتائج أهمها ضرورة قبول فكرة المنهجية الرشيقة والاستفادة من هذه التقنية الذكية في تحقيق النجاح في منظمات الأعمال.

وبحثت دراسة (Beerbaum, 2020) مزايا تطبيق المراجعة الداخلية الرشيقة في مشروعات تكنولوجيا المعلومات مقارنة بالمراجعة الداخلية التقليدية، ومن خلال إجراء خمس مقابلات للمراجعين الداخليين في خمس منظمات أعمال خلال عام ٢٠٢٠ بفنلندا، توصلت إلى

أن استخدام المنهجية الرشيقة يزيد من كفاءة وفعالية المراجعة الداخلية في مشروعات تكنولوجيا المعلومات.

وهدفت دراسة (Acharya, 2021) إلى استطلاع أراء ٤٤ مراجع في البنوك والقطاعات المالية وشركات المراجعة في نيبال، بشأن مدى الحاجة إلى تطبيق المراجعة الداخلية الرشيقة ودورها في كفاءة المراجعة، وتوصلت الدراسة إلى أن هناك حاجة إلى تطبيق المنهجية الرشيقة لزيادة كفاءة المراجعة الداخلية وتعزيز القيمة المضافة، كما أشارت نتائج الاستطلاع إلى أنه إذا لم يتم تطبيق المراجعة الداخلية الرشيقة بشكل مناسب فقد يؤثر ذلك سلبيا في أداء الأعمال، لذا يجب إجراء تقييم شامل لاحتياجات العمل وطريقة دمج التغييرات الناتجة عن التحول إلى المراجعة الداخلية الرشيقة.

واستطلعت دراسة (ACIIA and SGV, 2021) آراء ٣٧٦ من مديري المراجعة الداخلية وأصحاب المصالح في ١٥ دولة في منطقة آسيا والمحيط الهادي بشأن مستقبل المراجعة الداخلية في ضوء التطورات التكنولوجية المتسارعة وظهور استخدامات جديدة للتكنولوجيا مثل أدوات الذكاء الاصطناعي وتحليل البيانات؛ وتوصلت الدراسة إلى أن ٤١% ممن شملهم الاستطلاع قاموا بدمج المنهجية الرشيقة في إجراءات العمل، كما أن ٥٠% منهم قاموا بتطبيق المنهجية الرشيقة في تحليلات البيانات، وأشارت الدراسة إلى أن استخدام المنهجية الرشيقة في المراجعة يعمل على توفير مرونة الاستجابة للمخاطر، والتحديد الاستباقي للمجالات التي تتطلب تركيزا خاصا.

وقامت دراسة (Joshi, 2021) بإجراء استعراض تاريخي للمراجعة الداخلية الرشيقة بالإضافة إلى دراسة التوقعات المستقبلية المتعلقة باستخدام المنهجية الرشيقة، من حيث المفهوم، التاريخ، مدى الحاجة لها، الخصائص، أسلوب التنفيذ، المزايا، والتحديات؛ وتوصلت الدراسة إلى عدة نتائج أهمها أن المراجعة الداخلية الرشيقة تناسب المراجعات المعقدة والتي تتطلب فريق ذو خبرة وتركيز عالي، كما أنها تناسب دورات المراجعة قصيرة الأجل والحالات التي تتطلب تقديم خدمات المراجعة والاستشارات بسرعة عالية للعملاء؛ كما أشارت الدراسة إلى أن المراجعة الداخلية الرشيقة تختلف بشكل كبير ما بين منظمات الأعمال وفقا للحجم والثقافة التنظيمية السائدة.

ويتضح من عرض وتحليل هذا القسم من الدراسات السابقة، وجود اتفاق بين تلك الدراسات على أهمية التوجه نحو تطوير وظيفة المراجعة الداخلية من خلال استخدام المنهجية الرشيقة، نظرا لما توفره من مرونة في خطط المراجعة والتعامل بشكل استباقي مع المخاطر، كما أنها

تناسب المراجعات قصيرة الأجل التي تتطلب تقديم هذه الخدمات في أسرع وقت ممكن لأصحاب المصالح؛ وتلك السمات تجعل المنهجية الرشيقة أحد الأساليب المناسبة لتطوير المراجعة الداخلية في بيئة المخاطر السيبرانية؛ إلا أن تلك الدراسات السابقة أشارت أيضا إلى إن عدم تطبيق المنهجية الرشيقة بشكل مناسب قد يؤثر سلبيا في أداء مهام المراجعة، وهذا يتطلب التقييم الملائم لاحتياجات العمل واختيار الطريقة المناسبة لدمج التغييرات الناتجة عن استخدام المنهجية الرشيقة في تطوير المراجعة الداخلية؛ وبناء على ذلك سوف تركز الدراسة الحالية على تقديم إطار لتطبيق المنهجية الرشيقة في مجال تطوير أداء المراجعة الداخلية لمواجهة مخاطر الأمن السيبراني.

٣- مخاطر الأمن السيبراني والمراجعة الداخلية

١/٣ مخاطر الأمن السيبراني وتأثيراتها:

يشير الأمن السيبراني إلى حماية الأصول الرقمية من المخاطر الموجودة نتيجة لاستخدام تكنولوجيا المعلومات والاتصالات التي تشكل أساس الفضاء الالكتروني (Salin and Lundgren, 2022)؛ وقد عرف إطار NIST الأمن السيبراني بأنه عملية حماية المعلومات من خلال منع واكتشاف والرد على الهجمات السيبرانية، كما عرف حادثة الأمن السيبراني بأنها حادثة سوف يكون لها تأثير على المنظمة مما يستدعي الحاجة إلى الرد والتعافي (NIST, 2018)؛ وتتعلق حوادث الأمن السيبراني باختراق البيانات وفشل نظم المعلومات وقد تؤدي إلى خسائر ضخمة في بيانات المنظمات وممتلكاتها، وتلحق أضرارا كبيرة بسمعة منظمات الأعمال وبنيتها الأساسية (Pie et al., 2020). وتكمن خطورة هذه الهجمات السيبرانية في استنادها إلى تقنيات متقدمة ومتطورة، وسرعة وسهولة انتشارها، بالإضافة إلى اتساع نطاق تأثيرها (الاستراتيجية الوطنية للأمن السيبراني، ٢٠١٧).

وأحد الأمثلة على التأثيرات المتعددة لحوادث الأمن السيبراني، الهجوم السيبراني الذي تعرضت له متاجر التجزئة الأمريكية Mogul Target في عام ٢٠١٣ والذي تسبب في انخفاض أرباحها بأكثر من ٥٠% للربع الأخير من العام، ورفع ٨٠ دعوى قضائية ضد هذه المتاجر، ونتيجة لذلك مع عوامل أخرى أدرج المنتدى الاقتصادي العالمي عام ٢٠١٦ الهجمات السيبرانية كأحد أكبر المخاطر التي يواجهها العالم، كما صنف موقع Risk.net الهجمات السيبرانية بأنها أهم المخاطر التشغيلية في عام ٢٠١٧(Pie et al., 2020).

وقد أدى التحول على نطاق واسع إلى لترتيبات العمل عن بعد كنتيجة لأزمة كورونا إلى زيادة تعرض المنظمات إلى الهجمات السيبرانية، حيث يتغاضى بعض الموظفين عن إجراءات

الرقابة والحماية بهدف توفير الوقت، كما أن التقدم التكنولوجي يزيد من تكرار ودرجة تعقيد الهجمات السيبرانية (KPMG, 2020b)؛ ووفقا لموقع Fortune.com هناك ١٢٩١ اختراق للنظم الإلكترونية خلال عام ٢٠٢١ مقارنة بعدد هجمات بلغ ١١٠٨ عام ٢٠٢٠ مما يدل على استمرار الاتجاه التصاعدي لتلك الهجمات (BDO, 2021). كما تضمن تقرير (Sonicwall, 2022) إحصائيات تبين تصاعد الهجمات السيبرانية، حيث ارتفع عدد تهديدات التشفير في عام ٢٠٢١ بنسبة ١٦٧% (١٠.٤ مليون هجوم)، وارتفعت هجمات فيروس الفدية بنسبة ١٠٥% (٦٢٣.٣ مليون هجوم)، وزادت هجمات Cryptojacking على أجهزة الحاسب المرتبطة بالعملات المشفرة بنسبة ١٩% (٩٧.١ مليون هجوم)، وارتفعت محاولات التسلل بنسبة ١١% (٥.٣ تريليون هجوم)، كما زادت البرامج الضارة الموجهة إلى إنترنت الأشياء بنسبة ٦% (٦٠.١ مليون هجوم).

وفي عام ٢٠٢١ تم تسجيل هجوم سيبراني على شركة Colonial Pipeline Co.6 الأمريكية، وقد أدى هذا الهجوم إلى تعطل في تدفق ما يقارب نصف إمدادات البنزين ووقود الطائرات، وفي النهاية اضطرت الشركة إلى دفع فدية قيمتها خمسة ملايين دولار لمجموعة القراصنة لاستعادة الشبكة واستعادة البيانات (IIA, 2022). وتوقعت دراسة Cybersecurity Venture لعام ٢٠٢٢ أن تصل تكلفة الهجمات السيبرانية إلى ١٠.٥ ترليون دولار بحلول عام ٢٠٢٥ بمتوسط نمو سنوي ١٥% (Morgan, 2022)؛ كما يقدر صندوق النقد الدولي تكلفة الهجمات السيبرانية في قطاع الخدمات المالية بنحو ٢٧٠ إلى ٣٥٠ مليار دولار سنويا حال اتساع نطاق هذه الهجمات (صندوق النقد العربي، ٢٠١٩).

وأشارت إحدى الدراسات إلى أن مصر تعد ثالث الدول العربية من حيث تعرضها للهجمات السيبرانية على شبكاتها وأنظمتها الصناعية بعد الجزائر والمغرب (الرشيدي، عباس، ٢٠١٩)؛ كما توصلت دراسة (بانقا، ٢٠١٩) إلى زيادة عدد الهجمات السيبرانية في دول مجلس التعاون الخليجي مقارنة بدول العالم الأخرى، كما أن الخسائر الناتجة عن هذه الهجمات تتعدى المتوسط العالمي للخسائر، ويمكن أن تؤثر في البنية الأساسية والمرافق الحيوية، مما يتطلب المزيد من الجهود لسد هذه الثغرات الأمنية الإلكترونية، بالإضافة إلى ضرورة إدراج الأمن السيبراني ضمن استراتيجية إدارة المخاطر في الشركات.

٢/٣ أهم الجهود التنظيمية في مجال الأمن السيبراني دولياً ومحلياً:

١/٢/٣ إطار عمل Control Objectives for Information Technologies "COBIT":

صدرت النسخة الأولى من إطار **COBIT** من خلال جمعية مراجعة ورقابة نظم المعلومات **ISACA** عام ١٩٩٦ وهو يمثل إطارا عاما لتنفيذ مهام مراجعة تكنولوجيا المعلومات، وقد تم تطوير هذه النسخة وتم إصدار النسخة الثانية من **COBIT** عام ١٩٩٨، وفي ظل إدراك الأهمية المتزايدة لتكنولوجيا المعلومات والحاجة إلى رقابة فعالة على هذه التكنولوجيا، قامت جمعية **ISACA** بتأسيس معهد تكنولوجيا المعلومات **"ITGI" Information Technology Governance Institute** كمركز أبحاث لحوكمة تكنولوجيا المعلومات **(Haes et al., 2020).**

وقد ساهمت الأفكار والتصورات التي قدمها معهد **ITGI** في تطوير إطار **COBIT** ليكون إطارا شاملا لإدارة تكنولوجيا المعلومات، وبناء على ذلك تم إصدار النسخة الثالثة من إطار **COBIT** عام ٢٠٠٠ والتي تضمنت إرشادات الإدارة ومنها المقاييس، عوامل النجاح الأساسية، ونماذج النضج لعمليات تكنولوجيا المعلومات، وفي عام ٢٠٠٥ أصدرت جمعية **ISACA** النسخة الرابعة من إطار **COBIT 4** والذي يهدف إلى بناء إطار عمل يلقى القبول العام في مجال حوكمة تكنولوجيا المعلومات، واحتوت هذه النسخة على العديد من مفاهيم الإدارة والحوكمة ومنها **(Haes et al., 2020):**

١- التوافق بين أهداف الأعمال وتكنولوجيا المعلومات وعلاقتها مع العمليات الداعمة لتكنولوجيا المعلومات.

٢- الأدوار والمسئوليات في سياق تكنولوجيا المعلومات.

٣- العلاقات المتبادلة بين عمليات تكنولوجيا المعلومات.

كما قام معهد تكنولوجيا المعلومات بإصدار نسختين من إطار عمل **Val IT** عامي ٢٠٠٦ و٢٠٠٨، بالإضافة إلى إصدار إطار **Risk IT** عام ٢٠٠٩، وتناولت هذه الإصدارات العمليات والمسئوليات المتعلقة بتكنولوجيا المعلومات ودورها في خلق القيمة وإدارة المخاطر، ومثلت هذه الإصدارات أعمال تكميلية لكل من **COBIT4 COBIT 4.1** الصادر عام ٢٠٠٧، وفي خطوة تالية قام معهد تكنولوجيا المعلومات عام ٢٠١٢ بدمج هذه الأطر معا وإصدار **COBIT 5** كإطار عمل متكامل للممارسات الجيدة لحوكمة وإدارة تكنولوجيا المعلومات.

ويوفر COBIT 5 إطارا شاملا يساعد منظمات الأعمال في تحقيق أهدافها لحوكمة وإدارة تكنولوجيا المعلومات، كما أن COBIT 5 يساعد المنظمات في خلق قيمة مثالية من تكنولوجيا المعلومات وذلك عن طريق الحفاظ على التوازن بين تحقيق المنافع وتحسين استخدام الموارد ومستويات المخاطر (ISACA, 2012).

ويتيح COBIT 5 إدارة وحوكمة تكنولوجيا المعلومات بطريقة شاملة، مع الأخذ في الاعتبار مجالات المسئولية الوظيفية للأعمال وتكنولوجيا المعلومات، والمصالح المرتبطة بتكنولوجيا المعلومات لكل من أصحاب المصالح الداخليين والخارجيين، كما أن COBIT يلائم جميع منظمات الأعمال على اختلاف أحجامها وسواء كانت تجارية أو غير هادفة للربح أو قطاع عام (ISACA, 2012).

وقد قدم إطار COBIT 5 خمسة مبادئ تعمل معا على تمكين منظمات الأعمال من بناء إطار حوكمة وإدارة فعال، يعمل على تحسين الاستثمار في المعلومات والتكنولوجيا واستخدامها بما يحقق تطلعات أصحاب المصالح، وهذه المبادئ الخمسة هي: تلبية احتياجات أصحاب المصالح، تغطية الشركة من البداية إلى النهاية، تطبيق إطار واحد متكامل، تمكين المنهج الشمولي، وفصل الحوكمة عن الإدارة.

ويتميز إطار COBIT 5 بعلاقات قوية مع العديد من الأطر والمعايير الراسخة ومنها ISO/ IEC 38500، حيث تبنى إطار COBIT 5 الفصل وبشكل صريح بين حوكمة تكنولوجيا المعلومات وإدارة تكنولوجيا المعلومات، وذلك من خلال تقديم مجال عمل إضافي يحتوي على عمليات تتعلق بحوكمة تكنولوجيا المعلومات مثل التقييم والتوجيه والرقابة.

وفي نوفمبر ٢٠١٨ تم إصدار النسخة الحالية من الإطار تحت مسمى COBIT 2019، ويهدف هذا الإطار إلى توفير مرونة أكبر في تنفيذ حوكمة تكنولوجيا المعلومات EGIT، وتضمن هذا الإطار تعديل لمبادئ COBIT 5، وتحديث لسلسلة الأهداف، وإدخال بعض العمليات الجديدة، ومقدمة لمجالات التركيز التي تهدف إلى التركيز على مواقف محددة لحل المشكلات، بالإضافة إلى مقدمة لعوامل التصميم تهدف إلى تسهيل تنفيذ حوكمة تكنولوجيا المعلومات.

وبالمقارنة مع الأطر السابقة فإن إطار COBIT 2019 يتميز بما يلي (Heas et al., 2020):

١- يقدم ثلاثة أهداف جديدة للحوكمة والإدارة ويرتبط كل هدف بعملية تتعلق بالبيانات والمشروعات والتأكيد.

٢- يحدد مكونات نظام حوكمة تكنولوجيا المعلومات الفعال.

٣- يقدم سلسلة أهداف تم تحديثها.

٤- يحدد عوامل التصميم التي يجب اخذها في الاعتبار عند تصميم وتنفيذ نظام حوكمة تكنولوجيا المعلومات.

٥- يقدم مفهوم مجالات التركيز والذي يهدف إلى التركيز على مواقف محددة لحل المشكلات.

وقد تم تنظيم إطار عمل **COBIT 2019** في أربعة أقسام أساسية هي: مقدمة ومنهجية، أهداف الحوكمة والإدارة، دليل التصميم، ودليل التنفيذ. كما قدم الإطار ستة مبادئ تصف المتطلبات الأساسية لنظام حوكمة تكنولوجيا المعلومات وهي: تقديم قيمة لأصحاب المصالح، المنهج الشمولي، نظام الحوكمة الديناميكي، حوكمة منفصلة عن الإدارة، مصممة وفقا لاحتياجات المنظمة، ونظام حوكمة شامل.

٢/٢/٣ إطار تحسين البنية الأساسية الحيوية للأمن السيبراني الصادر عن NIST:

بدأ العمل في مشروع هذا الإطار عام ٢٠١٣ من خلال دعوة **NIST** لمنظمات وأفراد من القطاعين العام والخاص، وتم إصدار النسخة الأولى من الإطار عام ٢٠١٤ وتم تنقيحه في عامي ٢٠١٧ و٢٠١٨. ويركز هذا الإطار على توجيه أنشطة الأمن السيبراني والنظر في مخاطر الأمن السيبراني كجزء من عمليات إدارة المخاطر بالمنظمات؛ ويتكون هذا الإطار من ثلاثة أجزاء هي جوهر الإطار **Framework Core**، مستويات التنفيذ **Framework Implementation Tiers**، والملف الشخصي **Framework Profile**.

وجوهر الإطار هو عبارة عن مجموعة من الأنشطة والنتائج المرغوبة للأمن السيبراني تم تنظيمها في فئات وتتوافق مع المراجع الإعلامية **Informative References**، ويحدد جوهر الإطار خمسة وظائف كما يلي **(Morin, 2020)**:

١- وظيفة التحديد **Identify**: تشير إلى تطوير الفهم التنظيمي لإدارة مخاطر الأمن السيبراني للأنظمة والأصول والبيانات والقدرات.

٢- وظيفة الحماية **Protect**: تعني تطوير وتنفيذ الضمانات المناسبة لتأكيد تقديم خدمات البنية الأساسية الحيوية.

٣- وظيفة الاكتشاف **Detect**: تمثل تطوير وتنفيذ الأنشطة المناسبة لتحديد وقوع خطر الأمن السيبراني.

٤- وظيفة الرد **Respond**: تهتم بتطوير وتنفيذ الأنشطة المناسبة لاتخاذ الإجراءات المتعلقة بخطر الأمن السيبراني الذي تم اكتشافه.

٥- وظيفة الاستعادة **Recover**: تعمل على تطوير وتنفيذ الأنشطة المناسبة للحفاظ على مرونة الخطط واستعادة أي قدرات أو خدمات تعرضت للضرر بسبب وقوع خطر الأمن السيبراني.

أما مستويات التنفيذ فهي تصف إلى أي مدى تتوافق ممارسات إدارة مخاطر الأمن السيبراني في المنظمة مع الخصائص المحددة في هذا الإطار، وتسمح مستويات التنفيذ للمنظمات بتحديد أولوياتها، كما أنها تفترض أن المنظمات المختلفة تواجه مخاطر أمن سيبراني مختلفة (Morin, 2020)؛ والملف الشخصي يمثل التوافق الفريد بين المتطلبات التنظيمية وأهداف المنظمة وقابليتها للمخاطر والموارد مقارنة بالنتائج المرجوة من إطار العمل (NIST, 2018).

وعلى الرغم من تطوير هذا الإطار لتحسين إدارة مخاطر الأمن السيبراني في البنية الأساسية الحيوية، إلا أنه يمكن استخدامه من قبل المنظمات في جميع القطاعات وفي أي مجتمع؛ وهذا الإطار يعمل على تمكين المنظمات من تطبيق أفضل الممارسات لإدارة المخاطر ولتحسين كل من أمن المنظمة ومرونتها، وذلك بغض النظر عن حجم المنظمة أو درجة تعرضها للمخاطر (NIST, 2018).

ويتميز إطار تحسين البنية الأساسية الحيوية للأمن السيبراني بما يلي (NIST, 2018):

١- يوفر هيكل تنظيمي مشترك لمناهج متعددة لتحقيق الأمن السيبراني، من خلال تجميع المعايير والمبادئ الإسترشادية والممارسات التي تعمل بشكل فعال حاليا.

٢- يمكن أن يكون نموذجا للتعاون الدولي في مجال تعزيز الأمن السيبراني للبنية الأساسية الحيوية، نظرا لأن الإطار يشير إلى معايير معترف بها دوليا للأمن السيبراني.

٣- يوفر هذا الإطار طريقة مرنة لمعالجة الأمن السيبراني، بما في ذلك تأثير الأمن السيبراني على الأبعاد المادية والالكترونية والأفراد.

٤- قابل للتطبيق على المنظمات التي تعتمد على التكنولوجيا سواء كان تركيز الأمن السيبراني لديها على تكنولوجيا المعلومات أو أنظمة التحكم الصناعي أو الأنظمة المادية الإلكترونية أو الأجهزة المتصلة بشكل عام بما في ذلك إنترنت الأشياء.

٣/٢/٣ مقترحات SEC:

اتخذت لجنة تداول الأوراق المالية والبورصات الأمريكية SEC مؤخرا خطوات تاريخية في مجال الأمن السيبراني، سوف يكون لها آثار هامة على منظمات الأعمال الأمريكية المسجلة بالسوق وكذلك على المنظمات في جميع أنحاء العالم.

فقد كشفت SEC عن اقتراحين في مجال الأمن السيبراني، حيث أصدرت في فبراير ٢٠٢٢ الاقتراح الأول والذي يركز على مستشاري ومنظمات الاستثمار وصناديق تطوير الأعمال

المسجلة بالسوق الأمريكية، وبموجب هذا الاقتراح تحتاج منظمات الاستثمار وصناديق التطوير إلى ما يلي (SEC, 2022a):

١- اعتماد وتنفيذ سياسات وإجراءات مكتوبة للأمن السيبراني، والتي تصمم لمعالجة مخاطر الأمن السيبراني التي قد تؤدي إلى الإضرار بالعملاء.

٢- الإفصاح عن حوادث الأمن السيبراني الكبيرة التي تؤثر على منظمات وصناديق الاستثمار والتطوير أو عملائهم، وذلك من خلال تقرير يوجه إلى SEC وفقا لنموذج جديد.

٣- الإفصاح عن مخاطر وحوادث الأمن السيبراني الكبيرة التي وقعت خلال العامين الماليين السابقين في كتيبات وقوائم التسجيل الخاصة بهم.

وفي مارس ٢٠٢٢ صدر الاقتراح الثاني والذي تم توجيهه إلى جميع منظمات الأعمال العامة المقيدة بالسوق الأمريكية، ويهدف هذا الاقتراح إلى تعزيز وتوحيد الإفصاحات المتعلقة بإدارة مخاطر الأمن السيبراني، والاستراتيجية، والحوكمة، والإفصاح عن حوادث الأمن السيبراني لمنظمات الأعمال العامة، التي تخضع لقواعد الإفصاح الخاصة ببورصة الأوراق المالية قانون عام ١٩٣٤، ولتحقيق هذا الهدف تتطلب القواعد الجديدة من منظمات الأعمال العامة تقديم إفصاحات تتعلق بما يلي (SEC, 2022b):

١- سياسات وإجراءات المنظمة لتحديد وإدارة مخاطر الأمن السيبراني، وتتضمن القواعد قائمة موسعة ولكنها غير شاملة لاستراتيجيات وسياسات وإجراءات إدارة المخاطر التي تخضع للإفصاح.

٢- دور الإدارة في تنفيذ سياسات وإجراءات الأمن السيبراني.

٣- خبرات مجلس الإدارة في مجال الأمن السيبراني، وإشرافه على مخاطر الأمن السيبراني.

٤- حوادث الأمن السيبراني في غضون أربعة أيام عمل، كما هو مطلوب لأي حدث جوهري آخر، وذلك في ضوء التعديلات التي تضمنها هذا المقترح على النموذج K-8.

ويرى المعهد الأمريكي للمراجعين الداخليين أن مقترحات SEC لا تتعلق بالأمن السيبراني، ولكنها تتعلق بإدارة مخاطر الأمن السيبراني (IIA, 2022b).

٤/٢/٣ جهود الأمن السيبراني في مصر:

صدرت الاستراتيجية الوطنية للأمن السيبراني (٢٠١٧- ٢٠٢١) عن المجلس الأعلى للأمن السيبراني التابع لمجلس الوزراء عام ٢٠١٧، وتضمنت عدة برامج تدعم الهدف الاستراتيجي للأمن السيبراني والمتمثل في مواجهة المخاطر السيبرانية، وتعزيز الثقة في البنية الأساسية للاتصالات والمعلومات وتطبيقاتها وخدماتها في جميع القطاعات الحيوية وتأمينها، لتحقيق بيئة

رقمية آمنة وموثوقة للمجتمع المصري؛ وتناولت هذه الاستراتيجية أهم التحديات والمخاطر السيبرانية مثل خطر اختراق وتخريب البنية الأساسية للاتصالات وتكنولوجيا المعلومات، وخطر الإرهاب والحرب السيبرانية، وخطر سرقة الهوية الرقمية والبيانات الرقمية.

وقد حددت الاستراتيجية الوطنية للأمن السيبراني عدة برامج لتحقيق الأمن السيبراني كما يلي:

١- تطوير الإطار التشريعي الملائم للأمن السيبراني ومكافحة الجرائم السيبرانية وحماية الخصوصية والهوية الرقمية، من خلال صياغة قواعد تشريعية جديدة وملائمة لمواجهة تلك الجرائم المعاصرة.

٢- تطوير منظومة وطنية متكاملة لحماية الأمن السيبراني وتأمين البنية الأساسية للاتصالات وتكنولوجيا المعلومات، من خلال إعداد وتفعيل فرق الاستجابة للطوارئ أو فرق مواجهة حوادث أمن الحاسبات في القطاعات الحيوية.

٣- حماية الهوية الرقمية وتفعيل البنية الأساسية اللازمة لدعم الثقة في التعاملات والخدمات الالكترونية مثل بنية المفتاح المعلن التي يعتمد عليها التوقيع الالكتروني.

٤- إعداد الكوادر البشرية والخبرات اللازمة لتفعيل منظومة الأمن السيبراني في جميع القطاعات.

٥- دعم برامج ومشروعات التعاون بين الهيئات البحثية والشركات الوطنية لتطوير وتنمية صناعة الأمن السيبراني.

٦- نشر التوعية المجتمعية بفرص ومزايا الخدمات الالكترونية، وأهمية الأمن السيبراني لحماية تلك الخدمات من المخاطر والتحديات التي تواجهها.

وفي نفس السياق قام البنك المركزي المصري بإنشاء مركز الاستجابة لطوارئ الحاسب الآلي بهدف توفير الحماية اللازمة للمتعاملين مع البنوك وتعزيز الأمن السيبراني في القطاع المصرفي، ويقوم هذا المركز بالتعامل والإبلاغ الفوري عن أي مخاطر سيبرانية وتعميم الإنذار المبكر والتنبيهات واتخاذ الإجراءات الاحترازية، والقيام أيضا بالمراقبة الأمنية وتحديد التهديدات الالكترونية المحتملة، وفحص وتقييم المخاطر المرتبطة بالثغرات الأمنية والبرمجيات الضارة (صندوق النقد العربي، ٢٠١٩). كما أطلق البنك المركزي مبادرة تعزيز الأمن السيبراني في القطاع المصرفي، والتي تهدف إلى زيادة أعداد الخبراء المعتمدين دوليا في مجال الأمن السيبراني في القطاع المصرفي (البنك المركزي المصري، ٢٠١٩).

٣/٣ دور المراجعة الداخلية في الأمن السيبراني:

على الرغم من اهتمام منظمات الأعمال بأساليب الحد من الحوادث والاختراقات المتزايدة لنظم المعلومات، إلا أن الأساليب المقترحة من خلال خبراء تكنولوجيا المعلومات ليست كافية، وفي هذا الشأن تستطيع المراجعة الداخلية أن تؤدي دورا فعالا في تحقيق أهداف الحماية وتقديم خدمات تأكيد أمن أنظمة المعلومات التي تحتوي على معلومات عالية الحساسية (Lois et al., 2021). ويشير تقرير (IIA, 2022b) إلى أن المشكلة في الأمن السيبراني تتمثل في تأرجح المساءلة بين عدة أطراف، وتستطيع المراجعة الداخلية من خلال خدمات التأكيد وتقديم المشورة تحقيق التوازن والمساعدة في تحديد المساءلة بشكل واضح؛ كما يمكن أن تقدم المراجعة رؤيتها بشأن احتمالات زيادة مخاطر انتهاك البيانات والاختراقات الأمنية الناتجة عن تخفيف أو زيادة الضوابط الرقابية، ويمكن أيضا أن تعمل على تقييم مدى الوعي بالأمن السيبراني وكفاية البرامج التدريبية للموظفين في ظل بيئة تكنولوجيا المعلومات، بالإضافة إلى مساهمتها في تحسين فهم المنظمة لمخاطر الأمن السيبراني، وتحديد الاستراتيجيات الممكنة للتخفيف من حدة هذه المخاطر، ومدى فعالية إدارة مخاطر الأمن السيبراني (KPMG, 2020b).

كما ربطت دراسة (Alina et al., 2017) بين مراحل التعامل مع مخاطر الهجمات السيبرانية ودور المراجعة الداخلية كما يلي:

١- مرحلة الحماية: تساعد المراجعة الداخلية من خلال العمل مع خطي الدفاع الأول والثاني في تطوير برنامج حوكمة تكنولوجيا المعلومات ويشمل استراتيجيات وسياسات الأمن السيبراني، كما أنها تشارك في تقييم واختبار مخاطر الأمن السيبراني، وتقييم خطط الأمن السيبراني ومدى فعاليتها في الحد من هذه المخاطر.

٢- مرحلة الكشف عن المخاطر: تقوم المراجعة الداخلية بتقييم ضوابط الرقابة على الأمن السيبراني، وتقدم تقاريرها إلى الإدارة التنفيذية ولجنة المراجعة حول فعالية هذه الضوابط والتهديدات المحتملة، بالإضافة إلى التحقق من فعالية الإجراءات المطبقة وحلول نظم الرقابة.

٣- مرحلة استمرار النشاط: تعد برامج الاستجابة للمخاطر السيبرانية وبرامج استمرار النشاط من أهم أولويات منظمات الأعمال للصمود ضد الهجمات السيبرانية، لذا تساعد المراجعة الداخلية في التحقق من توافر إجراءات وخطط بديلة فعالة لاستمرار النشاط في حالة وقوع هجوم سيبراني.

٤- مرحلة رد الفعل: تحتاج منظمات الأعمال لإعداد برنامج إدارة الأزمة كأحد أجزاء إدارة استمرار النشاط، ويعد تقييم المخالفات وإيجاد طرق الاستجابة المناسبة لها الخطوة الأولى في

التعامل مع الهجمات السيبرانية، وتستطيع المراجعة الداخلية في هذه المرحلة مراقبة وتقييم مدى ملاءمة طرق الاستجابة التي اتبعتها الإدارة.

٥- مرحلة التطوير: تضيف وظيفة المراجعة الداخلية قيمة في هذه المرحلة من خلال إبداء الرأي في كل من النشاط بشكل كامل، وإجراءات الأمن، وبروتوكولات التعامل مع المخاطر، والاستراتيجيات، بالإضافة إلى اقتراح التحسينات الضرورية لضمان الاستعداد الدائم للتصدي للهجمات السيبرانية.

وفي مجال تقييم كفاءة المراجعة الداخلية في الوقت الراهن ومدى قدرتها على القيام بمهام الأمن السيبراني؛ تناولت دراسة (IAF and Deloitte, 2021) تقييم كفاءة المراجعة الداخلية وتحديد نقاط القوة وفجوة الكفاءة في ضوء إطار الكفاءة المهنية الصادر عن معهد المراجعين الداخليين IIA، ومن خلال استطلاع آراء ١١٨١ مرجع داخلي في ٩٥ دولة، توصلت الدراسة إلى وجود فجوة كفاءة تتعلق بعدم توافر المهارات الكافية لكثير من المراجعين الداخليين لتقديم خدمات التأكيد والاستشارات فيما يتعلق بتكنولوجيا المعلومات والتكنولوجيا الرقمية، كما أن هناك فجوات أخرى للكفاءة ترتبط بتطبيق منهجية المراجعة الرشيقة وتحليلات البيانات؛ وقدمت هذه الدراسة مجموعة من التوصيات لسد فجوات الكفاءة من خلال تقييم المراجعين الداخليين لكفاءتهم باستمرار والموارد المتاحة لهم، والعمل التعاوني مع لجان المراجعة والإدارات التنفيذية عند وضع خطط المراجعة.

وقد كشف أحدث استطلاعات الرأي في هذا المجال عن ضعف مشاركة المراجعة الداخلية في مجال الأمن السيبراني، حيث أنه وفقا لاستطلاع Pulse يتم تخصيص ٩% فقط من خطة المراجعة الداخلية لمهام الأمن السيبراني في منظمات الأعمال العامة، ويرجع ذلك إلى قيود الميزانية ونقص كل من الموارد والمعرفة والخبرة في هذا المجال، وأشار الإستطلاع إلى أن القيمة الحقيقية التي يمكن أن توفرها المراجعة الداخلية ليست بالضرورة تنتج عن المعرفة بالأمن السيبراني، ولكن القيمة تنشأ من المعرفة بتحديد المخاطر، والإفصاح عن المخاطر، وتقييم الضوابط العامة للتعامل مع المخاطر (IIA, 2022a).

وفيما يتعلق بواقع المراجعة الداخلية في جمهورية مصر العربية، كشفت دراسة (الإبياري، ٢٠١٨) أن المراجعة الداخلية في منظمات الأعمال المصرية تعمل وفقا للمنظور التقليدي، ولكن المسئولين عن الحوكمة لديهم إدراك بحاجة المراجعة الداخلية إلى تحسينات جوهرية، إلا أن الدراسة لم تثبت توافر مقومات تطوير وإعادة هندسة المراجعة الداخلية في منظمات الأعمال المصرية.

٤- المنهجية الرشيقة كأحد مناهج تطوير أداء المراجعة الداخلية

١/٤ نشأة وتطور المنهجية الرشيقة Agile Approach:

استخدمت منظمات الأعمال العاملة في مجال التكنولوجيا كثير من الأدوات والتقنيات الآلية لتطوير البرمجيات بهدف زيادة الإنتاجية وتوفير المنتجات المطلوبة للعملاء في الوقت المحدد وبأعلى جودة ممكنة، وتم تجربة مناهج متعددة لتطوير البرمجيات أثناء التطبيق العملي، ونتج عن هذه المحاولات ظهور نموذج جديد للأعمال خلال القرن الحادي والعشرين يسمى منهجية التطوير الرشيقة Agile Approach وقد حققت هذه المنهجية نتائج جيدة، عن طريق إعطاء قيمة للتفاعل بين مطوري البرمجيات والمشغلين، والتعاون مع العملاء وإدارة التغيير (Kim et al., 2013)؛ وتعد المنهجية الرشيقة أحد أساليب إدارة المشروعات التي تهدف إلى تقليل التكلفة والوقت وتطوير جودة وتسليم المنتجات، عن طريق تقسيم مشروعات الأعمال إلى مهام صغيرة تدريجية وقابلة للتكرار تعرف بالسباقات Sprints والتي تستغرق عادة فترة أسبوع إلى أربعة أسابيع، بالإضافة إلى السعي نحو تعاون جميع أصحاب المصالح من خلال عقد اجتماعات للتواصل بشكل يومي وفقا لأسلوب Scrum (Agarwal, 2021).

وبالتالي يمكن القول إن ظهور مصطلح Agile يرجع إلى الاستخدام الأول في تطوير البرمجيات بداية من عام ٢٠٠١، للتأكيد على القرارات الجماعية القائمة على فريق العمل، والتعاون مع العملاء (Beerbaum, 2020). فهو مصطلح يعني القدرة على التحرك بسرعة وسهولة، والقدرة على الإبداع والتفكير بسرعة وبطريقة ذكية، والاستجابة للتغيير (Agarwal, 2021; Catton and Panavalli, 2020). وقد أصبح Agile يستخدم حاليا في كل وظائف المنظمة بما فيها وظائف خطي الدفاع الثاني والثالث (Agarwal, 2021)؛ وذلك بهدف التوافق مع تأثيرات التطور التكنولوجي على طرق أداء العمل، واستكشاف التكنولوجيا الجديدة والتكيف معها لتدعيم المركز التنافسي ومواجهة المخاطر (ACIIA and SGV, 2021).

وقد حددت دراسة (KPMG, 2019) نشأة وتطور استخدام المنهجية الرشيقة في خمسة مراحل كما يلي:

١- الفترة من ١٩٨٠ إلى ١٩٨٩: وخلال هذه الفترة اشتهر نظام الإنتاج المطبق في شركة تويوتا وبدأ استخدام نظام الانتاج Lean مع لفت الانتباه إلى منهج Scrum داخل الإنتاج.

٢- الفترة من ١٩٩٠ إلى ١٩٩٩: اتسمت هذه الفترة بالتعامل مع منهج Scrum وأساليب Lean في تطوير البرمجيات، وظهرت مناهج أخرى في صناعة تطوير البرمجيات.

٣- الفترة من ٢٠٠٠ إلى ٢٠٠٩: تعد هذه الفترة من أهم فترات تطور المنهجية الرشيقة حيث تم توقيع ما يعرف بالبيان الرسمي للمنهجية الرشيقة Agile Manifesto، وبدأ التوسع في استخدام هذه المنهجية داخل صناعة تطوير البرمجيات.

٤- الفترة بداية من ٢٠١٠: بدأ تطبيق المنهجية الرشيقة في الأعمال بخلاف تكنولوجيا المعلومات، مثل مشروعات التحسين المستمر للمنتجات، كما بدأت هولندا في تطبيق المنهجية الرشيقة في مجال المراجعة الداخلية.

٥- التطورات الأخيرة والتوقعات المستقبلية: وتشهد الفترة الراهنة التوجه نحو تطبيق المنهجية الرشيقة في جميع أنشطة منظمات الأعمال داخل خط الدفاع الأول، وداخل خط الدفاع الثاني في مجال إدارة المخاطر والالتزام، بالإضافة إلى المراجعة الداخلية الرشيقة؛ ومن المتوقع أن تطبق وظائف المراجعة الداخلية المنهجية الرشيقة وإن اختلفت درجة تطبيق هذه المنهجية من منظمة إلى أخرى.

وتشير دراسة (Galvanize, 2020) إلى تصاعد الاهتمام بممارسات المراجعة الداخلية الرشيقة في الوقت الراهن، حيث قدرت الدراسة أن ٥٥% من مجموعات المراجعة الداخلية تستخدم حاليا المنهجية الرشيقة أو تفكر في استخدامها.

٢/٤ مفهوم المراجعة الداخلية الرشيقة Agile Internal Audit:

يتمثل الاختلاف الأساسي بين المراجعة الداخلية التقليدية والمراجعة الرشيقة في المرونة، حيث تركز المراجعة التقليدية على التخطيط الصارم والذي يتم قبل البدء في المهام وفي مرحلة واحدة، بينما تركز المراجعة الداخلية الرشيقة على التخطيط المرن والمتكرر وعلى أساس مستمر، كما أن مراحل المراجعة التقليدية تتطلب فترة زمنية تصل إلى ثمانية أسابيع أو أكثر من ذلك، بينما يحتاج إكمال كل مرحلة في المراجعة الرشيقة فترة زمنية أقل بكثير، بالإضافة إلى أن التركيز الأساسي في المراجعة الرشيقة على التعاون والتواصل بين فريق المراجعة وأصحاب المصالح طوال العمل بأكمله (Galvanize, 2020).

وتعتبر المراجعة الداخلية الرشيقة منهجية تكرارية تم تصميمها لتعظيم القيمة، وتمكين وظيفة المراجعة الداخلية من العمل بفعالية ومرونة والاستجابة للاحتياجات والأولويات المتغيرة، فهي تمثل منهج يساعد على إحداث تغيير في السلوك والثقافة (Catton and Panavalli, 2020).

وتصف دراسة (Wright, 2019) المراجعة الداخلية الرشيقة بأنها تحول في أعمال المراجعة التقليدية، حيث تتضمن المراجعة الرشيقة تطوير الأعمال، التخطيط المتكرر، العمل

القائم على الفريق، التحركات السريعة في أوقات محددة، الاجتماعات اليومية، التعاون مع عملاء المراجعة وأصحاب المصالح، والإصدار المتكرر لنتائج وتقارير المراجعة.

كما حددت دراسة (Wright, 2019) مجموعة من السمات المشتركة للمراجعة الداخلية الرشيقة، التي تتمثل فيما يلي:

١- التركيز على القيمة بدلا من التركيز على أهداف المراجعة: بينما تركز المراجعة الداخلية التقليدية على تحديد أهداف المراجعة أثناء مرحلة التخطيط، فإن المراجعة الرشيقة تركز مقدما على القيمة عند ارتباط المراجعة، وبالتالي يتحقق هدف خلق القيمة عندما تتوافق مخرجات عملية المراجعة مع أهداف واستراتيجية الشركة.

٢- تعزيز التعاون مع عميل المراجعة: تعتمد المراجعة الداخلية الرشيقة على اعتبار عملاء المراجعة أحد مكونات فريق العمل الرشيق، وهذا يؤدي إلى زيادة التفاعل بين فريق المراجعة وعميل المراجعة، مما يؤدي إلى تحسين الاتصال بين الطرفين.

٣- الانضباط الزمني: وفقا للمنهجية الرشيقة يتم تحديد دورات عمل ذات فترات زمنية ثابتة، وهذا يؤدي إلى تحقيق الانضباط وإكمال عمليات المراجعة في الوقت المحدد.

٤- تقديم الرؤى والاستجابة في الوقت المناسب: نظرا لأن عملاء المراجعة يشاركون في مشروعات المراجعة الرشيقة فإنهم يحصلون على ملاحظات ورؤى متزامنة طوال عملية المراجعة، ولا يحدث تأخير في نقل هذه الرؤى والملاحظات كما يحدث في المراجعة التقليدية، وبالتالي يتمكن عملاء المراجعة من البدء في صياغة استجابات فورية للمخاطر.

٥- تقليل الخلافات: نظرا لمشاركة عملاء المراجعة الوثيقة في مهمة المراجعة الداخلية الرشيقة، فإن ذلك يؤدي إلى مناقشة نتائج المراجعة وفحصها بشكل متبادل والاتفاق عليها بشكل متزامن مع فريق المراجعة، وبالتالي تنخفض درجة الخلاف بين الطرفين، ويزيد احتمال تبني عملاء المراجعة لنتائج المراجعة واتخاذ مواقف أقوى بشأن الاستجابة لهذه الملاحظات والنتائج.

٦- ترشيد عملية التوثيق: ينصب تركيز المراجعة الداخلية الرشيقة على زيادة كفاءة المراجعة، واستبعاد العناصر غير الضرورية وبالتالي تبسيط المستندات وترشيد استخدام الوثائق.

٣/٤ منافع المراجعة الداخلية الرشيقة:

يرى (Kim et al., 2013) أن المنهجية الرشيقة تلبي احتياجات العملاء بشكل أكثر سرعة وفعالية؛ وتشير دراسة (Beerbaum, 2020) إلى أن المراجعة الداخلية الرشيقة تتضمن فرصا جديدة لخلق القيمة، وليس مجرد الحفاظ على القيمة، كما أن منظمات الأعمال التي تطبق

المنهجية الرشيقة أكثر قدرة على استشعار التغيرات البيئية، والاستجابة بسهولة للأحداث التي يمكن التنبؤ بها، وكذلك الأحداث التي لا يمكن التنبؤ بها. بالإضافة إلى أن المراجعة الداخلية الرشيقة تنمي التعاون داخل الفريق والتخطيط المستمر، وكذلك تدعم التقييم والتعلم الدائم وتحديد الأخطاء واقتراح الحلول (Agarwal, 2021). كما أثبتت دراسة (Gislen, 2016) أن استخدام المراجعة الداخلية الرشيقة يشجع على الالتزام بمعيار ISO 9001، كما أنه يؤدي إلى تحسن كبير في مؤشرات الأداء الرئيسية، وأشارت الدراسة إلى أن المنهجية الرشيقة يمكن استخدامها كطريقة لتحسين الجودة بشكل عام والتوافق مع نظم الجودة الرسمية.

وقد حددت دراسة (Catton and Panavalli, 2020) المنافع التالية للمراجعة الداخلية الرشيقة:

١- تحسين قدرة فريق المراجعة الداخلية على تغيير مسار العمل بشكل أسهل في فترات الأزمات والاستجابة للمخاطر وتقييم النتائج بشكل أسرع، نظرا لأنها تعتمد على تكرارات ذات فترة قصيرة في العمل، ويترتب على ذلك التركيز على الأمور عالية القيمة بدلا من التركيز على أهداف المراجعة والتي قد تكون ذات تأثير أقل.

٢- تسهم في تطوير فريق العمل متعدد التخصصات والوظائف، مع توفير رؤية شاملة لمختلف المجالات الوظيفية مثل العمليات والتمويل وتكنولوجيا المعلومات والالتزام، بدلا من المنهج التقليدي الذي يقسم فرق المراجعة إلى مجالات وظيفية لكل منها مسئولية خاصة بها.

٣- زيادة مشاركة أصحاب المصالح من خلال التسليم المبكر والمستمر للتقارير، ولإرضاء أصحاب المصالح الرئيسيين يتم صياغة اتفاق قبل البدء في العمل لتعزيز المشاركة والتعاون المستمر طوال دورة المراجعة بالكامل، ويتضمن هذا الاتفاق تحديد معايير النجاح ووتيرة الاتصال والمخرجات المطلوبة.

٤- تركز على العمليات أكثر من النتائج، لذا فهي توفر بيئة عمل آمنة لأعضاء الفريق لتحمل المخاطر عند تجربة طرق جديدة للعمل والتكيف مع الأزمات (مثل أزمة كورونا)؛ ويسمح ذلك لفريق المراجعة بالتطور والتحسين المستمر من خلال المناقشات الهادفة حول الممارسات الناجحة وغير الناجحة.

وتشير دراسة (Acharya, 2021) إلى أن المحصلة النهائية لاستخدام المنهجية الرشيقة هي تعزيز قيمة الأعمال، إلا أن تطبيق هذه المنهجية بشكل غير مناسب أو غير متسق قد يؤدي إلى نتائج سلبية، لذا يجب توخي الحذر عند إجراء التقييم الشامل لاحتياجات العمل وكيفية دمج التغييرات المطلوبة لتطبيق المراجعة الداخلية الرشيقة في منظمات الأعمال. كما أنه لا توجد

طريقة واحدة لتطبيق مبادئ المراجعة الداخلية الرشيقة تناسب جميع الظروف، لذا يجب على إدارة المراجعة الداخلية تحديد الطريقة المناسبة لتطبيق العمل الرشيق داخل فريق المراجعة وداخل المنظمة، بالإضافة إلى أن المنهجية الرشيقة ليست بالتأكيد واجبة التطبيق في جميع منظمات الأعمال حيث يجب أخذ البيئة والثقافة التنظيمية في الحسبان (KPMG, 2019; KPMG, 2020a).

٤/٤ مبادئ المراجعة الداخلية الرشيقة:

تستند المبادئ والقيم المستخدمة في المراجعة الداخلية الرشيقة على "البيان الرسمي لـــ Agile" والذي تم صياغته من خلال مجموعة من قادة تطوير البرمجيات، للتغلب على تحديات وقيود مناهج العمل التقليدية (Catton and Panavalli, 2020)؛ ومن خلال الاعتماد على المبادئ الإسترشادية الواردة في البيان الرسمي لـــ Agile حددت دراسة (Bakertilly, 2019) المبادئ التالية للمراجعة الداخلية الرشيقة:

١- الأولوية القصوى هي تلبية احتياجات لجنة المراجعة وإضافة القيمة، عن طريق التحديد المبكر والمستمر للمخاطر وتقارير المراجعة المؤثرة وذات القيمة المرتفعة.

٢- تقبل التغيير في منهج المراجعة في أي مرحلة من مراحل العمل الميداني، حيث تسهم التغييرات الناتجة عن العمليات الرشيقة في زيادة منفعة المراجعة وتعظيم القيمة للإدارة وأصحاب المصالح.

٣- القيام بعمليات مراجعة مؤثرة وبشكل متكرر، وتعديل خطة المراجعة باستمرار لتحقيق أقصى قيمة ممكنة.

٤- ضرورة التواصل المستمر طوال مشروع المراجعة بين المراجعين وأصحاب الأعمال.

٥- الثقة بفريق المراجعة، والسماح لهم بتخطي الطرق التقليدية في العمل، للحصول على نتائج تفيد في التعامل مع المخاطر وتعظيم القيمة.

٦- المقياس الأساسي للتقدم والنجاح هو تقارير المراجعة التي تتناول المخاطر الأساسية والفرص والنتائج المتوافقة مع الأهداف الاستراتيجية لمنظمات الأعمال.

٧- الطريقة الأكثر كفاءة وفعالية لنقل المعلومات بين المراجعين والأطراف الخاضعة للمراجعة هي الحوار وجها لوجه، والاستفادة من تكنولوجيا مؤتمرات الفيديو عند الضرورة.

٨- العمليات الرشيقة تعزز المراجعة المستدامة؛ ويجب أن يحافظ كل من المراجعين والخاضعين للمراجعة ومنظمات الأعمال على وتيرة ثابتة لفترة زمنية طويلة.

٩- الاهتمام المستمر بالنتائج، وتقديم نتائج مؤثرة تدعم المنهجية الرشيقة.

١٠- العمليات المؤثرة، والاختبارات، والنتائج أكثر أهمية من الدقة والتوثيق.

٥/٤ المكونات الأساسية للمراجعة الداخلية الرشيقة:

يعتمد تطبيق المراجعة الداخلية الرشيقة على عدة مكونات يمكن إيجازها فيما يلي (Deloitte, 2017; KPMG, 2019; Galvanize, 2020; Agarwal, 2021):

١- قائمة أعمال المراجعة المتراكمة Audit Backlog: هي قائمة مشابهة لخطة المراجعة لكنها تتسم بالمرونة، وتحتوي على مجموعة من البنود التي يتم تحديدها وفقا لاحتياجات أصحاب المصالح ولجنة المراجعة ومجلس الإدارة، وهذه البنود يتم مراجعتها من خلال فريق المراجعة الداخلية الرشيقة؛ وتتميز هذه القائمة بإمكانية استبعاد أو إضافة بعض البنود المحددة بها، وفقا للمخاطر المتوقعة والقيمة المضافة للعنصر الخاضع للمراجعة، بدلا من التركيز على البنود التي تم تحديدها مسبقا في خطة المراجعة السنوية التقليدية، حيث يمكن للمراجعين الداخليين من خلال قائمة الأعمال المتراكمة معالجة قضايا ناشئة ومستجدة تقع ضمن اهتمامات أصحاب المصالح؛ لذا يجب أن يتفق كل من المراجعين وأصحاب المصالح على كيفية اختيار البنود التي تحتوي عليها القائمة والقيمة المتوقعة من فحص هذه البنود وذلك قبل إضافة أي بند إلى القائمة.

٢- تعريف الاستعداد Definition of Ready (DoR): يعرف البند الموجود في قائمة أعمال المراجعة المتراكمة بأنه جاهز عندما يتفق كل من المراجعين الداخليين وأصحاب المصالح على ما سيتم فحصه ومراجعته، وعلى الهدف من المراجعة، والقيمة التي يتم الحصول عليها نتيجة مراجعة البند، كما يشمل تعريف الاستعداد أيضا ضرورة توفير الموراد اللازمة لإجراء المراجعة؛ وعند الوفاء بمتطلبات تعريف الاستعداد يبدأ فريق المراجعة الداخلية الرشيقة في عمله وتأدية مهامه.

٣- سباقات المراجعة Audit Sprints: عندما يبدأ عمل وظيفة المراجعة الداخلية الرشيقة ينتقل البند من قائمة الأعمال المتراكمة، ويتم تقسيم المهام المرتبطة بهذا البند إلى موضوعات محددة قابلة للمراجعة تسمى بسباقات المراجعة Sprints، والتي تتطلب اكتمال التنفيذ في وقت زمني قصير ومحدد؛ وهذا الوقت الزمني يتم تحديده من جانب فريق المراجعة لنفسه كإطار زمني لإتمام المهمة أو مجموعة المهام؛ وهذه العملية تتضمن التحسين المستمر من خلال الاجتماعات التفاعلية الأسبوعية، كما تنظم وظيفة المراجعة الداخلية في نهاية كل مهمة sprint عرضا توضيحيا للخاضعين للمراجعة يتضمن الملاحظات التي تم اكتشافها ويستعرض الحلول ويتلقى التعليقات على هذه الملاحظات من قبل الخاضعين للمراجعة.

٤- تعريف الإنجاز **Definition of Done (DoD):** يصف تعريف الإنجاز مخرجات سباقات المراجعة **Sprints** المطلوبة، ويمكن التعبير عن تعريف الإنجاز كمستوى التأكيد، مجموعة المهام المكتملة، قائمة الملاحظات والقضايا التي تم تحديدها، المخاطر أو التوصيات، والتقرير أو مسودة التقرير، وذلك في ضوء تطلعات أصحاب المصالح ووظيفة المراجعة الداخلية؛ ويساعد تعريف الإنجاز على تحديد اللحظة التي يعتبر فيها سباق المراجعة مكتمل، وبالتالي أثناء سباق المراجعة وبمجرد الوصول إلى نقطة تعريف الإنجاز تكون عملية المراجعة قد انتهت.

٥- اجتماعات **Scrums:** هي عبارة عن اجتماعات انتقادية قصيرة تستغرق من ١٥ إلى ٣٠ دقيقة، وتنعقد يوميا بين أعضاء فريق المراجعة الرشيقة وأصحاب المصالح الرئيسيين، ويغطي هذا الاجتماع بعض التساؤلات مثل:

- ماذا فعل فريق المراجعة الرشيقة بالأمس؟
- ماذا سيفعل الفريق اليوم؟
- ما هي معوقات سباق/مهمة المراجعة الحالية **sprint**؟
- ما هي القضايا المحتملة التي قد تواجه الفريق أو يهتم بها أصحاب المصالح؟

٦/٤ أثر تطبيق المراجعة الداخلية الرشيقة على مبادئ الممارسة المهنية:

تطبيق المراجعة الداخلية الرشيقة لا يعني عدم الاتساق مع معايير الممارسة المهنية للمراجعة الداخلية، أو المتطلبات التنظيمية والتشريعية المتعلقة بخدمات التأكيد وجودة التنفيذ والتقرير، ولكن التطبيق السليم للمنهجية الرشيقة يسمح لمنظمات الأعمال بالحصول على مزايا هذه المنهجية وتحسين الجودة وإضافة القيمة دون الإخلال بالمعايير والمتطلبات، وسوف تساعد المعرفة بالمنهجية الرشيقة وتحديد النتائج المستهدفة في التوافق مع المبادئ الجوهرية للمراجعة الداخلية **(Agarwal, 2021).**

وبمراجعة المعايير الدولية للممارسة المهنية يتبين تقسيم المعايير إلى معايير ترتبط بتصميم وظيفة المراجعة الداخلية (معايير السمات المجموعة ١٠٠٠)، ومعايير أداء المراجعات (معايير الأداء المجموعة ٢٠٠٠)؛ كما يتضح أن تطبيق المنهجية الرشيقة يؤثر على الإلتزام بالمعايير، إلا أن ذلك لا يعني الإخلال بمعايير الممارسة المهنية؛ فعلى سبيل المثال يتطلب معيار برنامج العمل رقم (٢٢٤٠) وجود برنامج عمل معتمد قبل البدء في العمل الميداني، إلا أن هذا المعيار يوفر مساحة لإجراء تعديلات على برنامج المراجعة أثناء مرحلة العمل الميداني.

وقد تناولت دراسة (KPMG, 2019) التأثير المحتمل لاتباع المراجعة الداخلية الرشيقة على الالتزام بالمعايير الدولية للممارسة المهنية كما يلي:

١- يتأثر معيار الكفاءة المهنية (١٢١٠) بتطبيق المنهجية الرشيقة، حيث تتطلب المراجعة الداخلية الرشيقة معارف ومهارات مختلفة في المراجع الداخلي، فعلى سبيل المثال عند العمل بأسلوب Scrum يجب أن يتوافر ضمن فريق المراجعة أحد المتخصصين على الأقل يسمى the Scrum Master وهو المسئول عن توجيه الفريق وإدارة العمل في الاتجاه الصحيح.

٢- يتطلب معيار برنامج تحسين وتأكيد الجودة (١٣٠٠) تقييم جودة وظيفة المراجعة الداخلية وتحديد التحسينات اللازمة، من خلال توثيق جميع الأنشطة بشكل كاف حتى يتمكن المراجع المستقل من إعادة المراجعة بناء على الوثائق، ويشكل هذا المعيار أحد تحديات المراجعة الداخلية الرشيقة في ظل ميل المراجعة الداخلية الرشيقة إلى تبسيط المستندات وتوثيق الإجراءات عالية الأهمية.

٣- يتأثر معيار التخطيط (٢٠١٠) بطريقة عمل المنهجية الرشيقة، والتي تعتمد على عدم التحديد المسبق لطريقة الوصول إلى أهداف المراجعة، كما أن التغيير في خطة المراجعة السنوية أو قائمة الأعمال المتراكمة للمراجعة يتطلب انتباه وظيفة المراجعة الداخلية بشأن تحديد أولويات المراجعة بناء على المخاطر.

٤- يتأثر معيار التخطيط للمهمة ومعيار إعداد برنامج العمل (٢٢٠٠ /٢٢٤٠) بالطريقة المرنة للعمل وفقا للمنهجية الرشيقة، حيث يتم استخدام أسلوب السباقات القصيرة للمراجعة Sprints وتقسيم نطاق المراجعة إلى عدة أجزاء فرعية، والعمل وفقا لأسلوب التكرارات، وأداء الأعمال في فترات زمنية قصيرة، بدلا من العمل التقليدي وفقا لجدول أعمال متسلسل ثابت يحدد في بداية العام؛ ولكن هذه التغييرات في نطاق وبرنامج العمل يجب أن يتم المصادقة عليها من قبل الرئيس التنفيذي للمراجعة الداخلية.

٥- دعم معيار توثيق المعلومات (٢٣٣٠)، إذ أن تطبيق المراجعة الداخلية الرشيقة يؤدي إلى إنتاج طريقة أكثر كفاءة في توثيق المعلومات، وتوفير مسار مراجعة واضح فيما يتعلق بكيفية التوصل إلى الملاحظات والنتائج.

٥- إطار مقترح لاستخدام المنهجية الرشيقة في تطوير أداء المراجعة الداخلية

تناولت الدراسة في القسم الثالث مفهوم مخاطر الأمن السيبراني، وأهم الجهود التنظيمية في هذا المجال، وانتهى هذا القسم بتحديد دور المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني ومدى فعالية هذا الدور؛ وتناول القسم الرابع ظهور المنهجية الرشيقة كأحد أساليب

تطوير المراجعة الداخلية، وكذلك مفهوم ومبادئ ومنافع المراجعة الداخلية الرشيقة، وتناول القسم الرابع أيضا مكونات المراجعة الداخلية الرشيقة؛ وفي هذا القسم ومن خلال الاستفادة من مساهمات الدراسات السابقة وجهود الهيئات التنظيمية والمهنية سوف يتم اقتراح إطار لتطوير أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني من خلال استخدام المنهجية الرشيقة.

١/٥ أهداف الإطار المقترح:

يهدف هذا الإطار إلى توفير مجموعة من المقترحات تسهم في تطوير أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني وذلك من خلال تطبيق المنهجية الرشيقة كأحد المنهجيات الحديثة للتطوير، ويمكن تقسيم هذا الهدف الرئيسي للأهداف الفرعية التالية:

١- تحديد مفاهيم الأمن السيبراني والمراجعة الداخلية الرشيقة.

٢- تحديد الأنشطة التي تؤديها المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني.

٣- تحديد خطوات تطبيق المراجعة الداخلية الرشيقة لمواجهة مخاطر الأمن السيبراني.

٢/٥ مفاهيم الإطار المقترح:

يعتمد هذا الإطار على المفاهيم التالية:

١- مفهوم الأمن السيبراني: يشير الأمن السيبراني إلى جميع الأنشطة والعمليات والإجراءات اللازمة لحماية نظم المعلومات والاتصالات من مختلف الانتهاكات بالإضافة إلى منع أو الحد من الآثار المرتبطة بهذه الانتهاكات.

٢- مفهوم مخاطر الأمن السيبراني: هي أنشطة غير مشروعة تتعرض لها البنية الأساسية للمنظمة عن طريق استغلال الثغرات الأمنية في نظم المعلومات، وذلك بهدف التأثير السلبي في جميع أنشطة المنظمة وإمكانياتها، وإلحاق الضرر المادي بها وبسمعتها والكشف عن معلومات المنظمة أو إجراء تعديلات عليها أو تدمير هذه المعلومات.

٣- مفهوم المراجعة الداخلية الرشيقة: هي طريقة للتفكير تركز على القيمة وتعزيز التعاون مع أصحاب المصالح لتقليل الخلافات حول نتائج المراجعة، وتحقيق الانضباط الزمني في تنفيذ مهام المراجعة، وتقديم الأفكار وتوفير الاستجابات في الوقت المناسب، وذلك من خلال تطوير الأعمال وتكرار التخطيط والعمل القائم على التعاون بين فرق العمل.

٣/٥ مبادئ الإطار المقترح:

١- تجنب الأفكار الخاطئة عند تطبيق المراجعة الداخلية الرشيقة: وفقا لتقرير (Deloitte, 2018) تم ملاحظة بعض الأفكار الخاطئة حول منهجية المراجعة الرشيقة مثل:

- إن فريق المراجعة الرشيقة يمكنه أن يفعل ما يشاء، والحقيقة أن المنهجية الرشيقة تعتمد على وضع ضوابط واضحة لعملية التطوير يتبعها أعضاء فريق المراجعة، مثل تعريف الإنجاز DoD والذي يعد معيارا لاكتمال العمل.
- إن المنهجية الرشيقة لا ينتج عنها وثائق، والحقيقة أن المراجعة الرشيقة تسهم في إنتاج وثائق أكثر ملاءمة وأكثر صلاحية للاستخدام.
- إن المنهجية الرشيقة لا تتبع ممارسات إدارة المشروع، والحقيقة أن المراجعة الرشيقة تتبنى منهج مختلف لإدارة المشروع بما يحقق الأهداف بأعلى كفاءة ممكنة.

٢- التدرج في التطبيق: تعد المنهجية الرشيقة من المنهجيات الحديثة التي تتطلب التدرج في تطبيقها تجنبا لمشاكل التطبيق الخاطئ الناتج عن عدم الإلمام والمعرفة الكاملة بجوانب تطبيق هذه المنهجية، بالإضافة إلى عدم التسبب في تعطيل الأعمال كنتيجة لنقص مهارات فرق المراجعة الرشيقة، والتي تحتاج إلى فترة من التدريب للتحول من تطبيق أسلوب المراجعة التقليدية إلى المراجعة الرشيقة.

٣- الوضوح: يستخدم الإطار الحالي مصطلحات قابلة للفهم والاستخدام من جانب جميع أنواع المنظمات، في ظل انتشار المعلومات عن الهجمات السيبرانية ومخاطرها وتأثيراتها، بالإضافة إلى دور المراجعة الداخلية في إدارة هذا النوع من المخاطر، والحاجة إلى استخدام المناهج الحديثة مثل المنهجية الرشيقة لتطوير أداء المراجعة الداخلية.

٤- الحداثة: يقدم هذا الإطار رؤية تتوافق مع الأحداث المعاصرة والتي تتمثل في تزايد مخاطر الهجمات السيبرانية، ودور المراجعة الداخلية في إدارة هذه المخاطر، والاهتمام المتزايد من جانب الهيئات التنظيمية والمهنية بتطوير أداء المراجعة الداخلية من خلال استخدام المنهجية الرشيقة.

٤/٥ أنشطة المراجعة الداخلية الرشيقة:

يمكن أن تؤدي المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني الأنشطة التالية:

١- المشاركة في وضع استراتيجيات وسياسات الأمن السيبراني.

٢- المشاركة في تقييم واختبار مخاطر الأمن السيبراني.

٣- تقييم فعالية الخطط الموضوعة لمواجهة مخاطر الأمن السيبراني.

٤- تقييم الضوابط الرقابية الموضوعة لتحقيق الأمن السيبراني، والتحقق من فعالية إجراءات وحلول نظم الرقابة.

٥- تقديم التقارير اللازمة إلى الإدارة العليا ولجان المراجعة بشأن فعالية الأمن السيبراني وأية تهديدات أو مخاطر محتملة.

٦- التحقق من توافر الإجراءات والخطط البديلة لاستمرار النشاط في حال وقوع هجمات سيبرانية.

٧- تقييم طرق استجابة الإدارة ومدى ملاءمتها كرد فعل على الهجمات السيبرانية.

٨- تقييم أداء خطي الدفاع الأول والثاني أثناء وقوع الهجمات السيبرانية.

٩- اقتراح التحسينات الضرورية لضمان الاستعداد لمواجهة المخاطر السيبرانية في المستقبل.

٥/٥ مراحل تطبيق المراجعة الداخلية الرشيقة:

المرحلة الأولى: البداية:

يتمثل الاختلاف الأساسي بين مرحلة البداية في المراجعة الداخلية الرشيقة ومرحلة التخطيط في المراجعة الداخلية التقليدية في مستوى التفاصيل؛ حيث يتم بناء خطة المراجعة في المنهج التقليدي بالتفصيل الدقيق وتوضع خطط اختبار محددة بدقة، أما في المنهجية الرشيقة فيتم تأجيل التخطيط التفصيلي إلى مرحلة دورات العمل أثناء المراجعة وتوضع خطة أولية؛ ويعتمد تطوير خطة المراجعة الأولية في المنهجية الرشيقة على التعاون بين فريق المراجعة وأصحاب المصالح الرئيسيين في مشروع المراجعة.

وتركز خطة المراجعة الأولية التي يتم تطويرها في بداية المراجعة الداخلية الرشيقة على النقاط التالية:

١- توضيح القيمة المضافة من مراجعة مخاطر الأمن السيبراني.

٢- تحديد النطاق والأهداف الرئيسية لمشروع المراجعة والمرتبطة بالأمن السيبراني.

٣- التعرف على مخاوف الإدارة والقضايا محل الاهتمام والتي تكون على صلة بالتهديدات والهجمات السيبرانية.

٤- تحديد المجالات التي تستدعي التركيز عند التخطيط والاختبار وإعداد التقارير، والتي تشمل التعامل مع مخاطر الأمن السيبراني في مراحل التحديد والحماية والاكتشاف والرد واستعادة النشاط.

المرحلة الثانية: المنتصف:

قد يبدو أن هذا الجزء في عمل المراجعة الداخلية الرشيقة يماثل مرحلة العمل الميداني في المراجعة الداخلية التقليدية، إلا أن النظرة المتعمقة تكشف وجود بعض الاختلافات الجوهرية فيما يتعلق باجتماعات سباقات المراجعة Sprints التي تتم في نهاية كل مهمة، وعمليات تقييم

الأداء التي تتم في نهاية كل مهمة والتي يترتب عليها إجراء تغييرات أو تعديلات لتحسين العمل في مهام المراجعة التالية؛ كما أن هذا الجزء من العمل الرشيق يختلف عن المراجعة التقليدية فيما يتعلق بتقديم التقارير، حيث يتم الاحتفاظ بالملاحظات الواجب الإبلاغ عنها حتى اكتمال جميع أنشطة العمل الميداني في المراجعة التقليدية، بينما يتم الإبلاغ عن هذه الملاحظات في المراجعة الداخلية الرشيقة بنهاية كل مهمة/سباق **Sprint** دون الانتظار حتى انتهاء جميع المهام.

وفي هذا الجزء من المراجعة الداخلية الرشيقة يتم تقسيم أعمال المراجعة في دورات متتالية محددة الوقت يطلق عليها **Sprints**، ويتم التعامل مع هذه المهام كعناصر في قصة، حيث يتم بناء بعض الفصول/المهام بالاعتماد على الفصول/المهام السابقة، بينما يتم تأدية مهام معينة بشكل مستقل بذاتها دون وجود علاقة بينها وبين المهام الأخرى.

ويتم في هذه المرحلة تنفيذ الخطوات التالية:

١- إنشاء خطة عمل لكل مهمة/سباق مراجعة **sprint** وتسمى هذه الخطة بقائمة المهام المتراكمة **Audit Backlog** وتحدد هذه القائمة تسلسل الأعمال التي يجب تحقيقها في كل مهمة **sprint**، أهداف المهمة، المخاطر المتوقعة، وإجراءات الفحص والاختبار.

٢- يجري فريق المراجعة الرشيقة اجتماع مبدئي مع الإدارة وأصحاب المصالح الرئيسيين ليطلعهم على خطة سباقات المراجعة، وبمجرد اكتمال الخطة وأخذ آراء وتوقعات أصحاب المصالح في الاعتبار تبدأ عمليات الفحص والاختبار.

٣- يحدد لكل مهمة/سباق مراجعة مدة زمنية (تكون في الغالب أسبوع ويمكن أن تتراوح بين أسبوع إلى أربعة أسابيع) مع تحديد تاريخ بدء المهمة وتاريخ نهايتها وعدم السماح بتغيير هذه التواريخ سواء تم اكتمال المهمة الموجودة في قائمة **Backlog** أو لم تكتمل، وذلك بهدف تعزيز الانضباط والمساءلة.

٤- يتم عقد اجتماع يومي خلال دورة عمل المهام يسمى **a daily stand-up** يتناول فريق المراجعة خلاله الأعمال التي تم إنجازها في اليوم السابق والأعمال المخططة لليوم الحالي، وأي معوقات تواجه التقدم في العمل.

٥- يعقد في اليوم الأخير من مهمة المراجعة **Sprint** اجتماع مع الإدارة والخاضعين للمراجعة وأصحاب المصالح الرئيسيين، يتناول مناقشة الملاحظات التي توصل إليها فريق المراجعة وأية ردود على هذه الملاحظات، ويساعد هذا الاجتماع في توفير دعم لإعداد تقرير المراجعة، كما سوف يساعد عميل المراجعة على تطوير الاستجابات اللازمة بشأن

المشكلات التي تم اكتشافها أو تطوير خطط العمل لتلافي جوانب القصور التي كشفتها مهمة المراجعة.

٦- يقوم فريق المراجعة الداخلية الرشيقة بتقييم الأداء بنهاية كل مهمة/سباق لتحديد نقاط القوة والضعف ومجالات تطوير الأداء للاستفادة منها في المهام التالية، وتحسين أداء فريق المراجعة الداخلية الرشيقة.

٧- تبدأ مهمة جديدة **sprint** بعد انتهاء المهمة السابقة مع ملاحظة إضافة أية أعمال لم تكتمل في المهمة السابقة إلى قائمة الأعمال المتراكمة **Backlog** وإعادة تقييم مدى الحاجة لإضافة هذه الأعمال غير المكتملة لمهمة العمل الحالية أو لمهمات عمل لاحقة.

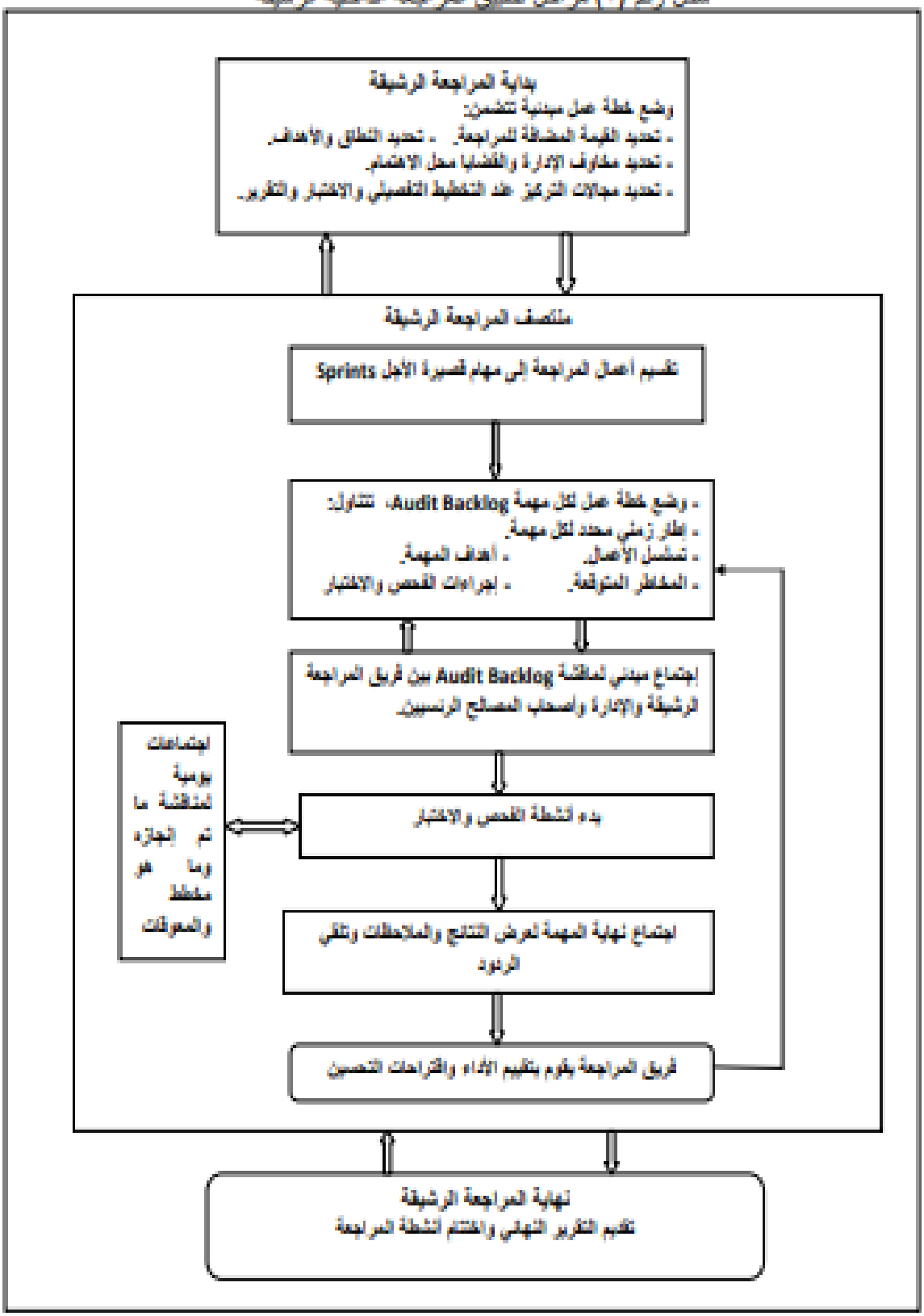
المرحلة الثالثة: النهاية:

يتضمن الجزء الأخير في مراحل عمل المراجعة الداخلية الرشيقة تقديم تقرير المراجعة النهائي واختتام مشروع المراجعة بمجرد اكتمال جميع أنشطة ومهام المراجعة **Audit Sprints**. ويجب أن يكون التقرير النهائي عبارة عن تجميع لما ورد بالتقارير التي تم تسليمها أثناء اجتماع نهاية كل مهمة عمل، بالإضافة إلى أية ملاحظات أخرى تم اكتشافها ولم تعرض في التقارير السابقة.

ونود التأكيد على أن شكل وتنسيق تقرير المراجعة الداخلية الرشيقة وكذلك توزيع هذا التقرير قد يختلف من منظمة إلى أخرى، أي أن تقارير المراجعة الرشيقة ليست نمطية وقد تكون ذات شكل فريد خاص بكل منظمة أعمال.

ويلخص الشكل التالي مراحل تطبيق المراجعة الداخلية الرشيقة:

شكل رقم (١) مراحل تطبيق المراجعة الداخلية الرشيقة



المصدر: من إعداد الباحثان

٦/٥ مزايا الإطار المقترح:

يحقق هذا الإطار عدة مزايا تتمثل فيما يلي:

١- زيادة الفهم لدور المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني.

٢- الاستفادة من أحد المناهج الحديثة لتطوير أداء المراجعة الداخلية.

٣- يلقي هذا الإطار الضوء على المنهجية الرشيقة من أجل توفير المعرفة الكافية لأبعاد هذه المنهجية ومراحل تطبيقها.

٤- يحدد هذا الإطار مراحل متتالية لتطبيق المنهجية الرشيقة في مجال تطوير أداء المراجعة الداخلية لمواجهة مخاطر الأمن السيبراني.

٦- الدراسة الميدانية

١/٦ منهجية الدراسة الميدانية:

تهدف الدراسة الميدانية إلى تحقيق ما يلي:

١- تقييم مدى إدراك عينة الدراسة لمخاطر الأمن السيبراني وتأثيراتها على مستوى منظمات الأعمال والمستوى القومي.

٢- التعرف على آراء عينة الدراسة بشأن قصور أداء المراجعة الداخلية التقليدية في مواجهة مخاطر الأمن السيبراني، وأسباب هذا القصور من وجهة نظرهم.

٣- التعرف على آراء عينة الدراسة بشأن إمكانية تطوير دور المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني من خلال استخدام المنهجية الرشيقة.

٤- تقييم مدى استعداد عينة الدراسة للتحول من المنهج التقليدي للمراجعة الداخلية إلى المراجعة الداخلية الرشيقة لتطوير الأداء في مواجهة مخاطر الأمن السيبراني.

١/١/٦ فروض الدراسة:

تحقيقا لأهداف هذه الدراسة، تم وضع عدة فروض في صيغة فرض العدم كما يلي:

الفرض الرئيسي الأول HO_1: لا توجد اختلافات معنوية بين آراء فئات المستقصى منهم بشأن مخاطر الأمن السيبراني وتأثيراتها.

ويمكن تقسيم هذا الفرض إلى فرضين فرعيين كما يلي:

الفرض الفرعي الأول HO_{11}: لا توجد اختلافات معنوية بين آراء فئات المستقصى منهم بشأن تزايد مخاطر الأمن السيبراني في الوقت الحالي وفي المستقبل.

الفرض الفرعي الثاني HO_{12}: لا توجد اختلافات معنوية بين آراء فئات المستقصى منهم بشأن تسبب مخاطر الأمن السيبراني في خسائر كبيرة على مستوى منظمات الأعمال وعلى المستوى القومي.

الفرض الرئيسي الثاني HO_2: لا توجد اختلافات معنوية بين آراء فئات المستقصى منهم بشأن قصور أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني، وأسباب قصور هذا الأداء.

ويمكن تقسيم هذا الفرض إلى فرضين فرعيين كما يلي:

الفرض الفرعي الأول HO_{21}: لا توجد اختلافات معنوية بين آراء فئات المستقصى منهم بشأن قصور أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني في الوقت الراهن.

الفرض الفرعي الثاني HO_{22}: لا توجد اختلافات معنوية بين آراء فئات المستقصى منهم بشأن أسباب قصور أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني في الوقت الراهن.

الفرض الرئيسي الثالث HO_3: لا توجد اختلافات معنوية بين آراء فئات المستقصى منهم بشأن إمكانية تطوير أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني من خلال استخدام المنهجية الرشيقة، واستعدادهم لتطبيق هذه المنهجية.

ويمكن تقسيم هذا الفرض إلى ثلاثة فروض فرعية كما يلي:

الفرض الفرعي الأول HO_{31}: لا توجد اختلافات معنوية بين آراء فئات المستقصى منهم بشأن إمكانية تطوير أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني من خلال استخدام مناهج التطوير الحديثة ومنها المنهجية الرشيقة.

الفرض الفرعي الثاني HO_{32}: لا توجد اختلافات معنوية بين آراء فئات المستقصى منهم بشأن عدم توافر المعرفة الكافية بالمنهجية الرشيقة كأحد مناهج تطوير أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني.

الفرض الفرعي الثالث HO_{33}: لا توجد اختلافات معنوية بين آراء فئات المستقصى منهم بشأن الاستعداد للتحول نحو المراجعة الداخلية الرشيقة لمواجهة مخاطر الأمن السيبراني.

٢/١/٦ أسلوب الدراسة:

استخدمت الدراسة الحالية أسلوب الدراسة المسحية من خلال قوائم الاستقصاء، وتم إدارة وتنفيذ الاستقصاء باستخدام التوزيع الشخصي والتوزيع الإلكتروني، كما تم التواصل مع المستقصى منهم للرد على الاستفسارات بشأن محتويات قائمة الاستقصاء، وذلك بهدف التأكد من الإجابة على جميع الأسئلة بشكل سليم وضمان الحصول على معدل ردود مناسب.

٣/١/٦ مجتمع وعينة الدراسة:

مجتمع الدراسة:

يتكون مجتمع الدراسة من ثلاث فئات كما يلي:

١- خطي الدفاع الأول والثاني وهم الإدارة العليا ومسئولي وحدات تكنولوجيا المعلومات (IT) بمنظمات الأعمال المالية وغير المالية.

٢- خط الدفاع الثالث وهم العاملين بإدارة المراجعة الداخلية بمنظمات الأعمال المالية وغير المالية.

٣- الباحثين من أساتذة الجامعات.

وتم تحديد الفئة الأولى والثانية من مجتمع الدراسة في ضوء نموذج خطوط الدفاع الثلاثة الصادر عن المعهد الأمريكي للمراجعين الداخليين، كما تم تضمين الباحثين في مجتمع الدراسة للاستفادة من آرائهم التي تعتمد على الدراسة العلمية والتقييم الموضوعي لموقف المراجعة الداخلية الراهن واقتراح الحلول للمشاكل التي تواجهها في الواقع العملي.

عينة الدراسة:

في ضوء المعادلة المقترحة من (Saunders et al., 2000) والتي تعتمد في حساب حجم العينة على متغيرين هما الحد الأدنى لحجم العينة المطلوب، ومعدل الردود المتوقع الحصول عليه؛ فقد تم الاسترشاد بعدة دراسات سابقة لتحديد هذين المتغيرين كما هو موضح في الجدول التالي:

جدول رقم (١) معدل الاستجابة في الدراسات السابقة

الدراسات السابقة	القوائم الموزعة	الردود	نسبة الردود
دراسة (Shamsuddin et al., 2018)	١٥٠	١٢٠	%٨٠
دراسة (الإبياري، ٢٠١٨)	٩٠	٥٧	%٦٣.٣
دراسة (Slapnicar et al., 2022)	٢٥٧	١٨٣	%٧١.٢
المتوسط الإجمالي	١٦٦	١٢٠	%٧٢.٢٩

وبتطبيق المعادلة التالية:

حجم العينة = (المتوسط الإجمالي للردود ×١٠٠) ÷ المتوسط الإجمالي لنسبة الردود

= (١٢٠ × ١٠٠) ÷ ٧٢.٢٩ = ١٦٦

وبالتالي فإن حجم العينة المطلوب للدراسة هو ١٦٦ مفردة، وتحوطا من انخفاض نسبة الردود فقد تم إضافة نسبة ٥% لحجم العينة المطلوب وبناء على ذلك تم توزيع ١٧٤ قائمة على عينة الدراسة.

٤/١/٦ تصميم قائمة الاستقصاء:

تم تصميم قائمة الاستقصاء كأداة لجمع البيانات اللازمة للدراسة الحالية، واستخدمت الأسئلة المغلقة ذات الإجابة بنعم أو لا، وكذلك الأسئلة الترتيبية وفقا لمقياس ليكارت الخماسي، واحتوت قائمة الاستقصاء على ثلاثة أقسام، تناول القسم الأول تقييم مدى إدراك عينة الدراسة لتزايد الهجمات السيبرانية والخسائر التي تتعرض لها منظمات الأعمال والاقتصاد القومي نتيجة لهذه الهجمات؛ وتناول القسم الثاني التعرف على آراء المستقصى منهم بشأن دور المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني ومدى فعالية هذا الدور، والأسباب التي تؤدي إلى قصور أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني؛ وتناول القسم الثالث استقصاء آراء عينة الدراسة بشأن دور المنهجية الرشيقة في تطوير أداء المراجعة الداخلية لمواجهة مخاطر الأمن السيبراني، والتعرف على آرائهم فيما يتعلق بمدى استعدادهم للتحول إلى استخدام المنهجية الرشيقة في تطوير المراجعة الداخلية.

٥/١/٦ تنفيذ الاستقصاء وجمع البيانات:

يوضح الجدول التالي القوائم الموزعة والقوائم المرفوضة بسبب عدم استيفائها لشروط التحليل، والقوائم الصحيحة التي تم إجراء التحليل الإحصائي عليها:

جدول رقم (٢) بيان بالقوائم الموزعة والقوائم التي أجري عليها التحليل

بيان	خطي الدفاع الأول والثاني		المراجعين الداخليين	الباحثين	الإجمالي	
	الإدارة العليا	مسئولي IT				
	عدد	عدد	عدد	عدد	عدد	نسبة
القوائم الموزعة	٤٤	٤٤	٤٤	٤٢	١٧٤	%١٠٠
القوائم المفقودة	٦	١١	٧	٦	٣٠	%١٧.٢٤
القوائم المستلمة	٣٨	٣٣	٣٧	٣٦	١٤٤	%٨٢.٧٥
القوائم المرفوضة	٤	٧	٦	ــ	١٧	%٩.٧٧
القوائم المقبولة	٣٤	٢٦	٣١	٣٦	١٢٧	%٧٢.٩٨

وتعد القوائم المقبولة وعددها ١٢٧ قائمة استقصاء والتي تمثل نسبة ردود ٧٢.٩٨% هي نسبة كافية للتحليل مقارنة بالدراسات السابقة في نفس المجال حيث بلغ حجم العينة ٧٢ مفردة في دراسة (Lois et al., 2021)، و٤٤ مفردة في ودراسة (Acharya, 2021)، و٤٧ مفردة في دراسة (Steinbart et al., 2013).

٦/١/٦ المعالجة الإحصائية للبيانات:

تم معالجة البيانات إحصائيا باستخدام حزمة البرامج الجاهزة **SPSS For Windows** وقد تم إعطاء الوزن النسبي (١) للإجابة بنعم والوزن النسبي (صفر) إذا كانت الإجابة لا؛ كما أعطيت الأوزان النسبية التالية للأسئلة الترتيبية:

موافق بشدة	موافق	موافق إلى حد ما	غير موافق	غير موافق على الإطلاق
خمس درجات	أربع درجات	ثلاث درجات	درجتان	درجة واحدة

وتم إجراء التحليلات الإحصائية التالية:

الإحصاء الوصفي: استخدمت مقاييس النزعة المركزية مثل الوسط الحسابي والانحراف المعياري لوصف البيانات وإجراء المقارنات بين فئات مجتمع الدراسة.

الإحصاء التحليلي: تم استخدام المقاييس التالية:

١- ألفا كرونباخ **Cronbach' Alpha** لتحديد مدى موثوقية إجابات عينة الدراسة على قائمة الاستقصاء وإمكانية تعميم نتائج الدراسة. وقد بلغت قيمة ألفا كرونباخ في ضوء تكرارات العينة ٠.٨٢٣ وهي تتعدي ٠.٦ مما يعني الوثوق في النتائج وإمكانية تعميمها.

٢- اختبار كروسكال واليز **Kruskal-Wallis** للكشف عن وجود اختلافات معنوية بين فئات العينة؛ فإذا كان مستوى المعنوية الإحصائية الناتج عن التحليل الإحصائي أقل من ٠.٠٥ يتم رفض فرض العدم وقبول الفرض البديل، أما إذا كان مستوى المعنوية الإحصائية أكبر من ٠.٠٥ فيتم قبول فرض العدم ورفض الفرض البديل.

٢/٦ تفسير نتائج التحليل الإحصائي:

١/٢/٦ مخاطر الأمن السيبراني وتأثيراتها:

سوف يتم في هذا الجزء التحقق من صحة الفرض الرئيسي الأول المرتبط بآراء فئات عينة الدراسة فيما يتعلق بمخاطر الأمن السيبراني وتأثيراتها على مستوى منظمات الأعمال وعلى المستوى القومي.

أ- تزايد مخاطر الأمن السيبراني:

يبين الجدول رقم (٣) مدى إدراك عينة الدراسة لمخاطر الأمن السيبراني، والتزايد المستمر لهذه المخاطر في الوقت الحالي وفي المستقبل.

جدول رقم (٣) إدراك المستقصى منهم لتزايد مخاطر الأمن السيبراني

الفئة	الوسط الحسابي	الانحراف المعياري	قيمة كروسكال واليز	المعنوية P.value
الإدارة العليا ومسئولي IT	٤.٦٠٠	١.٠٠٠	٢.٩٧٦	٠.٢٢٦
المراجعين الداخليين	٤.٣٦٣	٠.٨٠٩		
الباحثين	٤.٥٩٥	٠.٥٣٨		

توضح البيانات الواردة في الجدول رقم (٣) ما يلي:

١- سجلت درجة الموافقة على تزايد مخاطر الأمن السيبراني درجة مرتفعة في الفئات الثلاث، حيث بلغ الوسط الحسابي لنسبة الموافقة لدى الإدارة العليا ومسئولي IT (٤.٦٠٠)، وفي فئة المراجعين الداخليين (٤.٣٦٣)، وفي فئة الباحثين (٤.٥٩٥). ويلاحظ أيضا انخفاض قيمة الانحراف المعياري في الفئات الثلاثة مما يدل على ارتفاع درجة الاتفاق بين مفردات العينة في جميع الفئات.

٢- بلغت قيمة كروسكال واليز ٢.٩٧٦ بمستوى معنوية P.value بلغت ٠.٢٢٦ وهي أكبر من ٠.٠٥ مما يدل على عدم وجود اختلافات معنوية بين آراء فئات الدراسة الثلاثة بشأن تزايد مخاطر الأمن السيبراني في الوقت الحالي وفي المستقبل.

النتيجة: قبول الفرض HO_{11} القائل " لا توجد اختلافات معنوية بين آراء فئات المستقصى منهم بشأن تزايد مخاطر الأمن السيبراني في الوقت الحالي وفي المستقبل"

ب- تأثيرات مخاطر الأمن السيبراني:

يوضح الجدول رقم (٤) آراء عينة الدراسة بشأن التأثيرات الناتجة عن الهجمات السيبرانية على مستوى منظمات الأعمال وعلى مستوى الاقتصاد القومي.

جدول رقم (٤) تأثير مخاطر الأمن السيبراني

الفئة	الوسط الحسابي	الانحراف المعياري	قيمة كروسكال واليز	المعنوية P.value
الإدارة العليا ومسئولي IT	٤.٦٠٠	٠.٨١٦	٣.٢٥١	٠.١٩٧
المراجعين الداخليين	٤.٢٧٢	٠.٧٨٦		
الباحثين	٤.٦٥٩	٠.٥٢٢		

تدل البيانات الواردة في الجدول رقم (٤) على ما يلي:

١- سجلت درجة الموافقة على تأثيرات الهجمات السيبرانية على مستوى المنظمات وعلى المستوى القومي درجة مرتفعة في الفئات الثلاث، بقيمة مرتفعة للوسط الحسابي لنسبة الموافقة لدى الإدارة العليا ومسئولي IT (٤.٦٠٠)، المراجعين الداخليين (٤.٢٧٢)، والباحثين (٤.٦٥٩). ويلاحظ أيضا انخفاض قيمة الانحراف المعياري في الفئات الثلاثة

(٠.٨١٦)، (٠.٧٨٦)، (٠.٥٢٢) على التوالي، مما يعني ارتفاع درجة الاتفاق بين مفردات العينة في جميع الفئات بشأن تأثيرات الهجمات السيبرانية.

٢- سجل اختبار كروسكال واليز قيمة تبلغ ٣.٢٥١ بمستوى معنوية ٠.١٩٧ وهي تزيد عن ٠.٠٥ مما يعني عدم وجود اختلافات معنوية بين آراء فئات الدراسة بشأن تأثيرات مخاطر الأمن السيبراني.

النتيجة: قبول الفرض HO_{12} القائل "لا توجد اختلافات معنوية بين آراء فئات المستقصى منهم بشأن تسبب مخاطر الأمن السيبراني في خسائر كبيرة على مستوى منظمات الأعمال وعلى المستوى القومي"

٢/٢/٦ قصور أداء المراجعة الداخلية في مجال الأمن السيبراني وأسبابه:

سوف يتم في هذا الجزء التحقق من صحة الفرض الرئيسي الثاني والذي يتعلق بآراء عينة الدراسة بشأن وجود قصور في أداء المراجعة الداخلية لدورها في مواجهة مخاطر الأمن السيبراني وأسباب هذا القصور.

أ- قصور أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني:

توضح البيانات الواردة بالجدول رقم (٥) آراء فئات عينة الدراسة بشأن قصور أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني.

جدول رقم (٥) قصور أداء المراجعة الداخلية في مجال الأمن السيبراني

الفئة	الوسط الحسابي	الانحراف المعياري	قيمة كروسكال واليز	المعنوية P.value
الإدارة العليا ومسئولي IT	٤.٣٢٠	٠.٦٩٠	١.٠٨٦	٠.٥٨١
المراجعين الداخليين	٤.١٨١	٠.٩٨١		
الباحثين	٤.١٤٨	٠.٦٩٠		

يتضح من الجدول رقم (٥) ما يلي:

١- سجلت درجة الموافقة على قصور أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني درجة مرتفعة في الفئات الثلاث، حيث بلغ للوسط الحسابي لدرجة الموافقة لدى فئة الإدارة العليا ومسئولي IT (٤.٣٢٠)، ولدى المراجعين الداخليين (٤.١٨١)، والباحثين (٤.١٤٨). كما انخفضت قيمة الانحراف المعياري في الفئات الثلاثة لتسجل (٠.٦٩٠)، (٠.٩٨١)، (٠.٦٩٠) على التوالي، مما يعني ارتفاع درجة الاتفاق بين مفردات العينة في جميع الفئات فيما يتعلق بقصور أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني.

٢- بلغت قيمة كروسكال واليز ١.٠٨٦ بمستوى معنوية ٠.٥٨١ وهي تتعدى ٠.٠٠٥ وهذا يشير إلى عدم وجود اختلافات معنوية بين آراء فئات الدراسة بشأن قصور أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني.

النتيجة: قبول الفرض HO_{21} القائل "لا توجد اختلافات معنوية بين آراء فئات المستقصى منهم بشأن قصور أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني في الوقت الراهن"

ب- أسباب قصور أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني:

يبين الجدول رقم (٦) آراء فئات عينة الدراسة بشأن أسباب قصور أداء المراجعة الداخلية لدورها في مواجهة مخاطر الأمن السيبراني في الوقت الراهن.

جدول رقم (٦) أسباب قصور فعالية المراجعة الداخلية

البند	الإدارة العليا ومسئولي IT		المراجعين الداخليين		الباحثين		قيمة كروسكال واليز	المعنوية P.value
	الوسط الحسابي	الانحراف المعياري	الوسط الحسابي	الانحراف المعياري	الوسط الحسابي	الانحراف المعياري		
عدم توافر الخبرات اللازمة بالتكنولوجيا	٤.١٢٠	٠.٨٨١	٤.٠٩٠	٧.٠٠٦	٤.٢٥٥	٠.٨٢٠	٠.٨٤٢	٠.٦٥٦
تطبيق المنهج التقليدي	٤.١٢٥	١.٠٧٥	٤.٤٠٠	٠.٦٩٩	٤.٢٥٥	٠.٧٣٦	٠.٣١٩	٠.٨٥٣
عدم التواصل الفعال مع الإدارة وأصحاب المصالح	٤.١٦٠	٠.٨٥٠	٤.٠٠٠	٠.٧٧٤	٣.٨٧٢	٠.٨٤٩	٢.٠٢٥	٠.٣٦٣
عدم مرونة خطط المراجعة	٤.٢٤٠	٠.٨٣٠	٤.٠٠٠	٠.٦٣٢	٣.٩٧٨	٠.٧٩٣	١.٩٧٥	٠.٣٧٣
التأخير في تقديم تقارير المراجعة	٤.٠٤٠	٠.٩٧٨	٤.٠٠٠	٠.٦٤٢	٣.٧٠٢	٠.٩٣٠	٢.٥٥٩	٠.٢٧٨

في ضوء البيانات الواردة بالجدول رقم (٦) يتضح ما يلي:

١- سجلت جميع أسباب قصور أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني قيما أكبر من (٣) في جميع فئات الدراسة، وهذا يعني الموافقة على هذه الأسباب؛ إلا أن درجة الموافقة اختلفت من سبب إلى آخر، كما أن درجة الموافقة على السبب الواحد قد اختلفت أيضا من فئة إلى أخرى.

٢- سجل بند عدم مرونة خطط المراجعة الداخلية كأحد أسباب قصور أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني المرتبة الأولى من حيث الأهمية من وجهة نظر فئة الإدارة العليا ومسئولي IT بوسط حسابي بلغ (٤.٢٤٠)، يليه من حيث الأهمية بند عدم التواصل الفعال بين المراجعين الداخليين والإدارة وأصحاب المصالح الرئيسيين بوسط حسابي بلغ (٤.١٦٠)؛ بينما جاء بند التأخير في تقديم تقارير المراجعة كأحد أسباب قصور أداء المراجعة الداخلية في المرتبة الأخيرة من وجهة نظرهم بوسط حسابي بلغ (٤.٠٤٠).

٣- حقق بند تطبيق المنهج التقليدي في المراجعة كأحد أسباب قصور أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني المرتبة الأولى من حيث الأهمية من وجهة نظر فئة المراجعين الداخليين بوسط حسابي بلغ (٤.٤٠٠)، يليه في المرتبة الثانية من حيث الأهمية بند عدم توافر الخبرات اللازمة للمراجعين الداخليين في مجال التكنولوجيا والتحول الرقمي بوسط حسابي بلغ (٤.٠٩٠)، بينما جاء في المرتبة الأخيرة من الأهمية بند عدم التواصل الفعال بين المراجعين الداخليين والإدارة وأصحاب المصالح الرئيسيين بوسط حسابي بلغ (٤.٠٠٠) وانحراف معياري (٠.٧٧٤).

٤- جاء بند تطبيق المنهج التقليدي في المراجعة كأحد أسباب قصور أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني في المرتبة الأولى أيضا من حيث الأهمية من وجهة نظر فئة الباحثين بوسط حسابي بلغ (٤.٢٥٥) وانحراف معياري (٠.٧٣٦)، بينما جاء بند عدم توافر الخبرات اللازمة للمراجعين الداخليين في مجال التكنولوجيا والتحول الرقمي في المرتبة الثانية من وجهة نظرهم بوسط حسابي بلغ (٤.٢٥٥) وانحراف معياري (٠.٨٢٠)، واحتل بند التأخير في تقديم تقارير المراجعة المرتبة الأخيرة من وجهة نظر الباحثين بوسط حسابي بلغ (٣.٧٠٢).

٥- سجلت قيمة كروسكال واليز المناظرة لجميع البنود مستوى معنوية أكبر من ٠.٠٥ مما يعني عدم وجود اختلافات معنوية بين آراء فئات العينة بشأن أسباب قصور أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني.

النتيجة: قبول الفرض HO_{22} القائل "لا توجد اختلافات معنوية بين آراء فئات المستقصى منهم بشأن أسباب قصور أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني في الوقت الراهن"

٣/٢/٦ تطوير المراجعة الداخلية باستخدام المنهجية الرشيقة:

سوف يتم في هذا الجزء التحقق من صحة الفرض الرئيسي الثالث والذي يتعلق بآراء عينة الدراسة بشأن دور المنهجية الرشيقة في تطوير أداء المراجعة الداخلية لمواجهة مخاطر الأمن السيبراني.

أ- مدى إمكانية تطوير المراجعة الداخلية باستخدام المنهجية الرشيقة:

يوضح الجدول رقم (٧) آراء فئات عينة الدراسة بشأن إمكانية تطوير أداء المراجعة الداخلية من خلال استخدام المنهجية الرشيقة لمواجهة مخاطر الأمن السيبراني.

جدول رقم (٧) إمكانية تطوير أداء المراجعة الداخلية باستخدام المنهجية الرشيقة

الفئة	الوسط الحسابي	الانحراف المعياري	قيمة كروسكال واليز	المعنوية P.value
الإدارة العليا ومسئولي IT	٤.٤٤٠	٠.٧٦٨	١.٧٧٧	٠.٤١١
المراجعين الداخليين	٤.١٨١	٠.٧٥٠		
الباحثين	٤.٣١٩	٠.٦٦٢		

توضح بيانات الجدول رقم (٧) ما يلي:

١- تم تسجيل درجة موافقة مرتفعة في الفئات الثلاثة بشأن مدى إمكانية تطوير أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني من خلال استخدام المنهجية الرشيقة، حيث بلغت قيمة الوسط الحسابي لنسبة الموافقة لدى فئة الإدارة العليا ومسئولي IT (٤.٤٤٠)، ولدى المراجعين الداخليين (٤.١٨١)، والباحثين (٤.٣١٩). كما سجل الانحراف المعياري ارتفاعا في درجة الاتفاق بين آراء مفردات العينة داخل الفئات الثلاثة، حيث بلغت قيم الانحراف المعياري (٠.٧٦٨)، (٠.٧٥٠)، (٠.٦٦٢) على التوالي.

٢- بلغت قيمة كروسكال واليز ١.٧٧٧ بمستوى معنوية ٠.٤١١ وهي أكبر من ٠.٠٥ مما يعني عدم وجود اختلافات معنوية بين آراء فئات الدراسة بشأن إمكانية تطوير أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني من خلال استخدام المنهجية الرشيقة.

النتيجة: قبول الفرض HO_{31} القائل "لا توجد اختلافات معنوية بين آراء فئات المستقصى منهم بشأن إمكانية تطوير أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني من خلال استخدام مناهج التطوير الحديثة ومنها المنهجية الرشيقة "

ب- مدى توافر المعرفة الكافية لتطبيق المنهجية الرشيقة:

تبين البيانات الواردة بالجدول رقم (٨) آراء فئات عينة الدراسة بشأن مدى توافر المعرفة الكافية لاستخدام المنهجية الرشيقة في تطوير أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني.

جدول رقم (٨) توافر المعرفة الكافية بالمنهجية الرشيقة

الفئة	الوسط الحسابي	الانحراف المعياري	قيمة كروسكال واليز	المعنوية P.value
الإدارة العليا ومسئولي IT	٠.٢٤٠	٠.٤٣٥	٠.٦٠١	٠.٧٤١
المراجعين الداخليين	٠.٢٩٢	٠.٥٠٤		
الباحثين	٠.٣٦٤	٠.٤٦٢		

يتبين من الجدول السابق رقم (٨) ما يلي:

١- يشير الوسط الحسابي لآراء جميع الفئات إلى عدم توافر المعرفة الكافية بالمنهجية الرشيقة، حيث سجل الوسط الحسابي بشأن مدى توافر المعرفة الكافية عن المنهجية الرشيقة لدى

الإدارة العليا ومسئولي IT (٠.٢٤٠)، ولدى المراجعين الداخليين (٠.٢٩٢)، ولدى الباحثين (٠.٣٦٤).

٢- بلغت قيمة كروسكال واليز ٠.٦٠١ بمستوى معنوية ٠.٧٤١ وهي تزيد ٠.٠٥ مما يدل على عدم وجود اختلافات معنوية بين آراء فئات الدراسة بشأن مدى توافر المعرفة الكافية بالمنهجية الرشيقة كأحد أساليب تطوير أداء المراجعة الداخلية.

النتيجة: قبول الفرض HO_{32} القائل " لا توجد اختلافات معنوية بين آراء فئات المستقصى منهم بشأن عدم توافر المعرفة الكافية بالمنهجية الرشيقة كأحد مناهج تطوير أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني"

ج- مدى الاستعداد للتحول إلى تطبيق المنهجية الرشيقة إذا توافرت المعرفة الكافية:

يوضح الجدول رقم (٩) آراء فئات عينة الدراسة بشأن مدى الاستعداد للتحول إلى استخدام المنهجية الرشيقة في تطوير أداء المراجعة الداخلية بهدف زيادة فعاليتها في مواجهة مخاطر الأمن السيبراني؛ حيث تم عرض مجموعة من سمات المراجعة الداخلية الرشيقة على المستقصى منهم وطلب منهم تحديد درجة موافقتهم على تطبيق هذه السمات كمؤشر لمدى استعدادهم لتطبيق المنهجية الرشيقة.

جدول رقم (٩) سمات المراجعة الداخلية الرشيقة

البند	الإدارة العليا ومسئولي IT		المراجعين الداخليين		الباحثين		قيمة كروسكال واليز	المعنوية P.value
	الوسط الحسابي	الانحراف المعياري	الوسط الحسابي	الانحراف المعياري	الوسط الحسابي	الانحراف المعياري		
التركيز على خلق القيمة وليس أهداف المراجعة	٤.٥٠٠	٠.٥١١	٤.٣٦٤	٠.٦٧٤	٤.٢٧٧	٠.٦٨٢	١.٤٨٤	٠.٤٧٦
تعزيز التعاون مع عميل المراجعة	٤.٢٠٠	٠.٩١٣	٣.٣٦٣	٠.٩٢٤	٤.٠٦٤	٠.٦٧٢	٧.٩٥٨	٠.٠١٩
توفير دورات مراجعة ذات فترة زمنية ثابتة	٤.٢٠٠	٠.٧٦٤	٤.٢٧٣	٠.٧٨٦	٤.٠٨٥	٠.٧١٧	١.٠١١	٠.٦٠٣
زيادة مشاركة عملاء المراجعة في مشروعات المراجعة	٤.٠٨٠	١.٠٣٧	٤.٠٩١	٠.٧٠١	٤.٢٧٧	٠.٧٤٣	٠.٨٧٦	٠.٦٤٥
مناقشة نتائج المراجعة وفحصها بشكل متبادل مع عملاء المراجعة	٤.٢٩٢	٠.٦٩٠	٣.٤٥٥	١.١٢٨	٤.٠٨٥	٠.٨٠٣	٥.١١٨	٠.٠٧٧
ترشيد عملية التوثيق وتبسيط المستندات	٤.٢٠٠	١.٠٤١	٤.٠٠٠	١.٠٠٠	٤.١٠٦	٠.٨٦٦	٠.٩٨٨	٠.٦١٠

يتبين من الجدول السابق رقم (٩) ما يلي:

١- سجلت قيم الوسط الحسابي في جميع فئات الدراسة لقبول سمات المراجعة الداخلية الرشيقة قيما أكبر من (٣) وهذا يعني قبول تطبيق المراجعة الداخلية الرشيقة إذا ما توافرت المعرفة الكافية عن هذه المنهجية؛ إلا أن هناك تفاوت في درجة الموافقة على سمات المراجعة الداخلية الرشيقة بين الفئات وداخل الفئة الواحدة.

٢- حقق بند التركيز على خلق القيمة وليس التركيز على أهداف المراجعة كأحد سمات المراجعة الداخلية الرشيقة المرتبة الأولى من حيث الأهمية من وجهة نظر فئة الإدارة العليا ومسئولي IT بوسط حسابي بلغ (٤.٥٠٠)، يليه من حيث الأهمية بند مناقشة نتائج المراجعة وفحصها بشكل متبادل مع عملاء المراجعة بوسط حسابي بلغ (٤.٢٩٢)؛ بينما جاء بند زيادة مشاركة عملاء المراجعة في مشروعات المراجعة في المرتبة الأخيرة من حيث الأهمية بوسط حسابي قيمته (٤.٠٨٠).

٣- حقق أيضا بند التركيز على خلق القيمة وليس التركيز على أهداف المراجعة كأحد سمات المراجعة الداخلية الرشيقة المرتبة الأولى من حيث الأهمية من وجهة نظر المراجعين الداخليين بوسط حسابي بلغ (٤.٣٦٤)، يليه في الأهمية بند توفير دورات مراجعة ذات فترة زمنية ثابتة من وجهة نظرهم بوسط حسابي بلغ (٤.٢٧٣)، بينما احتل بند تعزيز التعاون مع عميل المراجعة المرتبة الأخيرة من حيث الأهمية بوسط حسابي بلغ (٣.٣٦٣).

٤- استمر بند التركيز على خلق القيمة وليس التركيز على أهداف المراجعة في تصدر الأهمية لدى فئة الباحثين بوسط حسابي بلغ (٤.٢٧٧)، بينما جاء بند زيادة مشاركة عملاء المراجعة في مشروعات المراجعة بوسط حسابي بلغ (٤.٢٧٧) وانحراف معياري (٠.٧٤٣)، واحتل بند تعزيز التعاون مع عميل المراجعة المرتبة الأخيرة من حيث الأهمية في وجهة نظرهم بوسط حسابي بلغ (٤.٠٦٤).

٥- سجلت قيم كروسكال واليز المناظرة لجميع البنود فيما عدا بند تعزيز التعاون مع عميل المراجعة مستوى معنوية أكبر من ٠.٠٥ مما يدل على عدم وجود اختلافات معنوية بين آراء فئات الدراسة بشأن تطبيق مفهوم المراجعة الداخلية الرشيقة ما عدا بند تعزيز التعاون مع عميل المراجعة، مما يشير إلى وجود استعداد للتحول نحو المراجعة الداخلية الرشيقة في مواجهة مخاطر الأمن السيبراني إذا ما توافرت المعرفة الكافية لهم.

النتيجة: القبول الجزئي للفرض HO_{33} القائل "لا توجد اختلافات معنوية بين آراء فئات المستقصى منهم بشأن الاستعداد للتحول نحو المراجعة الداخلية الرشيقة لمواجهة مخاطر الأمن السيبراني"، وقبول الفرض البديل فيما يتعلق ببند تعزيز التعاون مع عميل المراجعة.

٧- النتائج والتوصيات والدراسات المستقبلية

١/٧ النتائج:

هدفت هذه الدراسة إلى تطوير أداء المراجعة الداخلية لمواجهة مخاطر الأمن السيبراني في منظمات الأعمال المصرية، وذلك عن طريق تحديد مخاطر الأمن السيبراني وتأثيراتها، ودور المراجعة الداخلية في هذا المجال، وتحليل أسباب قصور أداء المراجعة الداخلية وفقا للمنهج التقليدي في مواجهة مخاطر الأمن السيبراني، وتحديد كيفية استخدام المنهجية الرشيقة لتطوير أداء المراجعة الداخلية، وتلافي أوجه القصور في مواجهة مخاطر الأمن السيبراني.

واستخدمت الدراسة أسلوب التحليل النظري للتعرف على مخاطر الأمن السيبراني وما يترتب عليها من خسائر على مستوى منظمات الأعمال وعلى المستوى القومي، وتحديد أهم الجهود الدولية والمحلية في مجال مواجهة مخاطر الأمن السيبراني، بالإضافة إلى دور المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني، وكيفية استخدام المنهجية الرشيقة لتطوير أداء المراجعة الداخلية والتغلب على أوجه القصور التي تتعرض لها في مواجهة هذه المخاطر؛ واختتمت الدراسة النظرية بوضع إطار مقترح لتطوير أداء المراجعة الداخلية باستخدام المنهجية الرشيقة.

كما استخدمت الدراسة الميدانية عينة من ١٢٧ مفردة من مسئولي الإدارة العليا وأقسام تكنولوجيا المعلومات والمراجعين الداخليين والباحثين، لتحليل آرائهم بشأن مخاطر الأمن السيبراني وتأثيراتها، وكذا آرائهم بشأن دور المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني ومدى الحاجة لتطوير المراجعة الداخلية، بالإضافة إلى تحليل آرائهم بشأن مدى الاستعداد للتحول إلى المراجعة الداخلية الرشيقة بدلا من المنهج التقليدي.

وتوصلت الدراسة في جانبها النظري إلى ما يلي:

١- أثبتت الدراسات السابقة وجود زيادة مستمرة في مخاطر الأمن السيبراني، وتسبب الهجمات السيبرانية في أضرار وخسائر كبيرة لمنظمات الأعمال والاقتصاد القومي؛ كما تناولت دور المراجعة الداخلية كخط دفاع ثالث في مواجهة مخاطر الأمن السيبراني، وطرحت مجموعة من العوامل اللازمة للقيام بهذا الدور بشكل فعال ومنها، تكرار عمليات المراجعة، التعاون مع خطي الدفاع الأول والثاني، معرفة المراجعين الداخليين بتكنولوجيا المعلومات ومفاهيم الأمن السيبراني، العلاقات الجيدة مع إدارة تكنولوجيا المعلومات، والتركيز على تقديم النصح والمشورة.

٢- كشف تحليل الدراسات السابقة عن قصور أداء المراجعة الداخلية في الوقت الراهن في مواجهة مخاطر الأمن السيبراني، وذلك بسبب عدم مرونة خطط المراجعة، وتطبيق المنهج التقليدي في المراجعة، وعدم التواصل الفعال بين المراجعين الداخليين والإدارة وأصحاب المصالح الرئيسيين، بالإضافة إلى عدم توافر الخبرات اللازمة في مجال التكنولوجيا والتحول الرقمي، مما إدى إلى الحاجة إلى تطوير أداء المراجعة الداخلية من خلال استخدام أحد مناهج التطوير الحديثة التي تلائم دور المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني، ومنها المنهجية الرشيقة.

٣- ظهرت المنهجية الرشيقة وتم استخدامها في صناعة تطوير البرمجيات، إلا أن الوقت الحالي شهد استخدام هذه المنهجية في جميع وظائف المنظمات ومنها المراجعة الداخلية، مما أدى إلى ظهور المراجعة الداخلية الرشيقة التي تركز على خلق القيمة وتعزيز التعاون مع عملاء المراجعة، وتحقيق الانضباط الزمني في إنهاء مهام المراجعة، وتقديم النصح والمشورة، والسعي إلى تقليل الخلافات من خلال الاتصال الفعال مع أصحاب المصالح الرئيسيين وتبسيط الوثائق والمستندات.

٤- تعد المنهجية الرشيقة أحد المناهج الملائمة لتطوير أداء المراجعة الداخلية وبشكل خاص في مواجهة مخاطر الأمن السيبراني، نظرا لأنها تتيح درجة عالية من المرونة في خطط المراجعة، وتعتمد على فرق العمل متعددة المهام والتخصصات، كما أنها تطبق الأسلوب الاستباقي في التعامل مع المخاطر، بالإضافة إلى أنها تستخدم دورات المراجعة قصيرة الأجل والتي تساعد على تقديم خدمات المراجعة في أسرع وقت ممكن وهذا يناسب دور المراجعة الداخلية في مواجهة مخاطر الامن السيبراني.

٥- يعتمد تطبيق المراجعة الداخلية الرشيقة على عدة مفاهيم لابد من توافر المعرفة الكافية بها مثل قائمة الأعمال المتراكمة، تعريف الاستعداد، سباقات المراجعة، تعريف الإنجاز، واجتماعات Scrums، وتستند إلى مجموعة من المبادئ المأخوذه عن البيان الرسمي لـــ Agile. كما يتطلب التطبيق السليم للمراجعة الداخلية الرشيقة تجنب بعض الأفكار الخاطئة ومنها أن فريق المراجعة الداخلية الرشيقة يفعل ما يشاء، وأن المراجعة الرشيقة لا ينتج عنها مستندات ووثائق، والقول بأن المنهجية الرشيقة لا تتبع ممارسات إدارة المشروع.

٦- تتوافر مجموعة من مرشدات التطبيق التي يمكن استخدامها في مجال دور المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني ومنها على المستوى الدولي إطار عمل COBIT وإطار تحسين البنية الأساسية الحيوية الصادر عن NIST وكذلك مقترحات

SEC، كما يتوافر محليا الاستراتيجية الوطنية للأمن السيبراني ومبادرات البنك المركزي المصري في مجال الأمن السيبراني.

٧- يتم تطبيق المراجعة الداخلية الرشيقة من خلال ثلاث مراحل قد تتشابه مع مراحل المنهج التقليدي في المراجعة من حيث الشكل، إلا أنها تختلف عنها في المضمون والمحتويات وطريقة أداء مهام المراجعة، والتعاون والتفاعل مع أصحاب المصالح الرئيسيين، ودورات العمل قصيرة الأجل وتكرار تقديم التقارير أثناء أعمال المراجعة، مما يجعل المراجعة الداخلية الرشيقة هي الطريقة الملائمة لأداء مهام المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني.

وتوصلت الدراسة الحالية في الجانب التطبيقي إلى ما يلي:

١- قبول الفرض القائل "لا توجد اختلافات معنوية بين آراء فئات المستقصى منهم بشأن تزايد مخاطر الأمن السيبراني في الوقت الحالي وفي المستقبل".

٢- قبول الفرض القائل "لا توجد اختلافات معنوية بين آراء فئات المستقصى منهم بشأن تسبب مخاطر الأمن السيبراني في خسائر كبيرة على مستوى منظمات الأعمال وعلى المستوى القومي".

٣- قبول الفرض القائل "لا توجد اختلافات معنوية بين آراء فئات المستقصى منهم بشأن قصور أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني في الوقت الراهن".

٤- قبول الفرض القائل "لا توجد اختلافات معنوية بين آراء فئات المستقصى منهم بشأن أسباب قصور أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني في الوقت الراهن".

٥- قبول الفرض القائل "لا توجد اختلافات معنوية بين آراء فئات المستقصى منهم بشأن إمكانية تطوير أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني من خلال استخدام مناهج التطوير الحديثة ومنها المنهجية الرشيقة ".

٦- قبول الفرض القائل "لا توجد اختلافات معنوية بين آراء فئات المستقصى منهم بشأن عدم توافر المعرفة الكافية بالمنهجية الرشيقة كأحد مناهج تطوير أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني".

٧- قبول جزئي للفرض القائل "لا توجد اختلافات معنوية بين آراء فئات المستقصى منهم بشأن الاستعداد للتحول نحو المراجعة الداخلية الرشيقة لمواجهة مخاطر الأمن السيبراني".

٢/٧ التوصيات:

بناء على نتائج الدراسة، يوصي الباحثان بما يلي:

١- ضرورة التوعية بمخاطر الأمن السيبراني وتأثيراتها السلبية على مستوى المنظمات وعلى المستوى القومي.

٢- تبني الأطر الدولية اللازمة في مجال مكافحة الهجمات والجرائم السيبرانية.

٣- ضرورة الاستفادة من مناهج التطوير الحديثة ومنها المنهجية الرشيقة في تطوير أداء المراجعة الداخلية.

٤- ضرورة الاعتراف بعدم توافر المعرفة الكافية واللازمة لتطبيق المنهجية الرشيقة، والاستفادة من جهود الباحثين في توفير هذه المعرفة ونشر ثقافة العمل الرشيق.

٥- توجيه جهود الباحثين نحو الاهتمام بهذا الجانب البحثي الحديث لتلافي القصور الموجود في أداء المراجعة الداخلية في مجال الأمن السيبراني.

٣/٧ الدراسات المستقبلية:

لم تتعرض الدراسة الحالية لعدة جوانب، مما يعد مجالا للبحوث المستقبلية ومنها ما يلي:

١- طرق وأساليب الإفصاح عن مخاطر الأمن السيبراني وتأثيراتها في التقارير المنشورة.

٢- أثر الإفصاح عن مخاطر الأمن السيبراني على أداء وقيمة منظمات الأعمال.

٣- دور لجان المراجعة في دعم أنشطة المراجعة الداخلية الرشيقة لمواجهة مخاطر الأمن السيبراني.

٤- أثر تطبيق المراجعة الداخلية الرشيقة على جودة المراجعة الخارجية.

المراجع:

أولا: باللغة العربية:

- الإبياري، هشام فاروق مصطفى (٢٠١٨). إعادة هندسة عملية المراجعة الداخلية: إطار ونموذج مقترح ودراسة استكشافية في بيئة الأعمال المصرية. مجلة البحوث المحاسبية، كلية التجارة، جامعة طنطا، ١، ١-٥٣.
- البنك المركزي المصري (٢٠١٩). تقرير الاستقرار المالي لعام ٢٠١٨.
- الرشيدي، طارق عبد العظيم وعباس، داليا عادل (٢٠١٩). أثر الإفصاح عن مخاطر الأمن السيبراني في التقارير المالية على أسعار الأسهم وأحجام التداول دراسة مقارنة في قطاع تكنولوجيا المعلومات. مجلة المحاسبة والمراجعة، ٢، ٤٣٩-٤٨٧.
- الزيود، محمود سليمان (٢٠٢١). أثر التدقيق الداخلي في الحد من مخاطر السيبرانية في البنوك التجارية الأردنية. رسالة ماجستير، كلية الاقتصاد والعلوم الإدارية، جامعة آل البيت- الأردن.
- القنبري، محمد قيس (٢٠٢٠). نحو مراجعة داخلية رشيقة. منصة المراجعة الداخلية iap.work.
- المجلس الأعلى للأمن السيبراني التابع لمجلس الوزراء المصري (٢٠١٧). الإستراتيجية الوطنية للأمن السيبراني (٢٠١٧-٢٠٢١).
- بانقا، علم الدين (٢٠١٩). مخاطر الهجمات الإلكترونية (السيبرانية) وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي. سلسلة دراسات تنموية، المعهد العربي للتخطيط بالكويت، ٦٣.
- صندوق النقد العربي "أمانة فريق الاستقرار المالي" (٢٠١٩). تقرير الاستقرار المالي في الدول العربية ٢٠١٩.
- عطية، أحمد صلاح (٢٠٢١). التحول الرقمي في مصر هل يلقي بمسئوليات جديدة على المراجع؟. مجلة البحوث التجارية، كلية التجارة، جامعة الزقازيق، ٤٣ (١)، ٥٣-٦٥.

ثانيا: مراجع باللغة الإنجليزية:

- Acharya, S. (2021). Agile Auditing for Increasing Efficiency. International Journal of Auditing and Accounting Studies, 3 (1), 79-107.
- Agarwal, C. A. R. (2021). Presentation on Agile Internal Audit Methodologies. agile internal audit.pdf (slideshare.net)

- Agile Manifesto (2001). 12 Principles. https://www.agilealliance.org/agile101/12-principles-behind-the-agile-manifesto/
- Alina, C. M., Cerasela, S. E., and Gabriela, G. (2017). Internal Audit Role in Cybersecurity. "Ovidius" University Annals, Economic Sciences Series, XVII (2), 510-513.
- Asian Confederation of Institutes of Internal Auditor "ACIIA" and SyCip Gorres Velayo& Co. "SGV" (2021). Internal Audit Transformed: Future of Work, Emerging Risks and Trends. 2020-IA-Survey-Report_June-2021.pdf (aciia.asia).
- Bakertilly (2019). The Agile Internal Audit Journey, Part 2: Applying the Agile Manifesto and Principles to Internal Audit. https://bakertilly.co.th/media/1273/bt_agile-journey-series_article-2.pdf
- BDO (2021). Audit Committee Priorities for 2022. https://www.bdo.com/getattachment/6c0a1d53-06bc-45c9-af17-da445f12ef91/ASSR_Audit-Committee-Priorities-for-2022.pdf
- Beerbaum, D. (2020). Application of Agile Audit: A Case Study Research. https://www.researchgate.net/publication/346652158_Application_of_agile_audit_A_case_study_research
- Catton, P. and Panavalli, P. (2020). Benefits of Utilizing Agile Internal Audit Methodology during COVID-19 Disruption. DHG. https://www.forvis.com/article/benefits-of-utilizing-agile-internal-audit-methodology-during-covid-19-disruption
- Crowe and Internal Audit Foundation (2018). The future of cybersecurity in internal audit. https://www.crowe.com/-/media/Crowe/LLP/folio-pdf/The-Future-of-Cybersecurity-in-IA-RISK-18000-002A-update.pdf
- Deloitte (2017). Becoming Agile a Guide to Elevating Internal Audit's Performance and Value Part 1: Understanding Agile Internal Audit. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-advisory-agile-internal-audit-part1-introduction-to-elevating performance.pdf
- Deloitte (2018). Auditing Agile Projects Your Grandfather's Audit Won't Work Here!. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-auditing-agile-projects-final.pdf
- Deloitte (2020). Internal Audit Considerations in Response to COVID-19 Navigating Change: An Unprecedented Challenge. https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-internal-audit-considerations-in-response-to-covid-19-noexp.pdf
- European Confederation of Institutes of Internal Auditors "ECIIA"(2020), Risk in Focus 2021. Hot Topics for Internal Auditors. https://www.eciia.eu/wpcontent/uploads/2020/09/100242-RISK-IN-FOCUS-2021-52PP-ECIIA-Online-V2.pdf (accessed 20 October 2020.

- Galvanize (2020). Sprinting Ahead with Agile Auditing. https://iiabelgium.org/wp-content/uploads/2020/08/eBook-sprinting-ahead-with-agile-auditing-002.pdf
- Gislen, M. (2016). Achieving Agile Quality an Action Research Study. Master Thesis, Faculty of Computing Blekinge Institute of Technology, Sweden.
- Haes, S., Van Grembergen, W., Joshi, A., and Huygh, T. (2020). Enterprise Governance of Information Technology: Achieving Alignment and Value in Digital Organizations. 3rd, Springer Nature Switzerland AG. Management for Professionals. https://doi.org/10.1007/978-3-030-25918-1.
- Institute of Internal Auditors "IIA" (2020), Rethinking Preparedness: Pandemics and Cybersecurity. https://global.theiia.org/knowledge/Public% 20Documents/IIA-Bulletin-Rethinking-Preparedness-Pandemics-and-Cybersecurity.pdf (accessed 15 October 2020).
- Institute of Internal Auditors "IIA" (2021). ONRISK a Guide to Understanding, Aligning, and Optimizing Risk 2022. https://www.theiia.org/globalassets/documents/content/research/onrisk/2021/2022-onrisk-report.pdf
- Institute of Internal Auditors "IIA" (2022a). North American Pulse of Internal Audit, March 2022, https://www.theiia.org/en/content/research/pulse-of-internalaudit/2022/2022-north-american-pulse-of-internal-audit/
- Institute of Internal Auditors "IIA" (2022b). Cybersecurity in 2022 Part 1: How the New SEC Proposals Could Change the Game. https://www.theiia.org/globalassets/site/content/articles/global-knowledge-brief/2022/cybersecurity-in-2022-part-1/cybersecurity-in-2022-part-1_final.pdf
- SonicWall, (2022). SonicWall Cyber Threat Report 2022. https://www.sonicwall.com/2022-cyber-threat-report/.
- Internal Audit Foundation "IAF" and Deloitte (2021). Premier Global Research Study- Assessing Internal Audit Competency: Minding the Gaps to Maximize Insights. https://web.theiia.org/cn/atxbg/Int_Audit_Competencie
- International Systems Audit and Control Association "ISACA" "COBIT 5" (2012). A Business Framework for the Governance and Management of Enterprise IT. https://books.google.com.eg/books?id=1iLKVlOIg9EC&printsec=frontcover&hl=ar&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false
- Islam, S., Farah, N., and Stafford, T. (2018). Factors Associated with Security/Cybersecurity Audit by Internal Audit Function: An International Study. Managerial Auditing Journal, 33 (4), 377-409.

- ISO/IEC. (2015). ISO/IEC Standard 38500: Information Technology - Governance of IT for the Organization. https://www.iso.org/standard/62816.html
- Joshi, P. L. (2021). A Review of Agile Internal Auditing: Retrospective and Prospective. International Journal of Smart Business and Technology, 9(2), 13-32.
- KPMG (2017). Cyber Security: The Changing Role of Internal Auditors, Survey of Internal Audit Professionals in Bahrain. https://assets.kpmg/content/dam/kpmg/bh/pdf/cyber-security-and-the-role-of-internal-auditors.pdf
- KPMG (2019). Agile Internal Audit White Paper on Working Agile within Internal Audit Functions Part I: Introducing Working Agile. https://assets.kpmg/content/dam/kpmg/nl/pdf/2020/sectoren/agile-internal-audit-1.pdf
- KPMG (2020a). Agile Internal Audit White paper on Working Agile within Internal Audit Functions Part II: Concrete Guidance for the set-up of the Agile Internal Audit Function and the Execution of Agile Audits. https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2020/10/agile-internal-audit-white-paper-on-working-agile-within-internal-audit-functions-part-2.pdf
- KPMG (2020b). Internal Audit: Key Risks & Focus Areas 2021. https://assets.kpmg/content/dam/kpmg/ie/pdf/2020/12/ie-internal-audit-focus-areas.pdf
- Kim, D. H., Kim, D. S., Koh, C., and Kim, H. W. (2013). An Information System Audit Model for Project Quality Improvement by the Agile Methodology. International Journal of Information and Education Technology, 3 (3), 295-299.
- Lois, P., Drogalas, G., Karagiorgos, A., and Vrontis, A. (2021). Internal Auditing and Cyber Security: Audit Role and Procedural Contribution. Int. J. Managerial and Financial Accounting, 13 (1), 25-47.
- Morgan, S. (2022). 2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics, Cybersecurity Ventures. Cisco. https://cybersecurityventures.com/cybersecurity-almanac-2022/.
- Morin, P. (2020). NIST Cybersecurity Framework- Assessing the Maturity of your Cybersecurity Program.
- National Institute of Standards and Technology "NIST" (2018). Framework for Improving Critical Infrastructure Cybersecurity. https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf
- Pei, R., Jin, Z., and Yang, Z. (2020). Cyber-attacks Measurement for Public Companies: An Empirical Analysis. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3607614

- Salin, H. and Lundgren, M. (2022). Towards Agile Cybersecurity Risk Management for Autonomous Software Engineering Teams. J. Cybersecurity. Priv., 2, 276–291.
- Shamsuddin, A., Adam, M., Adnan, S., Madzlan, S., and Yasin, Y. (2018). The Effectiveness of Internal Audit Functions in Managing Cybersecurity in Malaysia's Banking Institutions. International Journal of Industrial Management, 8 (4), 61-69.
- Sharton, B. R. (2020). Will Coronavirus Lead to More Cyber Attacks?. https://hbr.org/2020/03/will-coronavirus-lead-to-more-cyber-attacks?autocomplete=true (accessed 20 October 2020).
- Slapnicar, S., Vuko, T., Cular, M., and Drascek, M. (2022). Effectiveness of cybersecurity audit. International Journal of Accounting Information Systems, 44, 1-21.
- Steinbart, P., Gal, G., Raschke, R., and Dilla, W. (2013). The Influence of Internal Audit on Information Security Effectiveness: Perceptions of Internal Auditors. https://papers.ssrn.com/sol3/papers.cfm?abstractid=2685943
- U.S. Securities and Exchange Commission "SEC" (2022a). "SEC Proposes Cybersecurity Risk Management Rules and Amendments for Registered Investment Advisers and Funds," press release, February 9. https://www.sec.gov/news/press-release/2022-20.
- U.S. Securities and Exchange Commission "SEC" (2022b). Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. March 9. https://www.sec.gov/rules/proposed/2022/33-11038.pdf.
- Wright, R. A. (2019). Agile Auditing Transforming the Internal Audit Process. Internal Audit Foundation.

ملحق رقم (١) قائمة الاستقصاء

الأستاذ الفاضل /الأستاذة الفاضلة

السلام عليكم ورحمة الله وبركاته؛

نتوجه لسيادتكم بهذه القائمة أملا في الحصول علي تعاونكم للعمل على تطوير أداء المراجعة الداخلية من خلال استخدام المنهجية الرشيقة Agile Approach لمواجهة مخاطر الأمن السيبراني التي تتعرض لها منظمات الأعمال المصرية. وذلك من خلال البحث الذي يعده الباحثان بعنوان " استخدام المنهجية الرشيقة في تطوير أداء المراجعة الداخلية لمواجهة مخاطر الأمن السيبراني". وإننا نقدر سلفا مساهمتكم المشكورة في هذا المجهود المشترك ونضعها محل عناية وتقدير من أجل الرقي بدور المراجعة الداخلية كأحد آليات الحوكمة.

ونود التأكيد لسيادتكم أن الهدف من استيفاء هذه القائمة لن يتعدي أغراض البحث العلمي، لذلك سوف تكون إجاباتكم موضع سرية تامة.

والله ولي التوفيق؛

الباحثان

مصطلحات:

– مخاطر الأمن السيبراني (مخاطر الهجمات الإلكترونية): هي أنشطة غير مشروعة تتعرض لها البنية الأساسية للمنظمة عن طريق استغلال الثغرات الأمنية في نظم المعلومات، وذلك بهدف التأثير السلبي في جميع أنشطة المنظمة وإمكانياتها، وإلحاق الضرر المادي بها وبسمعتها والكشف عن معلومات المنظمة أو إجراء تعديلات عليها أو تدمير هذه المعلومات.

– مفهوم المراجعة الداخلية الرشيقة: هي طريقة للتفكير تركز على القيمة وتعزيز التعاون مع أصحاب المصالح لتقليل الخلافات حول نتائج المراجعة، وتحقيق الانضباط الزمني في تنفيذ مهام المراجعة، وتقديم الأفكار وتوفير الاستجابات في الوقت المناسب، وذلك من خلال تطوير الأعمال وتكرار التخطيط والعمل القائم على التعاون بين فرق العمل.

بيانات عامة

الاسم:.....(إذا رغبت في ذكره)

جهة العمل: .....

المؤهل العلمي:..... عدد سنوات الخبرة:.....

الوظيفة الحالية:.....

القسم الأول

ويهدف هذا القسم إلي تحديد مدى إدراك عينة الدراسة لتزايد مخاطر الهجمات السيبرانية وتأثيراتها على منظمات الأعمال المصرية وعلى المستوى القومي.

– برجاء وضع علامة (√) أمام العبارة التي تمثل الإجابة الصحيحة من وجهة نظركم :

١/١ من وجهة نظر سيادتكم هل توافق على أن مخاطر الأمن السيبراني تأخذ اتجاها متزايدا باستمرار في الوقت الحالي وفي المستقبل؟

موفق بشدة ( ) موافق ( ) موافق إلى حد ما ( ) غير موافق ( ) غير موافق على الإطلاق ( ).

٢/١ من وجهة نظر سيادتكم هل توافق على أن مخاطر الأمن السيبراني تؤدي إلى خسائر فادحة على مستوى الشركات وعلى المستوى القومي؟

موفق بشدة ( ) موافق ( ) موافق إلى حد ما ( ) غير موافق ( ) غير موافق على الإطلاق ( ).

القسم الثاني

ويهدف هذا القسم إلى تقييم أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني في الوقت الحالي، والتعرف على أسباب قصور أدائها في منظمات الأعمال المصرية.

١/٢ من وجهة نظر سيادتكم هل توافق على أن المراجعة الداخلية تعاني حاليا من قصور في أداء دورها في مواجهة مخاطر الأمن السيبراني بمنظمات الأعمال المصرية؟

موفق بشدة ( ) موافق ( ) موافق إلى حد ما ( ) غير موافق ( ) غير موافق على الإطلاق ( ).

٢/٢ هل توافق سيادتكم على أن ما يلي يعد من أسباب قصور أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني بمنظمات الأعمال المصرية:

البنود	موافق بشدة (٥)	موافق (٤)	موافق إلى حد ما (٣)	غير موافق (٢)	غير موافق على الإطلاق (١)
عدم توافر الخبرات اللازمة في مجال تكنولوجيا المعلومات والتكنولوجيا الرقمية					
تطبيق المنهج التقليدي في المراجعة الداخلية					
عدم التواصل الفعال والسريع مع الإدارة وأصحاب المصالح الرئيسيين					
عدم مرونة خطط المراجعة الداخلية					
التأخير في تقديم تقارير المراجعة الداخلية					

القسم الثالث

ويهدف هذا القسم إلى تحديد مدى إمكانية تطوير أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني من خلال استخدام المنهجية الرشيقة والوقوف على مدى استعداد منظمات الأعمال المصرية للتحول نحو تطبيق المراجعة الداخلية الرشيقة.

١/٣ من وجهة نظر سيادتكم هل توافق على أنه يمكن تطوير أداء المراجعة الداخلية في مواجهة مخاطر الأمن السيبراني بمنظمات الأعمال المصرية من خلال استخدام المنهجية الرشيقة Agile Approach؟

موفق بشدة ( ) موافق ( ) موافق إلى حد ما ( ) غير موافق ( ) غير موافق على الإطلاق ( ).

٢/٣ هل توافق سيادتكم على أن هناك معرفة كافية بمفاهيم ومبادئ وخطوات تطبيق المراجعة الداخلية الرشيقة في منظمات الأعمال المصرية؟

موفق بشدة ( ) موافق ( ) موافق إلى حد ما ( ) غير موافق ( ) غير موافق على الإطلاق ( ).

٣/٣ فيما يلي مجموعة من البنود التي تمثل سمات المراجعة الداخلية الرشيقة والتي توضح قبول سيادتكم لهذه المنهجية الحديثة، ودرجة استعداد سيادتكم لقبول وتطبيق مفاهيم المراجعة الداخلية الرشيقة، رجاء اختيار ما يمثل وجهة نظركم ومدى استعدادكم لقبول هذه البنود:

البنود	موافق بشدة (٥)	موافق (٤)	موافق إلى حد ما (٣)	غير موافق (٢)	غير موافق على الإطلاق (١)
التركيز على خلق القيمة وليس التركيز على أهداف المراجعة					
تعزيز التعاون بين المراجعين الداخليين وعميل المراجعة					
توفير دورات مراجعة ذات فترة زمنية ثابتة					
زيادة مشاركة عملاء المراجعة في مشروعات المراجعة					
مناقشة نتائج المراجعة وفحصها بشكل متبادل مع عملاء المراجعة					
ترشيد عمليات التوثيق وتبسيط المستندات					